

IntechOpen

IntechOpen Series
Civil Engineering Volume 21

Connected, Cooperative, and Automated Mobility

Policy and Deployment Challenges, Threats, and Future Directions

Edited by Stefano de Luca, Roberta Di Pace, Facundo Storani and Francesca Bruno



Connected, Cooperative, and Automated Mobility - Policy and Deployment Challenges, Threats, and Future Directions

Edited by Stefano de Luca, Roberta Di Pace, Facundo Storani and Francesca Bruno

Published in London, United Kingdom

Connected, Cooperative, and Automated Mobility - Policy and Deployment Challenges, Threats, and Future Directions
http://dx.doi.org/10.5772/intechopen.1009487
Edited by Stefano de Luca, Roberta Di Pace, Facundo Storani and Francesca Bruno

Contributors
Agostino Marcello Mangini, Anna Laura Pala, Antonio Salcuni, Ayan Roy, Behnood Baiky, Caterina Malandri, Chieh Tsai, Elena Haller, Emad El-Din Mazied, Facundo Storani, Franco Filippi, Gaetano Volpe, Giuseppe Stecca, Hesham A. Rakha, Hisham Y. Makahleh, Kenan Ahiska, Khaled Hamad, Luca Mantecchini, Maria Nadia Postorino, Maria Pia Fanti, Mario Binetti, Mario Marinelli, Mohamad Tulimat, Murad Mehrab Abrar, Nadia Giuffrida, Oscar Amador Molina, Rafael Corvillo, Ramin Ranjbar Motlagh, Raúl Parada, Roberta Di Pace, Salim Hariri, Salvatore Viscio, Sharon L. Burton, Stefano de Luca, Takahito Yoshizawa, Xuelian Wu, Yunfan Huang

© The Editor(s) and the Author(s) 2026
The rights of the editor(s) and the author(s) have been asserted in accordance with the Copyright, Designs and Patents Act 1988. All rights to the book as a whole are reserved by INTECHOPEN LIMITED. The book as a whole (compilation) cannot be reproduced, distributed or used for commercial or non-commercial purposes without INTECHOPEN LIMITED's written permission. Enquiries concerning the use of the book should be directed to INTECHOPEN LIMITED rights and permissions department (permissions@intechopen.com).
Violations are liable to prosecution under the governing Copyright Law.



Individual chapters of this publication are distributed under the terms of the Creative Commons Attribution 4.0 License which permits commercial use, distribution and reproduction of the individual chapters, provided the original author(s) and source publication are appropriately acknowledged. If so indicated, certain images may not be included under the Creative Commons license. In such cases users will need to obtain permission from the license holder to reproduce the material. More details and guidelines concerning content reuse and adaptation can be found at http://www.intechopen.com/ copyright-policy.html.

Notice
Statements and opinions expressed in the chapters are these of the individual contributors and not necessarily those of the editors or publisher. No responsibility is accepted for the accuracy of information contained in the published chapters. The publisher assumes no responsibility for any damage or injury to persons or property arising out of the use of any materials, instructions, methods or ideas contained in the book.

First published in London, United Kingdom, 2026 by IntechOpen
IntechOpen is the global imprint of INTECHOPEN LIMITED, registered in England and Wales, registration number: 11086078, 167-169 Great Portland Street, London, W1W 5PF, United Kingdom

For EU product safety concerns: IN TECH d.o.o., Prolaz Marije Krucifikse Kozulić 3, 51000 Rijeka, Croatia, info@intechopen.com or visit our website at intechopen.com.

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Connected, Cooperative, and Automated Mobility - Policy and Deployment Challenges, Threats, and Future Directions
Edited by Stefano de Luca, Roberta Di Pace, Facundo Storani and Francesca Bruno
p. cm.

This title is part of the Civil Engineering Book Series, Volume 21
Topic: Transportation Engineering
Series Editor: Assed Haddad
Topic Editor: Saúl Antonio Obregón Biosca

Print ISBN 978-1-83635-539-7
Online ISBN 978-1-83635-538-0
eBook (PDF) ISBN 978-1-83635-540-3
ISSN 3029-0287

If disposing of this product, please recycle the paper responsibly.

IntechOpen Book Series

Civil Engineering

Volume 21

Aims and Scope of the Series

Civil engineering is a traditional field of engineering from which most other branches of engineering have evolved. It comprises traditional sub-areas like transportation, structures, construction, geotechnics, water resources, and building materials. It also encompasses sustainability, risk, environment, and other concepts at its core. Historically, developments in civil engineering included traditional aspects of architecture and urban planning as well as practical applications from the construction industry. Most recently, many elements evolved from other fields of knowledge and topics like simulation, optimization, and decision science have been researched and applied to increase and evolve concepts and applications in this field. Civil engineering has evolved in the last years due to the demands of society in terms of the quality of its products, modern applications, official requirements, and cost and schedule restrictions. This series addresses real-life problems and applications of civil engineering and presents recent, cutting-edge research as well as traditional knowledge along with real-world examples of developments in the field.

Meet the Series Editor



Professor Assed N. Haddad is a Civil Engineer with a degree from the Federal University of Rio de Janeiro (UFRJ) earned in 1986, as well as a Juris Doctor degree from the Fluminense University Center earned in 1993, and a Master's degree in Civil Engineering from the Fluminense Federal University (UFF) obtained in 1992. He completed his Ph.D. in Production Engineering from COPPE / Federal University of Rio de Janeiro in 1996. Professor Haddad's academic pursuits have taken him to postdoctoral stays at the University of Florida, USA in 2006; at the Universitat Politècnica de Catalunya, Spain in 2010; and at the University of New South Wales Sydney, Australia in 2019. Currently, he serves as a Full Professor at the Federal University of Rio de Janeiro. He has held visiting professorships at various institutions including the University of Florida, Universitat Politècnica de Catalunya, Universitat Rovira i Virgili, and Western Sydney University. His research expertise encompasses Civil, Environmental, and Production Engineering, with a primary focus on the following topics: Construction Engineering and Management, Risk Management, and Life Cycle Assessment. He has been the recipient of research grants from the State of Rio de Janeiro, Brazil: CNE FAPERJ from 2019 to 2022 and from 2023 to 2025. Additionally, his research grants obtained from the Brazilian Government CNP since 2012 last to this date. Professor Haddad has been involved in several academic endeavors, being the Guest Editor of the International Journal of Construction Management; MDPI's Sustainability, Energies, and Infrastructures; Associate Editor at Frontiers in Built Environment / Sustainable Design and Construction; Guest Editor at Frontiers in Built Environment / Construction Management; and Academic Editor of the Journal of Engineering, Civil Engineering Section of Hindawi. He is currently a Professor of the Environmental Engineering Program at UFRJ and the Civil Engineering Program at UFF.

Meet the Volume Editors



Stefano de Luca has been a Full Professor of Transportation Planning in the Department of Civil Engineering at the University of Salerno since 2020. His research and teaching activities focus on Transportation Systems planning and design, Travel behavior modeling, Intelligent transportation systems, and Logistics. He is the Director of the Laboratory of Transport Systems Engineering and Sustainable Mobility, the Rector's Delegate for 'Mobility to/from the University', and the scientific coordinator of the National Center for Sustainable Mobility for the University of Salerno, as well as the scientific coordinator of the MaaS4Campania project. Author of over 165 scientific publications in international and national journals, books, and conference proceedings, he is a member of the Italian Society of Transport Professors and IEEE. He also serves on the editorial boards of Transportation Research Part F, Journal of Advanced Transportation, Sustainability, Standards, and Frontiers in Transportation.



Roberta Di Pace has been an Associate Professor in Transportation Engineering at the Department of Civil Engineering since 2021. Her research and teaching activities focus on: Connected, cooperative, and automated mobility; Intelligent transportation systems; Transportation Network resilience and optimization; models and algorithms; traffic flow modeling and control; choice behavior modeling and enhanced paradigms; and smart/sustainable mobility. She is the author of more than 200 articles in books, scientific journals, and conference proceedings. She has coordinated and participated in several national and international research projects on connected, cooperative, and automated mobility and intelligent transportation systems. She is an Academic Editor for *IEEE Transactions on Intelligent Transportation Systems, Transportmetrica B, Journal of Advanced Transportation, Mathematical Problems in Engineering*, and *Smart Cities.*



Facundo Storani is an Assistant Professor in the Laboratory of Transport Systems Engineering and Sustainable Mobility (ISTMoS) at the Department of Civil Engineering, University of Salerno, Italy. He holds a double degree in Civil Engineering from the National University of Córdoba (Argentina) and the University of Salerno, where he earned a Ph.D. in Risk and Sustainability in Civil, Architectural, and Environmental Engineering Systems. He has contributed to several national and international research projects on sustainable and intelligent mobility, focusing on optimizing travel demand and enhancing road network performance in cooperative, connected, and automated mobility systems. His research and teaching activities cover intelligent transportation systems, traffic analysis and control, transportation network modeling and simulation, discrete choice modeling, and sustainable mobility.



Francesca Bruno is a Research Fellow at the Laboratory of Transport Systems Engineering and Sustainable Mobility (ISTMoS), within the Department of Civil Engineering at the University of Salerno, Italy. She holds an MSc in Transportation Engineering and a Ph.D. in Risk and Sustainability in Civil, Architectural, and Environmental Engineering Systems. Her research focuses on travel and driving behavior analysis and modeling, as well as transport planning. She investigates behavioral paradigms underlying the adoption of innovative mobility solutions, designs stated- and revealed-preference surveys, and contributes to several national research projects on sustainable mobility. She is a member of the research unit involved in the SUNRISE Observatory of the National Center for Sustainable Mobility (MOST) and collaborates with ENEA within the Italian National Electricity System Research Program.

Contents

Preface **XIII**

Section 1
Frameworks and Strategy **1**

Chapter 1 **3**
Connected Mobility: Technologies, Gaps and the Road Ahead
by Elena Haller and Oscar Amador Molina

Chapter 2 **31**
Policy Pathways for Autonomous Vehicles in Urban Mobility: Insights and Strategic Lessons from a Systematic Review
by Hisham Y. Makahleh

Chapter 3 **55**
Cooperative Driving and Collective Navigation Architectures for CCAVs: Contemporary Techniques, Simulators, Datasets, and Research Directions
by Kenan Ahiska

Chapter 4 **77**
Perspective Chapter: Vehicle Platoon String Stability through the Lens of O-RAN – Opportunities, Challenges and Future Directions
by Emad El-Din Mazied and Hesham A. Rakha

Section 2
Security and Resilience **109**

Chapter 5 **111**
Security and Resilience in Autonomous Vehicles: A Proactive Design Approach
by Chieh Tsai, Murad Mehrab Abrar and Salim Hariri

Chapter 6 **133**
Security and Privacy Threats in Connected Vehicle Environment
by Ayan Roy

Chapter 7 **151**
Security and Privacy of ITS Standards and Their Research Challenges
by Takahito Yoshizawa

Chapter 8 **171**
Cybersecurity Risk Management in Cooperative Intelligent Transport Systems
by Ramin Ranjbar Motlagh

Chapter 9 **189**
The Road to Autonomous Vehicular Security: From Manual Updates to Lifetime Defenses Driven by Intelligent Agents
by Yunfan Huang

Section 3
Human Factors and Trust **211**

Chapter 10 **213**
Designing Trustworthy Futures: Research Priorities for Human-Centered, Connected, and Autonomous Mobility
by Sharon L. Burton

Chapter 11 **241**
Impacts of Autonomous Vehicles in a Mixed Roadway Environment: A Diamond Interchange Case Study
by Khaled Hamad and Mohamad Tulimat

Chapter 12 **261**
Applications of Driving Simulators in Intelligent Transportation Systems: Investigating Driver Behavior under Variable Speed Limits
by Behnood Baiky, Facundo Storani, Roberta Di Pace and Stefano de Luca

Chapter 13 **277**
Trajectory Prediction for Collision Avoidance of Vulnerable Road Users in CCAM Scenarios Using Stacking Regression and Deep Learning
by Raúl Parada and Rafael Corvillo

Section 4
Applications and Operational Insights **305**

Chapter 14 **307**
Enhanced Strategies for Wide-Area Traffic Control
by Franco Filippi, Roberta Di Pace, Facundo Storani and Stefano de Luca

Chapter 15 **325**
A DRL-Based Control Strategy for Efficient Highway Entry in Congested Scenarios
by Agostino Marcello Mangini, Gaetano Volpe, Antonio Salcuni and Maria Pia Fanti

Chapter 16 **347**
Connected and Autonomous Vehicle Platoons and Traffic Bottlenecks: Effects on Recurrent and Non-Recurrent Congestion in Mixed Traffic Conditions
by Caterina Malandri, Luca Mantecchini, Maria Nadia Postorino and Xuelian Wu

Chapter 17 **371**
Optimization of Highway On-Ramp Merging Maneuvers in Pure and Mixed CAV Environments: An Overview
by Salvatore Viscio, Nadia Giuffrida, Mario Marinelli and Mario Binetti

Chapter 18 **393**
Route Guidance in ITS: Systems Classification, Enabling Technologies, and Methodological Approaches
by Anna Laura Pala and Giuseppe Stecca

Preface

Connectivity and automation are opening new opportunities to enhance vehicles and mobility services, making transportation safer, more efficient, and more user-oriented. By seamlessly connecting users, vehicles, and services through digital infrastructures, travel experiences are enriched, transforming mobility into more than the mere act of moving from one place to another. Technologies related to Intelligent Connected Vehicles and Intelligent Transportation Systems are profoundly reshaping travel and driving patterns, generating significant economic and social benefits. Advances in communication protocols, artificial intelligence (AI), and big data analytics are driving the development of increasingly effective intelligent and connected transport systems. However, several open challenges remain, particularly in the domains of control, management, and data-driven analysis, which require further research and innovation.

Modern vehicles increasingly rely on digital connectivity, enabling communication with other vehicles and road infrastructure through Cooperative Intelligent Transport Systems (C-ITS). These systems allow road users and traffic managers to share information and coordinate actions, enhancing road safety, traffic efficiency, driving comfort, and the integration of automated vehicles. Cooperation, connectivity, and automation are no longer separate technological pathways but are progressively converging into a unified smart mobility ecosystem.

This book aims to analyze, develop, and validate approaches, methodological tools, and procedures for testing Cooperative, Connected, and Automated Mobility (CCAM). It brings together contributions that present innovative control and analytical methods based on next-generation intelligent transportation systems, with the aim of advancing scientific and technological knowledge and providing methodological support to stakeholders involved in defining strategies, technical standards, and guidelines for future mobility. The volume integrates both review and methodological contributions, focusing on traffic optimization strategies, technological solutions, analytical frameworks, and future market perspectives. It also includes assessments of the potential positive and negative impacts on transport system performance, environmental sustainability, safety, and equity.

The book is structured into four interconnected sections, each addressing a key dimension of the evolving ecosystem of connected, cooperative, and automated mobility.

Section I (Frameworks and Strategy) brings together four contributions that define roadmaps, governance models, and policy directions. It addresses how institutions, researchers, and industry can shape coherent strategies to guide the transition toward intelligent and sustainable mobility systems.

Section II (Security and Resilience) explores the critical issue of protecting increasingly connected transport infrastructures. It examines cybersecurity threats, system vulnerabilities, and resilience strategies to safeguard both physical and digital components against malicious actors.

Section III (Human Factors and Trust) investigates the interaction between users and technology. This section highlights behavioral aspects, acceptance dynamics, and the conditions under which trust in automated and connected systems can be established and maintained.

Section IV (Applications and Operational Insights) extends the previously introduced perspectives to real-world contexts, presenting applied studies and experimental evidence on how advanced technologies can be implemented in practice, bridging the gap between theory and deployment.

The sections offer a comprehensive, multidisciplinary perspective, combining strategic, technological, and human-centered perspectives to support the development of safe, resilient, and user-oriented mobility systems.

Section I, Frameworks and Strategy, consists of 4 contributions.

The first contribution presents connectivity as a key enabler of CCAM and outlines the main technologies and standards. It reviews V2V and V2I communication, highlighting real-world applications, limitations, and risks. It also discusses future directions, such as extending connectivity to multimodal road users to support more resilient mobility systems.

The second contribution highlights how Autonomous vehicles (AVs) have the potential to improve safety, accessibility, efficiency, and emissions in cities, yet their adoption remains limited. This chapter develops evidence-based policy pathways for urban AV deployment, drawing on a review of 41 studies and insights from AV pilots and mobility transitions, including electric, shared, and micromobility. The findings highlight the importance of transparent governance, stakeholder collaboration, alignment with climate goals, and equity to support the transition from pilots to sustainable urban transport systems.

The third contribution explores the CCAM framework, using connected and cooperative autonomous vehicles (CCAVs) to improve safety and efficiency. It examines architectures for autonomous driving and navigation, including multi-agent reinforcement learning and deep learning–based cooperative approaches. It also analyzes simulators and datasets for benchmarking, examines fusion strategies for navigation, and outlines future research directions.

The final contribution reviews platoon control within a wireless networked control framework, highlighting Open RAN (O-RAN) as a key enabler through its open, programmable, and AI-driven architecture. O RAN supports integrated communication and control while addressing challenges such as latency, reliability, and coordination in intelligent transportation systems.

Section II, Security and Resilience, consists of 5 contributions.

The first contribution establishes a comprehensive taxonomy of AV cyber-physical threats and proposes a resilient architecture rooted in redundancy and proactive anomaly detection. Validated through hardware testing, the research demonstrates how integrated fallback mechanisms maintain operational safety during sensor and software attacks, ensuring continuity in adversarial environments.

The second contribution reviews threats and solutions (cryptography, IDS, blockchain) related to data exchange among vehicles, infrastructure, and users in Connected Vehicle (CV) and V2X technologies, which may pose significant security and privacy risks, including eavesdropping, spoofing, and system attacks. The paper also highlights open challenges, including scalability, post-quantum resilience, and privacy protection.

The third contribution examines security vulnerabilities in ITS standards developed by IEEE, SAE, and ETSI, highlighting critical unresolved issues and related threats. It discusses adversarial attacks and system-level weaknesses that may compromise the integrity of ITS. It also emphasizes the need to transition to post-quantum cryptography to ensure resilient, trustworthy ITS deployments.

The fourth contribution analyzes threats and risk management frameworks (NIST CSF, ISO/SAE 21434), highlighting the need for integrated cybersecurity to ensure safe and trusted connected mobility. Indeed, C-ITS significantly extends this connectivity and improves safety, efficiency, and intelligence in transport systems. However, this expanded connectivity increases cybersecurity risks, exposing critical functions to potential remote attacks.

The fifth contribution reviews the development of lifelong learning-in-the-loop-based intrusion detection systems (LL IDS), from human-in-the-loop models to federated, privacy-preserving approaches. It highlights their role in developing resilient, adaptive security mechanisms. Future directions, including the use of large language models to enable fully autonomous cybersecurity for CCAM ecosystems, are explored.

Section III, Human Factors and Trust, consists of 4 contributions.

The first contribution outlines human-centered research priorities for CCAM, balancing AI-driven innovation with essential ethical considerations like transparency and accountability. It advocates for a multidisciplinary, inclusive design approach to ensure mobility systems are sustainable, equitable, and validated through real-world testing.

The second contribution examines the CCAM framework as a transformative paradigm integrating AI, big data, and advanced communication to enhance transportation safety, efficiency, and mobility services. It highlights key challenges in system control, management, and validation, as well as the need for secure, interoperable, and accountable infrastructures. It also argues for inclusive, sustainable mobility systems and multidisciplinary research approaches.

The third contribution investigates driver behavior and compliance with Variable Speed Limits (VSLs) by analyzing the current state of the art on research utilizing driving simulators. It highlights simulators as essential, safe environments for bridging the gap between theoretical traffic control models and real-world human responses.

The fourth contribution enhances the safety of Vulnerable Road Users (VRUs) in CCAM through AI-based trajectory prediction and collision-avoidance systems. It leverages geospatial data from user devices and lightweight models optimized for real-time, low-latency inference. By integrating predictive models into the CCAM infrastructure, it improves situational awareness and proactive risk mitigation.

Section IV, Applications and Operational Insights, consists of 5 contributions.

This section, except for the fifth contribution, presents the results obtained within the Italian Sustainable Mobility Center, funded by "NextGenerationEU" - Italian Ministry of University and Research MUR Missione 4 Componente 2, Investimento 1.4 - Grant id CN00000023, PNRR Sustainable Mobility Center (Centro Nazionale per la Mobilità Sostenibile).

The first contribution evaluates wide-area traffic control strategies, focusing on MFD-based models and gating techniques to optimize urban flow and reduce congestion. It explores the theoretical foundations and adaptive mechanisms required for real-time management while weighing environmental and safety benefits against implementation challenges.

The second contribution addresses the challenge of traffic management in high-density urban areas, focusing on ramps and merging points where congestion and safety risks are critical. It proposes a Deep Reinforcement Learning approach based on an Actor-Critic framework to optimize vehicle coordination via intelligent traffic-light control. The methodology balances efficiency and safety by minimizing delays and penalizing abrupt braking events.

The third contribution examines the transformative role of Connected and Autonomous Vehicle (CAV) platooning in improving highway traffic, particularly at bottlenecks. It analyzes mixed traffic scenarios with both CAVs and Human-Driven Vehicles, accounting for recurrent merging congestion and non-recurrent disruptions, such as breakdowns. Through microsimulation, the study evaluates the effects of platoon size and market penetration on capacity, travel times, and environmental impacts.

The fourth contribution reviews optimization strategies for highway on-ramp merging in both pure CAV and mixed traffic environments with Human-Driven Vehicles. In fully automated settings, coordinated control and real-time communication enable precise optimization of speed, position, and trajectories, improving efficiency and safety. In mixed traffic, methods integrate CAV control with behavioral models of human drivers to manage heterogeneous interactions during merging.

The final contribution introduces an innovative trajectory prediction approach that integrates regression models and deep learning techniques to enhance collision avoidance systems across CCAM operational domains, including urban driving and protected zones. Particular emphasis is placed on computational efficiency and real-time applicability, which are essential requirements for large-scale deployment.

Stefano de Luca, Roberta Di Pace, Facundo Storani and Francesca Bruno
Transportation Systems Engineering and
Sustainable Mobility Laboratory - ISTMoS Lab,
Department of Civil Engineering,
University of Salerno,
Fisciano (SA), Italy

Section 1

Frameworks and Strategy

Chapter 1

Connected Mobility: Technologies, Gaps and the Road Ahead

Elena Haller and Oscar Amador Molina

Abstract

This chapter explores connectivity as a foundational element in the evolution of the connected aspect of Cooperative, Connected, and Automated Mobility (CCAM). Beginning with an accessible tutorial on the core principles, metrics, and technologies – such as cellular or Dedicated Short Range Communications (DSRC) – the chapter offers a comparative analysis of existing communication standards. It also examines the current implementations, addressing Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) connectivity, highlighting real-world applications, known limitations, and risk factors, including spectrum constraints, coexistence of different technologies/versions, and scenario dependence. Future perspectives are presented to address these challenges and include alternative approaches such as Integrated Sensing and Communication (ISAC). The chapter also emphasizes expanding connectivity to Multimodal Road Users (MRUs), aiming for a fully inclusive connected ecosystem. Through this structured analysis, we identify technological gaps and outline future research needs, helping guide the development of resilient and universal communication frameworks in mobility systems.

Keywords: connectivity, connected vehicles, CCAM, V2X, DSRC, ISAC, RadCom, C–V2x

1. Introduction

Road accidents remain a major global concern, causing 19,800 fatalities in Europe in 2024 [1] and about 1.9 million deaths worldwide every year [2]. Initiatives such as Vision Zero [3] aim to eliminate traffic fatalities and serious injuries by 2050 through a combination of education, law enforcement, road infrastructure improvements, and the development of Intelligent Transport Systems (ITSs).

ITSs integrate smart infrastructure and vehicles to improve both road safety and traffic efficiency. Their cooperative extension, Cooperative Intelligent Transport System (C-ITS), relies on Vehicle-to-Anything (V2X) communications, where vehicles interact with other vehicles (V2V), infrastructure (V2I), pedestrians (Vehicle-to-Pedestrian (V2P)), and the network (Vehicle-to-Network (V2N)). This connectivity underpins the vision of CCAM, enabling increasingly automated and coordinated mobility.

Vehicular communications, however, differ fundamentally from traditional wireless networks due to high mobility, dynamic topologies, and strict safety requirements. The field of Vehicular Ad Hoc Networks (VANETs) has addressed these aspects first in purely *ad hoc* settings and later through cellular-based approaches. Today, two complementary technologies – IEEE 802.11p-based DSRC and Cellular V2X (C–V2X) – provide the foundation for CCAM services, with further deployments expected. Their coexistence raises challenges of interoperability, spectrum sharing, and harmonization, especially as fleets remain heterogeneous in terms of connectivity and automation capabilities.

In this chapter, we first provide a tutorial on the foundations of vehicular communications (Section 2). We then discuss current enabling technologies and deployments (Section 3), and finally outline open challenges and future perspectives (Section 4). Conclusions are presented in Section 5.

2. Tutorial

Vehicular networks enable a wide range of safety and efficiency applications by allowing vehicles, infrastructure, and other road users to exchange timely information. International standardization bodies, such as SAE International and the European Telecommunications Standards Institute (ETSI), have defined applications and particular use cases, approaching them through the exchange of messages between road users [4, 5]. In this section, we describe these applications, analyze the phenomena that affect their communication channels, and identify the performance metrics and communication challenges that underlie the design of reliable V2X systems.

2.1 Applications and challenges of connected mobility

Building a V2X network starts with understanding its purpose and the factors that distinguish it from other wireless systems. V2X is designed to make transportation *safer and more efficient*, supporting a wide range of real-world applications (see **Tables 1–2** [4–8]).

By enabling real-time communication between vehicles, infrastructure, and vulnerable road users (VRUs), V2X can prevent or decrease the impact of accidents, improve traffic flow, reduce congestion, and optimize energy use. Beyond these immediate benefits, it also contributes to broader goals such as environmental sustainability, automation, and smart city integration (see **Table 3**).

Achieving these outcomes requires communication networks that meet stricter demands than conventional wireless systems. V2X must, therefore, integrate the following capabilities:

- *Low latency*: Many safety applications only make sense if information arrives almost instantly. For example, a forward collision warning becomes useless if it reaches the driver after the crash has occurred. This means that end-to-end communication delays must be kept very low.

- *High reliability*: Messages must be delivered with a very high success probability. Missing a video frame in a streaming service is tolerable; missing a message about a braking vehicle ahead may not be. Hence, V2X systems must guarantee the delivery of critical messages even under difficult channel conditions.

Application	Connectivity impact
Intersection collision avoidance	V2V shares real-time position, speed, and trajectory; V2I provides Signal Phase and Timing (SPaT) data.
Forward collision warning	V2V broadcasts sudden braking; V2N warns of distant hazards like pile-ups.
Pedestrian/Cyclist safety (V2P)	V2P devices share locations via smartphones; V2I relays crosswalk or school zone data.
Emergency vehicle preemption	V2V alerts drivers to yield; V2I prioritizes signals for ambulances or fire trucks.
Hazardous road condition alerts	V2V/V2I/V2N warn of ice, debris, or roadwork.
Cooperative adaptive cruise control (CACC)	V2V coordinates speed and spacing for safe platooning; V2N optimizes routes.
Wrong-way driver detection	V2V/V2I alerts oncoming traffic of wrong-way vehicles.
Work zone safety	V2I broadcasts lane changes; V2N updates navigation.
Cooperative maneuvers	V2V enables joint evasive actions, like lane changes or sudden stops, in emergencies.

Table 1.
V2X safety applications.

Application	Connectivity impact
Traffic signal optimization	V2I provides SPaT data; V2N adjusts signal timings dynamically for green waves.
CACC and platooning	V2V synchronizes vehicle formations; V2N optimizes routes for fuel efficiency.
Dynamic route optimization	V2N/V2I provides real-time traffic and congestion updates for rerouting.
Eco-driving assistance	V2I/V2V recommends optimal speeds for smoother driving.
Emergency vehicle preemption	V2I prioritizes signals; V2V clears paths for emergency vehicles.
Work zone management	V2I/V2N guides vehicles around construction or congestion.
Cooperative parking	V2V/V2I share parking spot data and coordinate curbside access in urban areas.
Bus lane sharing	V2I allows authorized vehicles temporary access to dedicated lanes.

Table 2.
V2X transportation efficiency applications.

- *Security vs. privacy balance*. Because vehicles act on received information, it is essential to ensure that these messages are authentic and have not been corrupted. At the same time, the continuous broadcast of position and identity data raises privacy concerns: vehicles must remain trustworthy to others while still protecting the long-term anonymity of their users.

All of it has to function under various dynamic conditions. V2X networks must operate reliably despite extreme dynamics: fast-changing neighbors, varying propagation environments, and irregular coverage. Unlike in stationary networks, vehicular connectivity must adapt to 1) high mobility and 2) heterogeneous conditions – without interruptions or delays.

Application	Connectivity impact
Environmental sustainability	V2I/V2N optimizes speeds and routes; V2G integrates with smart grids for efficient charging.
Convenience and infotainment	V2N streams high-definition content and enables over-the-air vehicle updates.
Autonomous driving support	V2X shares sensor data for tele-operated control or automated valet parking.
Societal and community enhancements	V2N automates accident reports and shares vital signs in ambulances.
Smart city integration	V2I connects with urban systems for better transit and planning.

Table 3.
V2X other applications of interest.

While these requirements are universal, their relative importance and the dominant technical challenges differ depending on the environment. The following examples highlight three representative scenarios – highways, rural roads, and urban centers (see **Figure 1**) – each posing unique demands on V2X communication.

- *Highways* (see **Figure 1a**) are characterized by very high mobility and relatively predictable road geometry. Communication links must manage large Doppler shifts, frequent topology changes, and long distances that increase path loss. At the same time, many cooperative applications are especially relevant on highways. *Platooning* requires, e.g. vehicles to maintain small inter-vehicle gaps while coordinating speed and braking in real time (strict latency and reliability constraints). Similarly, *overtaking maneuvers* can be assisted by V2X to exchange trajectory and lane-change intentions, enabling safer and more efficient execution.

- *Rural roads* (**Figure 1b**) are characterized by sparse infrastructure, longer inter-vehicle distances, and fewer multipath reflections, although terrain features such as forests can create additional signal challenges. Vehicles often travel at moderate to high speeds, but traffic density is low. In such environments, V2X can enhance safety by providing timely information about unexpected obstacles. For example, a vehicle can be warned of an *animal crossing* or alerted to a *slow-moving tractor* ahead, allowing sufficient time to slow down or maneuver safely. Reliable long-range communication is critical in these scenarios, especially with limited or unstable network coverage.



(a) Highway (b) Rural road (c) City center

Figure 1.
Traffic scenarios.

- *City environments* are characterized by dense traffic (**Figure 1c**), frequent intersections, and a high presence of VRUs. Communication links are affected by dense multipath propagation and frequent line of sight (LOS) blockages by, e.g., buildings. Speeds are generally lower than on highways, but the high density and complex interactions make timely information critical. V2X can improve safety and efficiency by supporting applications such as *collision avoidance at intersections* and *VRU warnings*.

Achieving safety and efficiency objectives requires meeting strict latency, reliability, and security/privacy requirements across various environments. With this in mind, in the next section, we continue with the fundamentals of V2X channel modeling, including propagation phenomena and communication mechanisms, as the foundation for designing reliable V2X solutions.

2.2 Communication models and theoretical foundations

Designing reliable V2X systems requires a clear understanding of how the wireless medium affects transmitted signals under diverse mobility and propagation conditions. Since direct experiments in all possible traffic scenarios are not feasible, channel models are used as mathematical abstractions of the propagation environment. These models capture how transmitted waveforms are modified by path loss, shadowing, multipath, and Doppler effects, providing grounds for analysis and simulation.

In vehicular settings, the radio channel is highly dynamic and non-stationary: links may alternate rapidly between LOS and non-line of sight (NLOS) states, delay spreads vary depending on surrounding geometry, and Doppler shifts arise from high relative speeds. To represent these effects, most V2X models combine predictable, distance-based attenuation with stochastic components that describe random fluctuations of the received power and phase. **Figure 2** conceptually illustrates three key components of the received signal power as a function of distance: the overall *path loss*, the slower large-scale variations (*shadowing*), and the fast local fluctuations (small-scale *fading*).

The received power decays with distance due to path loss, which follows a predictable logarithmic trend in the average sense. Superimposed on this trend are slower fluctuations known as large-scale fading or shadowing, caused by obstacles such as buildings, trucks, and trees that might block or reflect the signal. These variations occur over $10 - 100$ m and are spatially correlated – nearby vehicles tend to experience similar shadowing conditions.

At smaller spatial and temporal scales, multipath propagation gives rise to rapid oscillations of the received amplitude (small-scale fading). It occurs when multiple reflected, scattered, and diffracted signal components combine constructively and destructively as the receiver moves by distances comparable to the carrier wavelength. Depending on whether a strong LOS path exists, the fading statistics vary: they are typically Rayleigh-like in obstructed non-LOS conditions, and Rician or Nakagami-like when a dominant LOS component is present. Typical fading parameters such as the Rician K-factor or Nakagami-m parameter differ across highway, urban, and intersection scenarios (see **Table 4** [9, 10]).

The channel is also time-varying due to the relative motion between transmitters, receivers, and scatterers. This motion causes Doppler shifts in the

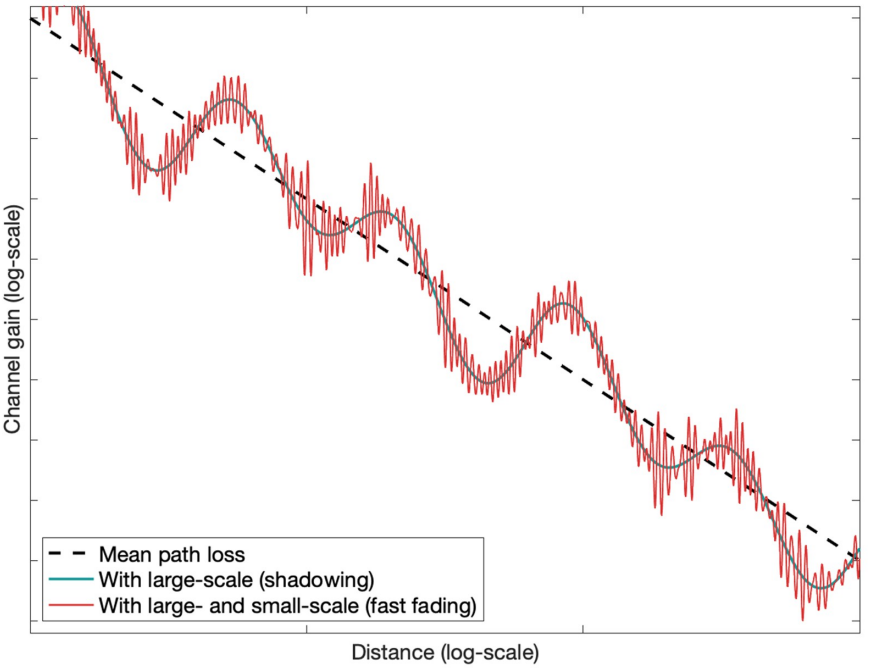


Figure 2.
Representation of path loss, large- and small-scale fading.

Scenario	Delay spread	Small-scale model	Typical parameters
Highway LOS	30–50 ns	Rician	$K \approx 5$–15 dB
Highway NLOS	80–150 ns	Rayleigh/Nakagami	$m \approx 1$–2
Urban LOS	100–200 ns	Rician	$K \approx 2$–8 dB
Urban NLOS	200–300 ns	Rayleigh/Nakagami	$m \approx 1$
Intersection (dense)	200–400 ns	Nakagami	$m \approx 0.5$–1.5
Tunnel/Bridge	20–50 ns	Rician	$K > 20$ dB

Table 4.
Typical V2X fading parameters.

received signal frequency. E.g. two vehicles moving in opposite directions at highway speeds (around 100 km/h) at 5.9 GHz experience frequency shifts of roughly 0.5 kHz. Such shifts shorten the channel coherence time to about 1ms, meaning that channel conditions can change significantly even within the duration of a single packet transmission. Doppler must be taken into account in channel models for realistic performance evaluation across highway, rural, and urban scenarios.

Overall, these combined phenomena – path loss, shadowing, multipath fading, and Doppler dynamics – define the structure of V2X channel models. The specific balance between physical accuracy and analytical simplicity differs across standardized and research models, which are compared below.

The models in **Table 5** illustrate how different approaches combine the fundamental channel components discussed earlier. Each has its own scope and limitations:

- **3GPP TR 38.901** [9]: Widely used for 5G and V2X extensions, it provides comprehensive modeling of path loss, shadowing, clustered multipath, fading, and geometry-based Doppler. Its main advantage is standardization and versatility across frequencies up to 100 GHz. However, its complexity and parameterization overhead make it heavy for large-scale system simulations.

- **WINNER II/WINNER +** [11]: Historically important as a precursor to 3GPP models, with dual-slope path loss and clustered multipath. It is computationally simpler but less accurate at high frequencies and under dense urban V2X conditions.

- **COST 2100** [12]: Introduces a geometry-based stochastic framework with visibility regions and clusters that capture environment-dependent dynamics. While physically insightful, it is less widely used today and lacks complete parameter sets for vehicular deployments above 6 GHz.

- **IEEE 802.11p models** [13]: Tailored to DSRC at 5.9 GHz, these use simplified tapped-delay line structures (vehicular A/B) with Rayleigh fading. They are lightweight and convenient for fast simulations but fail to capture strong Doppler dynamics or large delay spreads found in dense intersections and urban canyons.

- **ITU-R Vehicular A/B** [14]: Similar in spirit to IEEE 802.11p, these models are useful as baseline references but are too coarse for advanced V2X evaluations, as they neglect non-stationarity and complex scattering.

- **Ray tracing** [15]: Offers the highest fidelity by deterministically computing multipath components from environment maps. This yields site-specific

Model	Type	Frequency range	Mobility
3GPP TR 38.901	Geometry-based stochastic	0.5–100 GHz	Up to 500 km/h
Widely used for 5G; includes V2X extensions			
WINNER II/WINNER +	Stochastic (GBS)	2–6 GHz	Up to 350 km/h
Precursor of 3GPP; dual-slope PL, cluster-based PDP			
COST 2100/	Geometry-based stochastic	2–6 GHz	Up to 300 km/h
Early geometry-based channel model			
IEEE 802.11p (TGn/NGV)	Stochastic	5.9 GHz	Up to 200 km/h
Simple PDPs; tailored for DSRC			
ITU-R (Vehicular A/B)	Stochastic (tapped delay line)	0.5–6 GHz	Up to 250 km/h
Standard reference models (V2V, V2I)			
Ray-tracing	Deterministic	Any	Any
Requires full environment map; high accuracy, low generality			

Table 5.
Overview of vehicular channel models.

accuracy, useful for validation and safety-critical studies. The drawback is poor scalability: ray tracing requires detailed knowledge of the environment and is computationally expensive, limiting its applicability to small-scale scenarios.

In practice, the choice of a V2X channel model depends on the evaluation purpose. For theoretical insight and tractable performance analysis, simple statistical models (Rayleigh, Rician, Nakagami) suffice. For system-level simulation and standardization, geometry-based stochastic models (3GPP, WINNER) offer the right balance of realism and generality. For site-specific validation, deterministic ray tracing is preferred. This reflects the trade-off between accuracy and complexity: no single model fits all purposes, and selecting an appropriate channel model is itself a crucial design choice in V2X research.

2.3 Remarks about multi-band: 5.9 GHz vs. 60 GHz

Millimeter-wave (mmWave) frequencies (e.g. 60GHz) allow for high-capacity links [16]. However, those frequencies make differences in channel model characteristics – due to shorter wavelength ($\lambda \approx 5$ mm) path loss becomes steeper and shadowing harsher. Scattering even from e.g. raindrops, foliage is high and therefore multipath gets sparser with shorter delay spread. Long-range communication becomes impossible due to weather effects (oxygen has its absorption peak at those frequencies and snow and rain add to signal attenuation). However, it exhibits potential for V2X bumper-to-bumper applications (e.g., platooning, cooperative perception), and as such, it has been added to new specifications for vehicular networks (e.g., IEEE 802.11bd [17] operates in both 5.9 and 60 GHz). **Table 6** summarizes the characteristics of both bands and highlights the differences between them in terms of physical layer phenomena.

2.4 Performance metrics

The performance of V2X services can be assessed on several levels and from different viewpoints [5, 9]. First, the general metrics from wireless communication systems are applicable, but their numerical targets are influenced by V2X context. Path loss and shadowing determine the received signal strength, which, in turn, influences link reliability, achievable data rate, and coverage. Multipath propagation and fast fading cause rapid amplitude and phase variations, leading to increased packet loss, jitter, and higher error rates. Vehicle mobility adds another layer of complexity: Doppler shifts shorten the channel coherence time, making channel estimation more difficult and potentially increasing latency. In dense urban or highway scenarios, the situation is further aggravated by interference from neighboring transmissions, which lowers the signal-to-interference-plus-noise ratio (SINR) and constrains modulation, coding efficiency, and throughput, as explored in Section 2.5.

An overview of these metrics and their typical V2X-relevant targets is presented in **Table 7**. Understanding the relationship between channel characteristics and performance metrics is essential for evaluating whether a given protocol, message frequency, or transmission power can meet safety-critical requirements under different traffic scenarios.

Channel component	**5.9 GHz (DSRC/C–V2X)**	**60 GHz (mmWave V2X)**
Path loss	Moderate free-space PL; longer communication ranges ($10^2 - 10^3$ m with RSUs).	Extra ~20 dB free-space PL; practical range limited to $10 - 10^2$ m; requires directional antennas.
Shadowing/ Penetration	Vehicles, buildings, and foliage attenuate, but partial penetration is possible (walls, cars).	Strong attenuation through obstacles; weaker NLOS links; blockage by vehicles or pedestrians.
Multipath	High scattering; suitable for Rayleigh/Rician fading models.	Sparse multipath; dominated by LOS and a few strong reflections; cluster-based models needed.
Delay spread	Larger ($10^{-7} - 10^{-4}$ s) due to scattering.	Smaller on average ($10^{-8} - 10^{-7}$ s) because of sparse multipath.
Small-scale fading	Rayleigh or Rician	Fewer components, i.e. higher Rician K-factor or two-ray-like fading.
Doppler shift	≈ 1 kHz per 100 km/h	≈ 10 kHz per 100 km/h; coherence time ~ 0.1 ms.
Atmospheric/ Weather effects	Negligible under most conditions.	Strong oxygen absorption (15 dB/km at 60 GHz); rain and humidity add extra attenuation.
Interference	Wide-area reuse, interference from many terminals is important.	Highly directional beams reduce interference, but alignment and beam-tracking are critical.

Table 6.
Comparison of channel characteristics between 5.9 GHz and 60 GHz.

While the general metrics reflect fundamental communication performance, vehicular applications set additional requirements tied to the application layer: what matters is not just whether a packet was delivered, but whether it was delivered in time to maintain cooperative awareness or to trigger a safety maneuver. In this sense, fading or interference may reduce reliability and SINR (general metrics), but their impact is felt most critically through shortened awareness ranges, reduced update rates, or outdated situational knowledge (captured by the age of information).

Table 8 lists the most common indicators defined in ETSI and 3GPP standards. Their relationship to both the underlying channel phenomena and the general metrics is illustrated in **Figure 3**, where both sets of indicators converge to determine whether service-level requirements, such as safety, efficiency, and automation, can ultimately be satisfied.

2.5 Media phenomena and their effect on V2X performance

As shown in this section, there are specific metrics for V2X service provision that define how large of an area communications shall reliably cover within a short deadline. Standardization organisms such as SAE International and ETSI rely on the expertise of researchers from the industry and academia, and take into account their analysis of the possibilities for the radio medium to provide reliability and low latency. Then, compliant implementations must meet the requirements set by technical specifications and norms. However, once deployed in the real world, V2X services must face unexpected situations. For example, at the application

Metric	Definition	V2X context/acceptable values
General metrics		
Throughput	Amount of successfully delivered data per unit time (bps, Mbps).	Application-dependent; safety beacons are small (≈ 300–800 bytes), throughput is less critical than reliability.
Latency	Time taken for a packet to travel from source to destination.	≤ 100 ms for general safety apps; ≤ 20 ms for collision avoidance (ETSI/3GPP URLLC targets).
Jitter	Variation in packet delay over time.	Keep minimal (< 10 ms) for control loops (e.g., CACC).
Reliability	Probability a message is delivered correctly.	Often expressed as "message success rate within deadline"; ≥ 99% within required latency for safety-critical apps.
Link quality metrics		
Packet loss rate (PLR)	Fraction of packets lost during transmission.	PLR < 10% at 300 m for ETSI ITS-G5 CAM/DENM.
Packet delivery ratio (PDR)	Fraction of successfully received packets over total sent.	PDR ≥ 90% at 300 m for cooperative awareness messages.
Bit error rate (BER)	Ratio of incorrect bits to total transmitted bits.	Target BER $\approx 10^{-5}$ for safety messages in good channel conditions.
Signal-to-interference-plus-noise ratio (SINR)	Ratio of signal power to interference and noise power (dB).	> 20 dB often needed for high-modulation modes; lower thresholds for robust MCS.
Channel capacity	Maximum achievable throughput under given channel conditions.	Time-varying due to mobility; relevant for dense platooning or high-rate sensor sharing.
Link stability	Average time a link remains usable.	Seconds for V2V on highways; minutes for V2I in the city with RSUs.
Handover delay	Time to switch an active connection to a new cell/RSU.	< 50 ms desirable for seamless safety message delivery.
Doppler spread	Spectral broadening due to relative motion.	At 5.9 GHz:≈ 1 kHz per 100 km/h relative speed.
Channel coherence time	Interval over which the channel remains approximately constant.	For 100 km/h at 5.9 GHz: ≈ 1 ms.
Interference level	Power from undesired transmissions relative to noise.	Keep low to maintain PDR; critical in mixed DSRC/C–V2X environments.

Table 7.
Communication channel metrics for V2X networks.

level, operating in places where jaywalking is the norm, VRU alerts can potentially create a traffic shockwave or *phantom jams*. For the access layer, vehicles encounter the different phenomena that we describe in Section 2.2 in scenarios that change constantly.

Figure 4 shows the phenomena affecting two different scenarios. In both scenarios, nodes in yellow wish to communicate, and there is a red node that wrongly senses the medium as idle and interferes (e.g., hidden and exposed node

Metric	Definition	Typical V2X targets/ standards
Packet delivery ratio (PDR)	Fraction of successfully received packets over total sent, usually measured over a defined distance.	≥ 90% at 300 m for CAM/ DENM (ETSI ITS-G5).
Awareness range	Maximum distance at which the required PDR is met.	≥ 300 m for cooperative awareness; longer on highways.
Update rate	Frequency of periodic awareness messages.	ETSI CAM: typically 10 Hz; adaptive 1–10 Hz.
Channel busy ratio (CBR)	Fraction of time the channel is sensed as busy (above CCA threshold).	< 60% to prevent congestion (ETSI ITS-G5).
Age of information (AoI)	Time since last update about a given entity was received.	< 1 s for awareness; lower for high-speed scenarios.
Safety deadline	Maximum allowable end-to-end latency for a safety message to remain effective.	≤ 100 ms for general safety; ≤ 20 ms for collision warnings.
Cooperative awareness rate (CAR)	Proportion of relevant neighbors from which timely updates are received within the awareness window.	≥ 90% within defined awareness range.

Table 8.
V2X-specific performance indicators.

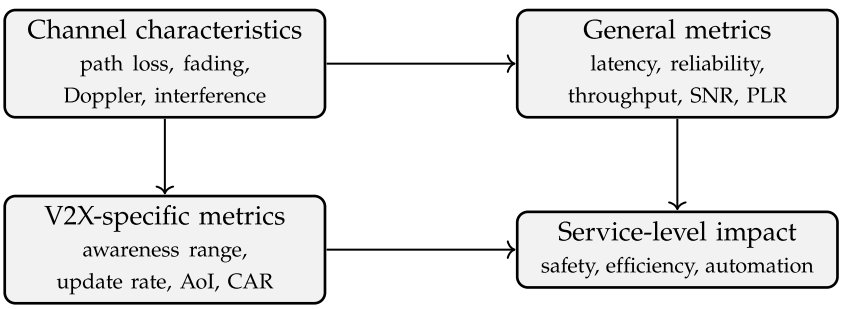
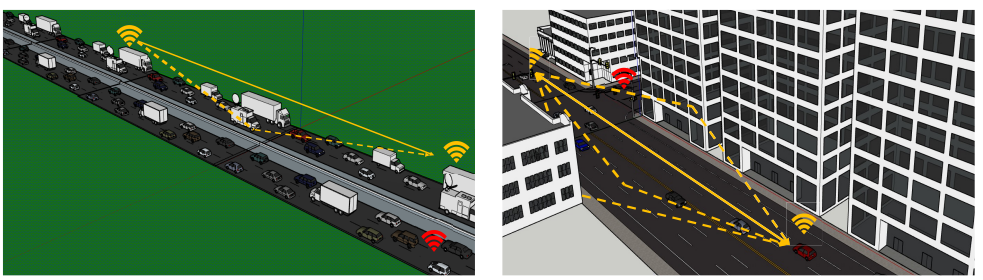


Figure 3.
Channel characteristics affecting the performance of V2X channel.



(a) Highway (b) Urban

Figure 4.
Propagation phenomena.

phenomena). The solid yellow lines show the direct signal – which is affected by attenuation and Doppler – and the dotted lines are reflections. Note that there are more reflections in the urban scenario (urban canyon effect), affecting channel convergence. There are other effects in the urban scenario, such as the fact that signals will not propagate around corners, causing a phenomenon where messages that are relevant to vehicles approaching an intersection are not delivered reliably. Furthermore, urban canyons and highway tunnels can create an artificial scenario of medium congestion by decreasing the SINR and making nodes sense an idle channel as busy – i.e., triggering collision avoidance and decentralized congestion control (DCC) at the access layer.

Thus, media phenomena affect performance for Access layer protocols and influence what can be done by upper layers and what can be expected from service provision. For example, while IEEE 802.11p is technically capable of handling changes in data rate, and the ETSI ITS standard considers data-rate control as one form of DCC, implementers have decided on a single data rate (6 Mbps), and the specification only refers to transmission rate control (i.e., how frequently messages can be sent) as its only technique for DCC [18]. We explore more of the influence between theory, research, validation, and deployment on current and upcoming vehicular networks in the following sections.

3. Current technologies

3.1 Evolution of vehicular Ad hoc networks (VANETs)

The spectrum allocation for ITS communications has been one of the major issues for wide deployments. In 1999, the United States' Federal Communications Commission (FCC) allocated 75 MHz in the 5.9 GHz band (5.850–5.925 GHz) for its national ITS program [19]. At that moment, the decision specified that the spectrum would be used for a variety of DSRC applications. Other countries followed suit, with the European Commission allocating 30 MHz in the 5.9 GHz band in 2008 [20]. Furthermore, Canada, Mexico, Australia, Korea, Singapore, China, and Japan have also allocated spectrum in the 5.9 GHz band, nevertheless, with different bandwidths – e.g., Canada and Mexico reserved 75 MHz, while China only allocated 20 MHz [21].

Two regions spearheaded the development of ITS – and more specifically, V2X services – the United States and the European Union. SAE International in the United States and ETSI released a batch of standards for ITS services by 2013. These standards came after a series of tests and adaptations to proposals by stakeholders and converged into a similar set of services for each region. For example, the SAE Basic Safety service, which relies on the Basic Safety Message (BSM), covers the same use cases as the European Cooperative Awareness Message (CAM) – for beaconing – and Decentralized Environmental Notification Message (DENM) – which alerts of risks, e.g., emergency braking, roadworks, etc. Both organizations also defined one access technology: IEEE 802.11p, which is an amendment to the 802.11 WiFi standard to provide wireless access in vehicular environments (WAVE). For Europe, it was adapted into ETSI ITS-G5 [22]. Thus, both regions relied on DSRC for the access layer, although there were provisions allowing other access technologies.

By 2018, while it was clear which spectrum band was going to be used to fulfill ITS use cases, specifically in V2X, the use of DSRC communications was not the only option anymore. While the use of cellular technologies (3G, 4G) was considered for long-range communications, the appearance of long term evolution (LTE) and 5G, with their capability for device-to-device (D2D) communications (i.e., *sidelink* – with devices communicating without relying on a base station), opened the door for C–V2X [8], also known as 5G New Radio (5G–NR). As of Release 16, 5G–NR brings the promise of having two possible modes: Mode 1 (managed by a base station) and Mode 2 (which does not require management from a base station). In Section 3.3, we will summarize the works in the literature assessing the trade-offs between DSRC and C–V2X technologies.

It is not only C–V2X that is in constant evolution – with sidelink being present since LTE Release 14 [20]. DSRC, represented by WiFi-based technologies, has also evolved from IEEE 802.11p to IEEE 802.11bd [17], known in ETSI as *Profile 2* [23]. Among the updates that are specific to either C–V2X or DSRC, one addition in common is the use of the 60 GHz band for ISAC [24] – i.e., using the communications spectrum to perform radar-like and other types of sensing, positioning, and localization. **Table 9** summarizes the characteristics of currently standardized VANET technologies. Note that the data for 802.11p comes from actual deployments and an extensive body of work from research, while those for 802.11bd are a product of what the technologies it is based on can achieve [25], and those for 5G NR also include the managed mode [26], i.e., they show the expected best-case scenarios.

3.2 Deployments, pilots, and testing scenarios

3.2.1 Deployments

Since the first release of technical specifications for ITS services, consortia formed by international bodies, vehicle manufacturers, network operators, and

Feature	**802.11p**	**802.11bd**	**5G NR[1]**
Frequency bands	5.9 GHz	{5.9, 60} GHz	5.9 GHz, licensed
System bandwidth	10 MHz	{10, 20} MHz	Up to 100 MHz
Data subcarriers	48	48 and 52	OFDM-based
MIMO	N/A	2 × 2 MIMO	Supported
Data rates	3–27 Mbps[2]	Up to 39 Mbps	Multi-Gbps
Channel BW	10 MHz	10 or 20 MHz	5–100 MHz
Relative vehicle speed	252 km/h	500 km/h	> 500 km/h
mmWave (60 GHz)	Not supported	Supported	Supported
Localization	N/A	Supported	cm-level positioning
Latency	~100 ms	< 10 ms	< 5 ms
Reliability	Moderate	High	99.999%
Backward compatibility	–	With 802.11p	Dual-radio with LTE-V2X

[1] *Considering both managed and unmanaged modes.*
[2] *Only 6 Mbps is typically used in 802.11p deployments.*

Table 9.
Specifications for 802.11p, 802.11bd, and 5G NR.

national and regional transport authorities have led efforts to deploy ITSs on public roads. **Table 10** summarizes a selection of mature deployments from the United States [27], Japan [28], the C-Roads consortium in Europe [29], Germany [30], Austria [31], and Taiwan [32].

The focus of the European deployments has been on 1) cross-national corridors like C-Roads (with 18 countries as core members), and 2) inter-operability between access technologies (DSRC and C–V2X), i.e., not deciding itself on an access technology, which has created a stalemate. However, Austria's Autobahn and highway financing stock corporation (ASFINAG) set an example by deciding on DSRC as its only platform and launched the first full deployment of ITS on all Austrian highways [31], which can now communicate with compliant vehicles (such as Volkswagen's ID series) to deliver beacon and emergency messages (i.e., ETSI CAM and DENMs). This goes beyond pilots in which ASFINAG is also involved, which are discussed in Section 3.2.2.

3.2.2 Pilots

Table 11 shows the progress of pilot tests for C-ITS in Europe [33] and the United States [34]. There are some examples of pilots that evolved into deployments, such as the ones from the United States, Austria, and Germany in **Table 10,** which is also reported as a completed pilot in [33]. Furthermore, this also includes pilots that are not strictly V2X or based on VANETs, such as Sweden's Nordic Way, which relies solely on conventional cellular communications with a centralized cloud-based interchange service.

One takeaway when comparing **Tables 10** and **11** is that the commitment from stakeholders is crucial for a pilot to become a full deployment. Take ASFINAG's and the UK's corridor as an example: in Austria, any ETSI ITS-compliant vehicle (such as VW's ID series) can interact with the road-side units (RSUs) that are maintained by ASFINAG, while in the UK, the on-board units (OBUs) were returned to the supplier. These trends, where infrastructure and nodes are removed

Region	Deployment status	Deployment timeline	Network technology
USA	Wyoming Department of Transportation; no federal mandate	Since ~ 2016	802.11p (DSRC), C–V2X (some trials)
Japan	Active deployment (ETC2.0, SIP-adus); large-scale testing	Since ~ 2015	700 MHz ITS, DSRC (802.11p), mmWave, cellular
C-Roads (EU)	Coordinated deployment across 18 + countries	First services since 2019	Hybrid: ITS-G5 (802.11p) + 3G/4G/5G cellular
Germany (Hessen)	Trial completed; rollout in progress across federal states	Since mid-2019	ETSI ITS-G5 (802.11p), cellular integration
Austria (ASFINAG)	Large-scale deployment on motorways; 525 RSUs planned	Since 2020	ITS-G5/802.11p (DSRC)
Taiwan	Field trials in multiple cities; expanding	Since 2015	IEEE 802.11p/DSRC, ETSI ITS-G5, hybrid V2X

Table 10.
Status of C-ITS deployment and communication technologies used across selected regions.

Region	Deployment status	Deployment timeline	Network technology
Belgium (Flanders)	Pilot completed; virtual infrastructure tested with 630 users	2016–2021	Cellular (3G/4 G), HERE Location Cloud
Belgium (Wallonia)	Pilot completed; six RSUs installed on A602; 427 km covered via cellular	2017–2021	ITS-G5 (802.11p), Cellular (4 G)
Czech Republic	National rollout in progress; 379 RSUs and 1930 OBUs installed	Since 2021	Hybrid: ITS-G5 + LTE
France (InDiD)	Multi-city deployment; 588 RSUs and 43 OBUs installed	Since 2017	ITS-G5, Cellular, Hybrid
Ireland	Pilot on M50 and M1; 74 RSUs and 62 OBUs installed	Since 2023	Hybrid: ITS-G5 + Cellular
Italy (C-Roads 1–3)	National and urban deployments; 206 RSUs and 24 OBUs installed	2017–2023	Hybrid: ITS-G5 + Cellular
Netherlands	Pilot completed; 19 RSUs installed for testing	2016–2019	ITS-G5, Cellular
Portugal	National and urban deployments; 132 RSUs installed	Since 2017	Hybrid: ITS-G5 + Cellular
Slovenia	Pilot in progress; 12 RSUs installed, 50 more planned	Since 2020	ITS-G5, Cellular, Hybrid
Spain	5 regional pilots; 298 RSUs installed	Until 2021	Hybrid: ITS-G5 + Cellular
Sweden (NordicWay 3)	Pilot completed; OBUs used, no RSUs installed	2019–2023	Cellular, Hybrid (PoC)
UK (A2/M2 Corridor)	Pilot completed; 33 RSUs installed, OBUs returned	Until 2020	ITS-G5, Cellular
USA (NYC)	Urban safety-focused pilot; 3,000 fleet vehicles, 12 MTA buses, pedestrian alert systems	2015–2022	DSRC (802.11p), pedestrian mobile apps
USA (Wyoming)	Freight corridor pilot on I-80; 325 vehicles equipped including trucks and snowplows	2015–2022	DSRC (initial), C–V2X (Phase 4)
USA (Tampa)	Downtown congestion and safety pilot; 1,000 cars, 7 buses, 8 trolleys; wrong-way alerts	2015–2022	DSRC (802.11p)

Table 11.
Status of C-ITS pilots across selected regions.

after the completion of the project, are present in the finalized pilots that did not progress into the deployment stage.

3.2.3 Test scenarios and plug-in tests

The pipeline from ideation to wide implementation goes through a research and development (R&D) phase. Researchers in academia and industry test protocols in the different layers of the VANET stack, first using simulation tools (e.g., veins [35], artery [36], 5G-LENA [37]), and then moving to conditions that are more realistic, such as test tracks operated by vehicle manufacturers [38, 39] and research institutes [40–42]. Up to this point in the pipeline, developments are mostly compartmentalized, and it is yet to be proven that new ideas will comply with standards and can operate with proposals and devices from others.

This is where plug-in tests (or plugtests) come into play. These are events organized by standardization organizations where vendors, developers, and stakeholders (e.g., vehicle manufacturers, mobility providers, logistics companies) validate compliance and interoperability, as well as identify and resolve implementation issues. **Table 12** summarizes the latest plugtest for ETSI-defined DSRC [43] and the first four plugtests for ETSI-sanctioned C–V2X [44–47].

3.3 Current issues with vanets

One takeaway from Sects. 3.1 and 3.2 is that there are two strong competitors to become the dominant access technology for C-ITSs. DSRC and C–V2X – represented by 802.11p and 5G NR, respectively – are not mutually compatible, and the best-case scenario expected by stakeholders is that they coexist and share the 5.9 GHz spectrum [20]. Furthermore, there is an effort from network card manufacturers to push for their access technology. While DSRC was *first to market*, C–V2X has lobbied even for policy makers to declare them as the official option, e.g., in the United States [48]. In Europe, however, there is no official consensus on which access technology shall prevail, although we have shown examples of large-scale deployments where national authorities and stakeholders have chosen DSRC as the most mature and cost-efficient technology.

This leads us to the first main issue of current VANETs – heterogeneity and interoperability. If two last-generation, fully-equipped vehicles interact on the road, it is necessary for both to have the same configuration at the access layer – i.e., having the same network access technology (DSRC or C–V2X), being tuned to the same channel, and using the same data rate [49]. Furthermore, at upper layers, vehicles might use different releases of protocols. Our work in [50] tests – among other heterogeneous traffic phenomena – the effects on efficiency of having vehicles using two different releases of an ETSI network layer protocol. While this is indeed a current problem (ETSI ITS releases 1 and 2 are currently deployed), the

Event	Location and date	Technology	Main takeaways
6th ITS CMS Plugtests	Sophia Antipolis, France; 25 Feb – 1 Mar 2019	ETSI ITS-G5	Validated Release 1 security standards; PKI and ITS-S interoperability; ECTL parsing tested; Brainpool curves not widely supported.
1st ETSI C–V2X Plugtests	Malaga, Spain; 2–6 Dec 2019	C–V2X (LTE-V2X PC5)	Validated Release 14 interoperability; 95% success rate; field testing of RWW, LCRW, and ICRW.
2nd ETSI C–V2X Plugtests	Remote; 20–31 Jul 2020	C–V2X (LTE-V2X PC5)	Remote VPN-based testing; 94% success rate; focused on ITS security and PKI interoperability.
3rd ETSI C–V2X Plugtests	Klettwitz, Germany; 28 Mar – 1 Apr 2022	C–V2X (LTE-V2X PC5)	93% success rate; tested advanced use cases like time-to-green and traffic jam warning; GN MID and L2 ID issues noted.
4th ETSI C–V2X Plugtests	Malaga, Spain; 10–13 Sep 2024	C–V2X (ETSI Release 2)	94% success rate; focused on CPM and VRU features; UPER encoding and CAM rate mismatch with PC5 policy identified.

Table 12.
Summary of ETSI plugtests events: location, date, technology, and main takeaways.

constant addition of services and the evolution of protocols and access technologies make it a future problem, which we explore in Section 4.1.

The second issue is more related to the readiness level for each technology. Let us refer back to **Table 9**, where the column for 802.11p has a note clarifying that – despite the technology's supported data rates – only the 6 Mbps configuration is typically used. This came from the profiles established by the consortia in charge of deployments, like the Car-2-Car consortium [51]. Thus, it was after thorough validation that a stable profile was created and is being used. For 802.11bd and C–V2X, more validation is required, but works in the literature have assessed problems that hinder the promise of high reliability and low latency for C–V2X, namely the difficulties of resource allocation in the unmanaged mode of C–V2X [52], the problems with mode switching [53], and the effect of these problems in safety applications – e.g., collisions that affect reliability and sub-optimal resource allocation that affects latency [54, 55].

4. Future perspectives and gaps

In this section, we explore the open questions and future scenarios in connected mobility. Some stem from current issues, however, some of them are set solely in the future. We start with heterogeneity in fleet capabilities, problems with the limitations of the radio medium and how it can accommodate new and stringent demands, and we close with a summary of the gaps and challenges we identify.

4.1 Connected fleet heterogeneity

We have discussed the problem of having two different access technologies using the medium and how it makes two highly-equipped vehicles *deaf* to each other – i.e., a DSRC-equipped vehicle cannot receive messages sent using C–V2X. Our work in [56] explores the problem of heterogeneity brought up by 1) the uptake rate for CCAM, and 2) the average lifespan of a vehicle. This creates a problem where CCAM-equipped vehicles of different generations and even access technologies must interact with each other and with conventional road users (i.e., non-equipped vehicles or VRUs).

The analysis presented in [50, 56] examines the effect of heterogeneity in network protocols, as well as the interaction between conventional road users and CCAM-equipped vehicles. The premise stems from the average age of the vehicles on the road, which implies that a vehicle produced now will very likely still be on the road in 15 years [57, 58]. Currently, only a few hundred thousand connected vehicles are on the road [59], which means that there will definitely be non-equipped vehicles in the fleet for the next couple of decades.

The work in [56] explores the risks of connected vehicles being impaired by listening to each other and relates those risks to the ones present for conventional drivers. Even though CCAM-equipped vehicles should not be affected by human factors, such as sickness or age itself, the fact remains that the age of a vehicle might determine the technologies it can use. While over-the-air updates might help vehicles stay updated in software-based protocols, access layer technologies are more difficult to update. Thus, a vehicle equipped with a C-ITS access technology from the current generation (802.11p, LTE) might not be able to interoperate with the next

generation. 802.11bd is backward compatible with 802.11p, and this will most likely be the case for WiFi-based technologies, which is a design principle for the WiFi alliance and a requirement for WiFi certification [60]. However, this is not the case for cellular-based technologies in the 3GPP alliance [61].

For the interaction between CCAM-enabled vehicles and conventional drivers, the work in [50]. Taking away intra-CCAM variables, a homogeneous CCAM fleet shares the road with conventional drivers at penetration rates between 0 and 100%. Both ends of the spectrum show a level of stability (i.e., purely CCAM or conventional fleets are safer and more efficient). However, even a small level of heterogeneity brings instability. The work in [50] also explores that it is not only the ratio of conventional and CCAM vehicles that affects stability, but also the place they occupy, e.g., in a lane full of vehicles. Finally, it discusses heterogeneity in automated vehicles, since it is likely that this will be affected by brands and their target markets – i.e., more sport-oriented brands might be more aggressive on the road than family-oriented cars.

4.2 Spectrum limitations

Radio spectrum is a limited resource. For C-ITS, depending on the country or region, there are 20–75 MHz reserved for the exclusive use of C-ITS. Different technologies and applications lobby for extra spectrum, as seen in the transition from analog to digital television to liberate spectrum that is now used, e.g., for cellular communications. The 5.9 GHz spectrum is no exception, and even the government of the United States – a country with mature deployments – has released mandates to shave bands off the C-ITS spectrum and to declare it for use with C–V2X (i.e., phasing out DSRC) [62].

This fight for radio resources between technologies is not new, and it is also not the only competition for the medium. Even within a node running one access technology, multiple applications create messages to provide safety and efficiency services. In current deployments, beaconing and emergency messages compete for resources, with emergency messages having priority. However, new and sometimes more resource-heavy applications are being released, and this intra-node competition for the medium will become a bigger issue. In this section, we explore how vehicular communications deal with limitations in spectrum while trying to accommodate more applications and maintain the network metrics to ensure service provision.

4.2.1 New applications: Congestion control and resource

As explored in [63, 64], DCC is needed to maintain awareness levels, but it affects delay and influences the operation of other protocols or services. Even though they do not formally call it DCC in C–V2X, radio resource allocation creates similar issues in cellular communications, especially in unmanaged modes, where it is a direct comparison to DSRC (as explored in 3.3).

As uptake is expected to increase – creating scenarios with high densities of connected vehicles – it becomes harder to maintain performance. Methods such as DCC must be adapted to handle more complex traffic scenarios. For ETSI, this is a problem that is addressed proactively [65]. There are efforts to address how cross-layer resource management (i.e., DCC and cellular radio resource allocation) can be improved.

There are upcoming services, such as Collective Perception, which demand more radio resources than other services to exchange Collective Perception Messages (CPMs), which disseminate information derived from sensors to other vehicles – potentially sharing additional sets of "eyes" with connected vehicles that do not have, for example, cameras, radars, or LiDARs. The current generation of vehicular networks struggles to support CAM, DENM, and CPM traffic in both 802.11p [64] and C–V2X [54]. It is still an open question how more applications (e.g., Infrastructure-to-vehicle information (IVI), VRU protection, intention sharing, platooning, maneuver coordination) competing for resources inside a node will perform in a limited spectrum.

4.2.2 Multi-channel operation and multi-band operation

One alternative to open space for new applications is to use parallel communication channels. The use of multiple channels is supported by the ETSI ITS framework [49]. ETSI Release 1 messages (i.e., CAM and DENM) use one channel that is dedicated to safety services. Another six channels are available in the 5.9 GHz band, and it is expected that they are used by services with lower priority. However, a problem may arise if it is not well-defined how many channels a node should be able to access at a minimum and whether they will have several transceivers tuned to each channel or if one or more transceivers will hop through all of the channels. This will bring another type of heterogeneity, where some nodes will be able to access all channels at all times, and some others might need to hop through each channel, staying tuned for a fraction of the time – i.e., missing messages that are sent through the channels it is not tuned into at the moment.

Finally, another issue might arise with a new generation of vehicular communications (i.e., 6G and 802.11bd). The ability to use the 60 GHz band [17] will bring new opportunities for specialized services. Our work in [66] proposes the use of the 60 GHz band for bumper-to-bumper communications in platooning as an alternative to creating more load in the 5.9 GHz band. However, it also implies that only dual-band vehicles would be able to platoon with each other, leading to a scenario of segregation.

4.3 Gaps and challenges

We can identify heterogeneity caused by uptake as the main challenge for connected mobility. Interoperability between DSRC and C-V2X is a problem now, but it will only worsen with time – even if one access technology becomes the only standard. In the best case, we will have a majority of connected road users, however, they will be running different access technologies or different versions and implementations of the same one.

One gap is also heterogeneity in the connected fleet in behavioral terms. In the best case, all vehicles will share the same pool of information through the exchange of messages. However, how they react to this information is still an open question. In [56], we explore how conventional drivers have *styles* (e.g., patient, thrill-seeking), and how there is a risk that automated vehicles reflect this due to brand decisions. It is an open question left for specialists in behavior, networking, and game theory.

4.4 Proposals for mitigation

Heterogeneity is a multi-faceted problem with implications in connectivity and automation. Our work in [56] states, in summary, that standardization and consensus are the safest ways to deal with the interaction between the elements of a heterogeneous fleet. For example, avoiding automated cars having varying *driving styles* by standardizing vehicle-following algorithms and decision-making. This will create a scenario where, from a game theory perspective, every agent will follow the same strategy to respond to the same event – thus, avoiding the requirement for making a consensus. Another proposal is to control the Operational Design Domain (ODD) for CCAM. However, this is a compromise to CCAM in Vision Zero, which expects all vehicles, on all roads, and at all times, to coordinate their maneuvers [29].

For the case of accommodating new and more demanding services, while offloading services to a different band – as proposed in [16, 66] – might create scenarios of segregation, the standardization and consensus approach is also a possible solution. If we consider that many services apply only to certain types of road users, e.g., platooning has been mostly explored for heavy-duty vehicles, it might be convenient to make Platooning Awareness Messages (PAMs) exclusive to only a given type of vehicle and keep Platooning Control Messages (PCMs) in bumper-to-bumper channels in the ISAC band. This approach can also be applied to Maneuver Coordination Messages (MCMs) between passenger vehicles. However, this would require all passenger vehicles to have ISAC capabilities, which can be more challenging than in heavily-regulated fleets like commercial vehicles.

5. Conclusions

We have presented a view of the current state of connected mobility and the future perspectives in terms of research and development, as well as problems stemming from decisions made by stakeholders and policymakers. We started with a tutorial explaining the taxonomy of connected mobility – from the system level of ITS to specific networking protocols and access technologies.

We continued by explaining the topological challenges and their effect on network performance – i.e., not only from road topologies and scenarios, but also the dynamic nature of a network topology where nodes have high mobility. These considerations allow us to explain the evolution of VANETs to their current state – e.g., how it made IEEE 802.11p define itself for a fixed data rate of 6 Mbps – and how these phenomena might affect the performance of the next generation of vehicular networks, which try to make good on the promise of higher throughput by using network diversity (e.g., MIMO, MCO, multiple bands).

Furthermore, we explore the effect of uptake in fleet heterogeneity. Due to the nature of the vehicular market, it is expected that the CCAM fleet will consist of vehicles with different characteristics, capabilities, and performance – even driving styles. Furthermore, CCAM vehicles will share the road with vehicles that have no automation or communication capabilities. We finalize this chapter by proposing ways to mitigate the multi-faceted problem of heterogeneity.

Acknowledgments

This work was partially supported by SAFER in the project "Human Factors, Risks and Optimal Performance in Cooperative, Connected and Automated Mobility", the Swedish Transport Administration in the project "Here I go" – advanced functions for VRU-awareness protocol in C-ITS" and "the Knowledge Foundation in the project "SafeSmart – Safety of Connected Intelligent Vehicles in Smart Cities" (2019–2024).

Author details

Elena Haller*† and Oscar Amador Molina†

Halmstad University, Halmstad, Sweden

† These authors contributed equally

*Address all correspondence to: elena.haller@hh.se

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] European Commission. Eu road fatalities drop by 3% in 2024, but progress remains slow, 2025. Available from: https://transport.ec.europa.eu/news-events/news/eu-road-fatalities-drop-3-2024-progress-remains-slow-2025-03-18_en [Accessed: 2025-August-23]

[2] World Health Organization. Road Safety, 2025. Available from: https://www.who.int/health-topics/road-safety#tab=tab_1 [Accessed: 2025-August-23]

[3] European Commission (EC). Towards a European Road Safety Area: Policy Orientations on Road Safety 2011-2020, 2010

[4] SAE International. V2x communications message set dictionary, 2022. Available from: https://www.sae.org/standards/content/j2735_202211/ [Accessed: 2025-August-14]

[5] European Telecommunications Standards Institute. Intelligent transport systems (its); users and applications requirements; part 1: Facility layer structure, functional requirements and specifications; release 2. Technical Specification TS 102 894-1 V2.0.0, ETSI, 2023. Available from: https://www.etsi.org/deliver/etsi_ts/102800_102899/10289401/02.00.00_60/ts_10289401v020000p.pdf

[6] TV 3GPP. 3rd generation partnership project; technical specification group services and system aspects; study on lte support for vehicle to everything (v2x) services (release 14), 2015

[7] CAR 2 CAR Communication Consortium. Guidance for day 2 and beyond roadmap. White Paper C2CCC-WP-2072, CAR 2 CAR Communication Consortium, 2021. Available from: https://www.car-2-car.org/fileadmin/documents/General_Documents/C2CCC_WP_2072_RoadmapDay2AndBeyond_V1.2.pdf [Accessed: 2025-August-14]

[8] Soto I, Calderon M, Amador O, Urueña M. A survey on road safety and traffic efficiency vehicular applications based on c-v2x technologies. Vehicular Communications. 2022;**33**:100428. DOI: 10.1016/j.vehcom.2021.100428

[9] Zhu Q, Wang C-X, Hua B, Mao K, Jiang S, Yao M. 3gpp tr 38.901 channel model. In the Wiley 5G Ref: The Essential 5G Reference Online. Hoboken, NJ, USA: Wiley Press; 2021:1–35

[10] Boban M, Barros J, Tonguz OK. Geometry-based vehicle-to-vehicle channel modeling for large-scale simulation. IEEE Transactions on Vehicular Technology. 2014;**63** (9):4146–4164

[11] Kyösti P, Meinilä J, Hentila L, Zhao X, Jämsä T, Narandzic M, Milojevic M, Hong A, Ylitalo J, Holappa V-M, Mikko Alatossava RJC, Bultitude YJ, Rautiainen T. Winner ii channel models. IST-4-027756 Winner Ii D1.1.2 V1.2, 2008

[12] Yamamoto A, Tsutomu S, Hayashi T, Koichi Ogawa JON, Pedersen GF, Takada J-I, Sakaguchi K. Mimo performance evaluation in a street microcell using a spatial fading emulator in comparison with a radio propagation test. COST2100 TD. 2009;**09**:912

[13] Ieee standard for information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 6: Wireless access in vehicular environments. IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009); 2010, 1–51. DOI: 10.1109/IEEESTD.2010.5514475

[14] M Series. Guidelines for evaluation of radio interface technologies for imt-advanced. Report ITU. 2009;**638** (31):11–23

[15] Molisch AF. Wireless Communications. Hoboken, NJ, USA: John Wiley & Sons; 2012;**34**

[16] Haller E, Amador O, Nilsson E. On radcom channel capacity for v2v applications. In 2024 International Symposium on Electromagnetic Compatibility; EMC Europe, 385–390, 2024. DOI: 10.1109/EMCEurope59828.2024.10722065

[17] IEEE standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 5: enhancements for next generation V2X. IEEE Std 802.11bd-2022 (Amendment to IEEE Std 802.11-2020 as amended by IEEE Std 802.11ax-2021, IEEE Std 802.11ay-2021, IEEE Std 802.11ba-2021, IEEE Std 802.11-2020/Cor 1-2022, and IEEE Std 802.11az-2022); IEEE; 1–144, 2023. DOI: 10.1109/IEEESTD.2023.10063942

[18] European Telecommunications Standards Institute (ETSI). Intelligent Transport Systems (ITS); Decentralized congestion control mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part. ETSI EN 102 687 - V1.2.1, 2018

[19] Federal Communications Commission. Fcc allocates spectrum in 5.9 ghz range for intelligent transportation systems uses, 1999. Available from: https://transition.fcc.gov/Bureaus/Engineering_Technology/News_Releases/1999/nret9006.html [Accessed: 2025-August-12]

[20] C-Roads Platform. C-roads position paper on 5.9ghz band, 2017. Available from: https://www.c-roads.eu/fileadmin/user_upload/media/Dokumente/C-Roads_Position_paper_on_59GHz_final.pdf [Accessed: 2025-August-12]

[21] Intelligent Transportation Society of America. 5.9 ghz band: Myths vs. facts, 2020. https://itsa.org/wp-content/uploads/2020/04/V2X-Myth-Vs-Fact-Sheet.pdf [Accessed: 2025-August-12]

[22] European Telecommunications Standards Institute (ETSI). Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band. ETSI EN 302 663 1.2.0, ETSI, 2012

[23] European Telecommunications Standards Institute. ETSI EN 303 797 V2.1.1 (2024-02): Intelligent Transport Systems (ITS); ITS-G5 Access layer in the 5 GHz frequency band; Release 2, 2024. Available from: https://www.etsi.org/deliver/etsi_en/303700_303799/303797/02.01.01_60/en_303797v020101p.pdf. [Accessed: 2025-August-12]

[24] Tan DKP, Jia H, Yanchun L, Bayesteh A, Chen Y, Zhu P, Tong W. Integrated Sensing and Communication in 6G: Motivations, Use Cases, Requirements, Challenges and Future Directions. In 2021 1st IEEE International Online Symposium on Joint Communications & Sensing (JC&S); 2021. p. 1–6. DOI: 10.1109/JCS52304.2021.9376324

[25] Picazo-Martinez P, Barroso-Fernandez C, Martin-Perez J, Groshev M, de la Oliva A. IEEE 802.11az Indoor Positioning with mmWave. IEEE Communications Magazine; 2023, 1–7. DOI: 10.1109/MCOM.001.2300454

[26] Anwar W, Franchi N, Fettweis G. Physical Layer Evaluation of V2X Communications Technologies: 5G NR-V2X, LTE-V2X, IEEE 802.11bd, and IEEE 802.11p. In 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall); 2019, 1–7. DOI: 10.1109/VTCFall.2019.8891313

[27] William Whyte. C-its deployment in the us. Presentation at the 9th ETSI ITS Workshop. Sofia Antipolis, France: OnBoard Security; 2018

[28] Ishii T. Its radiocommunications in Japan – Progress report and future directions. Presentation at the 9th ETSI ITS Workshop, 2018. Ministry of Internal Affairs and Communications (MIC), Japan

[29] Martin Böhm. C-roads platform overview. Presentation at the 9th ETSI ITS Workshop. Sofia Antipolis, France: C-Roads Platform, Co-financed by the European Union; 2018

[30] Leitzke C. C-its corridor – Etsi g5 is reality. Presentation at the 9th ETSI ITS Workshop, 2018. Hessen Mobil, Germany

[31] ASFINAG. Asfinag connects roads with vehicles on a large scale in Europe, 2020. Available from: https://c-its-deployment-group.eu/activities/c-its-deployments/2020-10-09-asfinag-connects-roads-with-vehicles-on-a-large-scale-in-europe/ [Accessed: 2025-August-13]

[32] Tseng H-R. C-its in Taiwan. In Presentation at the 9th ETSI ITS Workshop. Sophia Antipolis, France: Industrial Technology Research Institute (ITRI); 2018

[33] C-Roads Platform. Annual deployment overview report 2023. C-Roads Platform Internal Report, 2023. Available from: https://www.c-roads.eu [Accessed: 2025-August-13]

[34] U.S. Department of Transportation, ITS Joint Program Office. Connected vehicle pilot deployment program (2024 update). Technical Report, U.S. Department of Transportation, 2024. Available from: https://www.its.dot.gov/pilots/cv_program_benefits.htm. Executive Briefing, Updated April 2024

[35] Sommer C, German R, Dressler F. Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis. IEEE Transactions on Mobile Computing. 2011;**10**(1):3–15

[36] Riebl R, Günther H, Facchi C, Wolf L. Artery: Extending Veins for VANET Applications. In 2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS); 2015. p. 450–456

[37] Koutlia K, Bojovic B, Ali Z, Lagen S. Calibration of the 5g-Lena system level simulator in 3gpp reference scenarios.

Simulation Modelling Practice and Theory. 2022;**119**:102580

[38] Volvo Cars. Volvo hällered proving ground, 2024. Available from: https://www.volvocars.com/se/hallered/ [Accessed: 2024-April-27]

[39] Group V. Volkswagen ehra-lessien proving grounds, 2024. Available from: https://en.wikipedia.org/wiki/Ehra-Lessien [Accessed: 2024-April-27]

[40] Technische Hochschule Ingolstadt. Carissma outdoor test facility, 2024. Available from: https://www.thi.de/en/research/carissma/laboratories/outdoor-test-facility/ [Accessed: 2024-April-27]

[41] RISE Research Institutes of Sweden. Astazero test track, 2024. Available from: https://astazero.ri.se/ [Accessed: 2024-April-27]

[42] RWTH Aachen University. Center for european research on mobility (cerm), 2024. Available from: https://www.elektrotechnik.rwth-aachen.de/cms/Elektrotechnik-und-Informationstechnik/Forschung/Interdisziplinaere-Einrichtungen/Interdisziplinaere-Einrichtungen/mcxi/CERM/lidx/1/ [Accessed: 2024-April-27]

[43] ETSI Secretariat. 6th its cooperative mobility services plugtest. ETSI Plugtests Report V1.1.2, European Telecommunications Standards Institute (ETSI), Sophia Antipolis, France; 2019. Available from: https://www.etsi.org. Held from 25 February to 1 March 2019

[44] ETSI Secretariat. 1st etsi c-v2x plugtests. ETSI Plugtests Report V1.0.0, European Telecommunications Standards Institute (ETSI), Malaga, Spain, 2019. Available from: https://www.etsi.org/images/files/Events/2019/CV2X-Plugtests/1st_ETSI_C-V2X_Plugtests_Report_v100.pdf. Held from 2 to 6 December 2019 [Accessed: 2025-August-14]

[45] ETSI Secretariat. 2nd etsi c-v2x plugtests. ETSI Plugtests Report V1.1.0, European Telecommunications Standards Institute (ETSI), Remote, 2020. Available from: https://www.etsi.org/images/files/Events/2020/CV2X-Plugtests/2nd_ETSI_C-V2X_Plugtests_Report_v100.pdf. Held from 20 to 31 July 2020

[46] ETSI Secretariat. 3rd Etsi C-v2x Plugtests. Etsi Plugtests Report, European Telecommunications Standards Institute (ETSI), Klettwitz, Germany; 2022. Available from: https://www.etsi.org/events/open-meetings/1759-cv2x-plugtests-3. Held from 28 March to 1 April 2022

[47] ETSI Secretariat. 4th etsi c-v2x plugtests. ETSI Plugtests Report V1.0.0, European Telecommunications Standards Institute (ETSI), Malaga, Spain; 2024. Available from: https://www.etsi.org. Held from 10 to 13 September 2024

[48] Autotalks. Dsrc vs. c-v2x, 2024. Available from: https://auto-talks.com/technology/dsrc-vs-c-v2x/ [Accessed: 2025-August-14]

[49] ETSI. Intelligent transport systems (its); access layer specification for intelligent transport systems operating in the 5 ghz frequency band. ETSI Technical Specification TS 103 697, European Telecommunications Standards Institute (ETSI), 2024. Available from: https://www.etsi.org/deliver/etsi_ts/103600_103699/103697/02.01.01_60/ts_103697v020101p.pdf [Accessed: 2025-August-14]

[50] Molina OA, Valle F, Sjögren N, Duc Huy V, Calderón M, Soto I, Urueña M. The smart highway to babel: The coexistence of different generations of intelligent transport systems and conventional drivers. International Journal on Advances in Intelligent Systems. 2025;**18**(1-2):1–10

[51] CAR 2 CAR Communication Consortium. C2c-cc basic system standards profile. Technical Report Release 1.5.1, CAR 2 CAR Communication Consortium, 2020. Available from: https://www.car-2-car.org/fileadmin/documents/Basic_System_Profile/Release_1.5.1/C2CCC_RS_2037_Profile.pdf [Accessed: 2025-August-14]

[52] Hegde A, Song R, Festag A. Radio resource allocation in 5g-nr v2x: A multi-agent actor-critic based approach. IEEE Access. 2023;**11**:87225–87244. DOI: 10.1109/ACCESS.2023.3305267

[53] Hegde A, Festag A. Mode switching performance in cellular-v2x. In: 2020 IEEE Vehicular Networking Conference (VNC); 2020, 1–8. DOI: 10.1109/VNC51378.2020.9318394

[54] Hegde A, Delooz Q, Mariyaklla CL, Festag A, Klingler F. Radio resource allocation for collective perception in 5g-nr vehicle-to-x communication systems. In: 2023 IEEE Wireless Communications and Networking Conference (WCNC); 2023, 1–7. DOI: 10.1109/WCNC55385.2023.10118606

[55] Hegde A, Lobo S, Festag A. Cellular-v2x for vulnerable road user protection in cooperative its. In 2022 18th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 118–123, 2022. DOI: 10.1109/WiMob55322.2022.9941707

[56] Molina OA, Aramrattana M, Chen L, Elena H. Human factors, risks and optimal performance in cooperative, connected and automated mobility: Final report; 2024. Available from: https://www.diva-portal.org/smash/record.jsf?pid=diva2 [Accessed: 2025-August-14]

[57] Milakis D, Snelder M, Arem B, Wee B, de Almeida Correia GH. Development and transport implications of automated vehicles in the Netherlands: Scenarios for 2030 and 2050. European Journal of Transport and Infrastructure Research. 2017;**17**:63–85. DOI: 10.18757/ejtir.2017.17.1.3180

[58] European Automobile Manufacturers' Association. Average age of the EU vehicle fleet, by country. Available from: https://www.acea.auto/figure/average-age-of-eu-vehicle-fleet-by-country/ [Accessed: 2024-January-31]

[59] Volkswagen Group. Volkswagen Group delivers 45 percent more all-electric vehicles in first 9 months. Available from: https://www.volkswagen-newsroom.com/en/press-releases/volkswagen-group-delivers-45-percent-more-all-electric-vehicles-in-first-9-months-17771/ [Accessed: 2024-January-31]

[60] Figueroa E, Paolini M. Wi-fi certified makes it wi-fi: An overview of the wi-fi alliance approach to certification. Technical Report, Wi-Fi Alliance, 2006. Available from: https://www.wi-fi.org [Accessed: 2025-August-14]

[61] 3GPP RAN and RAN WG Chairs. Interoperability and compatibility of 5g specifications, 2018. Available from: https://www.3gpp.org/news-events/

3gpp-news/copatibility [Accessed: 2025-August-14]

[62] Federal Communications Commission. Second Report and Order: Use of the 5.850–5.925 GHz Band. FCC Report FCC 24-123, Federal Communications Commission, 2024. Available from: https://docs.fcc.gov/public/attachments/FCC-24-123A1.pdf. ET Docket No. 19-138

[63] Amador O, Soto I, Calderón M, Urueña M. Experimental evaluation of the etsi dcc adaptive approach and related algorithms. IEEE Access. 2020;**8**:49798–49811. DOI: 10.1109/ACCESS.2020.2980377

[64] Delooz Q, Riebl R, Festag A, Vinel A. Design and performance of congestion-aware collective perception. In 2020 IEEE Vehicular Networking Conference (VNC), 1–8, 2020. DOI: 10.1109/VNC51378.2020.9318335

[65] European Telecommunications Standards Institute. Intelligent Transport Systems (ITS); Radio Resource Management for C-ITS Facilities Layer. Technical Report TR 104 073 V2.1.1. ETSI, 2023. Available from: https://www.etsi.org/deliver/etsi_tr/104000_104099/104073/02.01.01_60/tr_104073v020101p.pdf [Accessed: 2025-August-14]

[66] Haller E, Sidorenko G, Amador O, Nilsson E. Offloading platooning applications from 5.9 ghz v2x to radar communications: Effects on safety and efficiency. arXiv preprint arXiv:2401.09242, 2024

Chapter 2

Policy Pathways for Autonomous Vehicles in Urban Mobility: Insights and Strategic Lessons from a Systematic Review

Hisham Y. Makahleh

Abstract

Autonomous vehicles (AVs) could improve safety, accessibility, emissions, and efficiency in urban transport. Real-world adoption, however, remains slow because of technical, policy, behavioural, and infrastructure constraints. This chapter builds on an existing systematic review of AV literature (n = 41, peer-reviewed, 2003–23) and supplements it with additional practice evidence (AV pilot evaluations and policy) to develop an evidence-informed pathway for the policy design of urban AV adoption. It synthesises AV governance, behavioural and infrastructure requirements for their adoption, including lessons from early-adopter cities and related mobility transitions (eg, Electric Vehicles, micromobility, and shared mobility), to point to the importance of governance and implementation transparency, multi-stakeholder approaches, equity, and alignment with climate and emissions goals. The chapter closes with an actionable AV policymaking framework on the what, how, who, and when of policy action, as a step towards scaling up AVs beyond pilot-stage projects and towards resilient urban mobility.

Keywords: autonomous vehicles, sustainable transport, urban mobility, transport policy, AV adoption strategies, infrastructure readiness, climate adaptation, governance

1. Introduction

Autonomous vehicles (AVs) have moved from prototype to policy. They could reshape how cities plan, operate, and deliver transport services. One of the first international frameworks to describe the technical aspects of AVs and how they could interact with the environment around them was provided by the Society of Automotive Engineers (SAE [1]). The SAE taxonomy and definitions technical report is widely recognised around the world and has formed the basis for most policy, technical, and safety discussions around automated driving systems. The SAE differentiates between different levels of driving automation systems, from Level 0 (no automation) through to Level 5 (full automation), and describes how these

automated driving systems work differently across each level. This work also focuses on the resulting changes in the driver's role across levels of automation and the resulting legal, regulatory, and policy questions around liability and responsibility. These factors also have a direct effect on how transport services are operated under different transport service models.

The U.S. National Highway Traffic Safety Administration (NHTSA) defines AV safety as system safety, the interaction of humans with the systems in place, and the interaction of these systems in the natural traffic environment around us [2]. The NHTSA emphasises that AV capability develops continuously and that clear, shared terminology is essential [3]. This should provide consistency and agreement between engineers, manufacturers, policymakers, decision-makers, and the public.

Rolling out the first self-driving shuttle routes in Solihull, the trial of the SCALE self-driving shuttle in Birmingham, and associated government research and development programmes to support their innovation are expanding our real-world knowledge of AVs [4–7]. Other locally led AV-related trials, such as Sunderland's wider smart city infrastructure projects [8]. They are also helping to build on the DfT's testing framework Code of Practice for Testing and trailing AVs [9], which was itself based on lessons learned from earlier testing approaches, and the Future Transport Zones evaluation framework [10], which is intended to provide clarity on testing, developing, and scaling autonomous vehicles. Meanwhile, AV manufacturers such as Ohmio are active in developing market-leading micro autonomous shuttle platforms to meet the needs of their global and diverse autonomous shuttle market [11].

Electric Vehicles (EVs) adoption offers a close analogue to AV adoption: both require coordinated infrastructure, behavioural acceptance, and policy incentives. Taamneh and Makahleh examined the technical, economic, and human behavioural factors that affect EV uptake [12]. Shared mobility modes were found to be a driver for EV use because of their potential to enhance multi-modality and connect activity centres to public transport. The effects of shared mobility on multimodal choice and increasing access to public transport were investigated by Bankole et al. in low and middle-income countries [13], and more broadly for accessibility improvements by Bankole et al. [14].

Operational research is available on the interaction between automated cooperative vehicles (CAVs) and human-driven vehicles. Makahleh explored overtaking manoeuvres when CAVs overtake human-driven vehicles. The research demonstrated that overtaking distance and headway, as well as the lane-keeping performance and lane discipline of both CAVs and human-driven vehicles, are affected by the mix of these vehicle types on the road [15]. Makahleh and Makahleh studied lane-change decision-making for overtaking CAVs and demonstrated that lane changing and mixed traffic throughput are also affected by the presence of mixed vehicles on the road [16]. On the other hand, consumer acceptance factors, which determine their choice to use AVs, are important for AV usage. Nordhoff et al. used a stated choice experiment to investigate how these three factors (ie, safety perception, trust, and comfort) affect the intention to ride shared AVs, with acceptance being the main behavioural factor [17, 18]. In a related study, Nordhoff et al. empirically demonstrated the causal influence of context on AV acceptance and showed that the direct contextual factors had an impact on safety perception, trust, and comfort, which are the main behavioural factors in user acceptance of shared

AVs [19]. In a further paper, Nordhoff et al. developed a theoretical model for understanding shared AV acceptance by using a multi-level approach in a multi-level acceptance model for shared autonomous vehicles (MAVA) to study the links between AV-related contextual factors and individual acceptance in shared AV systems [20]. Fonzone et al. studied pre-ride expectations and post-ride experiences of passengers on an autonomous bus service [21]. The results showed a mismatch in how AVs are advertised pre-ride and the features passengers experienced post-ride. Passengers experienced both human-driven vehicles and automation-related features that affected their behaviour while on the ride. Fonzone et al. also found that contextual variables, such as weather conditions, influenced the experiences and behaviours of passengers on an autonomous bus service [22].

Deployment depends on physical infrastructure (road markings, junction design) and digital systems (C-ITS, V2X) [23]. Blumenfeld et al. have stated that the development of automated transport systems requires a systems approach that integrates the physical with the digital infrastructure, as well as the operation and maintenance with operational safety assurance aspects of transport automation [24]. The same group of researchers has also provided evidence that the development of smart roads should not under-optimise the role of autonomous vehicles in transport [25]. Meanwhile, resilience is also a key part of the conversation on AVs, and Ferranti et al. have provided evidence showing that transport systems which fail to take account of climate change in their design and infrastructure deployment run the risk of being operationally disrupted by physical climate events and changes [26]. Andres et al. have provided a resilience-focused systematic review that looked at different metrics for the resilience of transport systems as they become automated and connected [27]. These and similar findings and recommendations have also been highlighted by bodies such as the Intergovernmental Panel on Climate Change (IPCC), which has released research assessing the literature on physical climate risks and impacts [28], and adaptation for transport infrastructure and the challenges it faces [29].

The AV policy links directly to SDG 11.2 (safe, affordable access), 9.1 (resilient infrastructure), and 13.2 (climate action) [30]. Practitioner-focused research has also identified approaches for overcoming challenges and issues that need to be considered when integrating autonomous and automated transport into urban mobility [31]. Another recent systematic map related to the MAST MODES project investigated active modes and included evidence on associated psychological theories and behaviour change, which can provide insights for supporting the transition to sustainable transport [32].

Research related to autonomous shuttles (AS) also has an underpinning academic research infrastructure to ensure that evidence-based decision-making on policy and practice areas can draw on the highest quality and most relevant sources of evidence [33–38]. Academic research also has its own set of literature and data sources, which are subject to change and can be compared and evaluated to provide the most optimal selection of evident sources. One such study conducted a comparative evaluation of four major bibliographic databases to determine their suitability in identifying relevant literature for a rapid review on active travel [39]. This type of research-related study can support research on AVs, active travel, and other fields to inform decisions on where to direct search terms, collection efforts, and other strategies to best utilise the resources available to obtain relevant and high-quality sources of evidence.

The purpose of this chapter is to provide a set of policy pathways informed by evidence from a recent systematic review of 41 relevant peer-reviewed studies (2003–2023) on the impact of AVs on urban transport and mobility [40]. The research from the systematic review reported that the likelihood of specific types of AV uptake results from the interaction of technological advances, the policy environment, changes in behaviour, and wider changes in infrastructure. The pathways have also been produced to support global frameworks such as the Paris Agreement, which aims for the Agreement's signatories to take action to limit the global temperature rise to well below 2°C above pre-industrial levels and pursue efforts to limit the temperature increase to 1.5°C. The Agreement also sets out a commitment by all Parties to reach the global peaking of greenhouse gas emissions as soon as possible, achieve a balance between anthropogenic emissions by sources and removals by sinks in the second half of the century, increase adaptation efforts, and make finance flows consistent with a pathway towards low greenhouse gas emissions and climate-resilient development [41].

1.1 Why planning and transport policy determine AV outcomes?

The AVs are not policy-neutral. Planning and transport policy choices, street design standards, curb and parking policy, bus priority, and demand management mediate whether AVs increase vehicle-kilometres travelled (VKT) and sprawl or support compact, low-carbon mobility. International syntheses find that private point-to-point AVs tend to raise VKT and reduce transit/walking unless pricing, parking reform, and transit integration are in place; shared and feeder AVs can reduce parking demand and complement mass transit when embedded in SUMP-style plans. Accordingly, cities should treat AV policy as land-use and climate policy: couple AV pilots to transit hubs, protect bus lanes, and align permits with mode-shift and CO_2 Key Performance Indicators (KPIs) [42]. **Table 1** outlines the main AV deployment models, showing how each connects to planning and infrastructure decisions, the key risks that effective policy can address, and their alignment with relevant SDG targets.

Accordingly, the aim of this chapter is to translate that evidence into actionable strategies for policymakers, urban planners, and industry stakeholders to guide the adoption of AVs in urban mobility systems. This study is guided by the following research questions:

AV lever	Planning/ Infrastructure linkage	Primary risk addressed if managed	Policy handle	SDG linkages
Private, point-to-point AVs	Parking minima, curb space management	Induced vehicle kilometres travelled (VKT), public transport cannibalisation	Parking reform, bus priority, dynamic road pricing.	11.2, 13.2
Shared AV feeders (electrified)	Station siting, charging depots, service headways	First–last mile connectivity gaps	Integration with PT timetables and MaaS frameworks	11.2, 9.1, 13.2
V2X/C-ITS corridors	Signal priority, lane markings, junction geometry.	Operational reliability and safety incidents (eg, fewer disengagements).	AV-ready road codes, infrastructure audits	9.1, 11.2

Table 1.
AV levers → planning/infrastructure links → SDG targets.

RQ1: What policy levers and governance structures can most effectively support AV integration into urban mobility?

RQ2: What behavioural, infrastructural, and technological factors influence AV adoption in different urban contexts?

RQ3: How can AV deployment be aligned with climate action goals and sustainable transport policy frameworks?

2. Methodological foundations

The methodological approach that informed this chapter originated from an identified research gap in the broader AV literature, namely, a critical lack of synthesis between research outputs predominantly focused on either isolated technical feasibility or single-aspect acceptance factors. Whilst the primary evidence base for this chapter was informed by a recent and dedicated systematic literature review of 41 published, peer-reviewed studies [40], the chapter as a whole is informed by a broader methodological framework which facilitates active and iterative integration of multiple and complementary streams of knowledge, triangulation through case-based evidence, and future-looking scenario analysis. As such, while the results of this chapter are informed by the outputs of prior, discrete studies, the overall approach goes beyond simple synthesis and serves as a policy translation platform for urban mobility planning in the context of Connected and Automated Mobility (CAM). This section outlines the research philosophy, evidence-gathering process, appraisal techniques, and analytical synthesis strategies used to develop the policy pathways presented later in the chapter.

2.1 Research orientation and rationale

The overall aim was to develop a synthesis of the best available peer-reviewed evidence on AVs and urban mobility, including their technological, behavioural, infrastructural, and governance-related aspects; and to interpret and reframe this evidence with a policy and strategic emphasis. The focus was on avoiding the mechanical aggregation of findings and moving towards an interpretive, synthesising approach that can offer an understanding of the system in which AVs operate, with its internal linkages and trade-offs, as well as the conditions required to enable the successful uptake of AVs in urban areas in practice.

The approach follows policy-oriented evidence synthesis [43–45], with the added emphasis on ensuring that the knowledge gained is translated into a decision-making framework that is actionable by cities, transport authorities, practitioners, and industry actors. In addition, the approach was justified based on three criteria:

- Transparency: being able to demonstrate that the resulting propositions are directly traceable to an established and replicable evidence base.

- Rigour: having a quality appraisal approach that is structured and can help reduce bias and over-influence from sources without a clear evidence base or vested interests (including some media and industry sources, as well as less academically rigorous conference and working papers).

- Relevance: giving priority to the inclusion of studies with a direct, clear focus on urban mobility systems and public transport contexts and/or objectives, such as sustainable mobility.

2.2 Evidence identification

The evidence base was generated by searching two bibliographic databases (Scopus and Web of Science), selected for their comprehensiveness in engineering, policy, transport, and social science literature, respectively. Search terms combined controlled vocabulary and free-text terms to maximise cross-disciplinary retrieval of eligible studies, for example:

'Autonomous vehicles' OR 'self-driving' OR 'automated shuttles' AND 'Urban mobility' OR 'public transport' OR 'transport policy' OR 'sustainable transport'.

Searches were limited to 2003–2023 to minimise the year of publication bias and to maintain currency, given that AV research and development has only relatively recently transitioned from prototype engineering projects to issues such as regulation, social response, and policy. Citation chasing of review papers also manually supplemented the search [46, 47].

2.3 Inclusion and exclusion criteria

Eligibility criteria were developed to ensure that the included studies were both methodologically robust and policy-relevant. Inclusion criteria required that studies:

- Focus on AVs, or highly automated driving systems, within urban contexts.
- Examine policy, governance, behavioural, infrastructural, or environmental aspects relevant to mobility systems.
- Be published in peer-reviewed journals or reputable conference proceedings.
- Provide empirical, modelling-based, or systematic review evidence.

Exclusion criteria removed studies that were:

- Purely technical, without mobility, governance, or policy implications.
- Focused exclusively on non-urban or off-road contexts.
- Not available in English.

2.4 Analytical framework

A thematic synthesis method was adopted to organise the data into policy-relevant categories. This involved:

- Descriptive coding: distillation of key study features, including study context, AV type, target user group, and policy environment.

- Analytical coding: cross-mapping of distilled insights into thematic categories related to policy levers (eg, governance models, behavioural nudges, infrastructural preparedness).

- Integrative synthesis: aligning thematic insights with high-level policy trajectories, explicitly accounting for synergies between technological, behavioural, and regulatory levers.

The analysis framework in this chapter moves beyond a simple, descriptive compilation of existing studies towards a more strategic interpretation that actively seeks to pinpoint leverage points and actionable interventions. Instead of listing results, cross-theme matrices were used to identify how technical, behavioural, and regulatory mechanisms interact (eg, road-marking quality → safety disengagements → public trust).

2.5 Policy translation lens

One of the key methodological innovations in this work was the addition of a policy translation lens at the point of synthesis. This involved reframing the systematic review results against:

- Global policy frameworks, such as the Paris Agreement and the UN Sustainable Development Goals, play a crucial role in shaping international efforts towards sustainability and climate action.

- National and subnational policy frameworks (UK Future of Mobility Urban Strategy, regional transport decarbonisation plans, etc.)

- Urban operational realities (eg, budget limits, legacy infrastructure, political acceptability)

Each policy lever was mapped to corresponding SDG targets (11.2 access, 9.1 resilient infrastructure, 13.2 climate integration) and to national evaluation frameworks, such as the Future Transport Zones, for traceability. In this way, the policy pathways are evidence-based but also context-aware, so that they can be adapted to different urban or governance settings, while still rooted in empirical evidence.

3. Theoretical and policy framework (COM-B model)

The COM-B (Capability, Opportunity, Motivation, and Behaviour) framework offers a useful theoretical perspective for making sense of both behavioural and policy elements of AV adoption as part of mobility systems. It has been widely used in transport behaviour research to help 'diagnose' the determinants of behavioural change and to understand the types of interventions that can overcome or 'address' these determinants [48]. Using COM-B in the context of AV policy pathways enables a structured approach to understanding how aspects of technological readiness, governance arrangements, and public engagement strategies interact to determine patterns of uptake.

3.1 Rationale for using COM-B in AV policy design

Unlike many behavioural models, COM-B treats behaviour as part of a wider system. It recognises that behaviour both affects and is affected by that system. These are:

- Capability: the psychological and physical capacity of individuals or organisations to behave in a particular way, that is, to be able to adopt and integrate AV technology into the mobility system.

- Opportunity: the external factors (the environment and resources) that make behaviour possible or prompt it, that is, factors that either enable or hinder the adoption of AV technology.

- Motivation: the processes that affect individuals' and organisations' decisions about behaviour, in particular both reflective (conscious) and automatic (unconscious) processes, that is, the factors that lead to being willing to adopt and use AVs.

Applied to urban mobility policy, capability, opportunity, and motivation will need to be considered as a system in order to facilitate AV adoption, for the reasons noted above: using AVs is not simply a matter of individual preference; urban mobility also needs to reflect the design of infrastructure, the regulatory environment, trust in systems, and the operation of mobility systems.

3.2 Capability: Building skills and knowledge for AV integration

Capability includes both individual and institutional factors:

- Individual capability: User understanding of AV technology, safety features, and usage of autonomous services. Research has demonstrated that low public awareness of AV technology limits trust and acceptance [20].

- Institutional capability: Preparedness of transport agencies, local authorities, and operators to plan, regulate, and operate AV services. This requires training, inter-agency collaboration, and integration of AV into transport planning processes [46].

From a policy perspective, interventions to enhance capability include public education campaigns, professional training for mobility planners, and cross-disciplinary knowledge exchange between technology providers and regulatory bodies.

3.3 Opportunity: Creating an enabling environment

Opportunity describes the external environment that makes AV use possible or appealing:

- Physical opportunity: This covers the existence of safe and connected road infrastructure, reliable digital communications, and urban design that enables

AV operation. Trial evidence from the United Kingdom (SCALE, CAVForth, etc.) suggests poor road markings, inconsistent signage, and lack of connectivity are the key points for AV operation [10].

- Social opportunity: This covers cultural norms, public perceptions, and social acceptability. Studies have shown that visible demonstration projects and direct participation in real-world trials can help shift norms towards acceptance, especially when there is clear communication of safety protocols in place [22].

Policy levers in this space include selective investment in infrastructure, inclusion of AV-readiness within urban design codes, and, more broadly, embedding AV trials in sustainable mobility strategies.

3.4 Motivation: Building trust, perceived value, and engagement

Motivation: Psychological factors influencing AV adoption

- Reflective motivation encompasses deliberate choices based on beliefs about the AVs' safety, efficiency, and environmental impact. Research shows that perceived risk is a major barrier to AV adoption, even if the technical performance is consistent [20].

- Automatic motivation includes habitual behaviour and emotional reactions, such as the reluctance to give up driving control, which may persist even among populations that accept the efficiency benefits of AVs.

Strategies for addressing motivation include clear communication about incident reporting and resolution, incentives for early adopters, and aligning AV services with visible sustainability goals (eg, emissions reduction targets).

3.5 Integrating COM-B into policy pathways

A COM-B-informed approach to designing policy pathways for AV adoption may thus entail:

- Identifying barriers and facilitators in each of the domains of Capability, Opportunity, and Motivation from empirical data (eg, as seen in the evidence base of the systematic review [40]).

- Associating an intervention to each of these three domains, for example, a capability-building intervention mapped to public education and awareness raising, an opportunity-enhancing intervention mapped to physical infrastructure change, and a motivation-enhancing intervention mapped to trust in the technology.

- Monitoring and iterating: observing how interventions affect behavioural determinants over time and customising them to different urban settings.

By considering how the adoption pathway is affected by the behavioural determinants in each domain, policy pathways become not just technically robust but also behaviourally realistic, thus increasing the chances of long-term and equitable adoption.

4. Policy pathways for urban AVs: Planning, governance, and behaviour (COM-B-aligned)

The AV deployment is not only a technological change but also a complex transition requiring behavioural, infrastructural, and governance coordination. This synthesis paper on the global evidence from peer-reviewed literature, pilot evaluations, and policy documents presents the evidence-based, actionable pathways for the deployment of AVs. Using COM-B, it is possible for policymakers to target specific barriers and enablers in a cohesive and complementary strategy rather than disjointed interventions.

4.1 Building capability (users and institutions)

Capability gaps among users and institutions limit uptake even when technology works. International AV trials indicate that both public and institutional capability gaps are prevalent and hard to close. On the public side, insufficient operational understanding, including confusion around emergency response procedures, vehicle control restrictions, or the ride-booking process, has been shown to undermine AV usage intention [19, 49]. Within the European CityMobil2 project, lack of awareness of system features and safety functions provoked risk-averse behaviour, slowing boarding times and reducing system throughput [17].

Institutional capability is also important. Analyses of Finland's SOHJOA programme and Singapore's autonomous bus deployment found that even technology-ready cities may struggle to develop AV-specific governance capacity in areas such as safety auditing, insurance regulation, and operational data interpretation [46]. In the absence of this expertise, local governments may struggle to avoid delayed deployments or patchwork regulatory frameworks.

Policy pathway: Governments should embed AV literacy into existing mobility education programmes and invest in targeted training for transport agency staff. This could include simulation-based exercises, workshops with manufacturers, and joint scenario planning with emergency services.

4.2 Urban planning and infrastructure readiness

Street design standards and AV-ready codes, including consistent lane markings, legible signage, intersection geometry, and C-ITS/V2X connectivity, have a major effect on automated operation and user confidence. Trials often report disengagements and manual overrides at substandard junctions, while improving markings and signal logic reduces those incidents. Planning policy should fund connected corridors that prioritise legibility and bus priority, and design AV stops as feeders to rail or bus networks rather than as door-to-door replacements [50]. At the corridor scale, licensing to expand operations should depend on infrastructure audits and published safety cases to ensure that lessons

from operations inform the next deployment phase. Jurisdictions that maintain consistent AV-ready infrastructure show measurable improvements in system stability and safety.

4.3 Digital/data interoperability and transparency

Digital standards and open transparency tools make AVs legible to both the system (via V2X/MaaS) and the public (via safety data). Digital infrastructure is equally critical. Interoperable, open data-sharing platforms allow AVs to communicate with public transport timetables, on-demand transit services, and adaptive traffic control systems [51]. In Helsinki, a citywide MaaS framework that required AV providers to share real-time availability and routing data through open APIs increased both fleet use and user uptake. Public visibility also plays an important role [52]. In Milton Keynes and Oslo, open-access trials with free ride days, school visits, and public information events have helped normalise AV presence and shift attitudes from skepticism to acceptance [53].

Policy pathway: Adopt infrastructure codes that ensure AV readiness, create secure but open data-sharing protocols, and require public engagement components in AV licensing processes.

4.4 Public motivation: Trust, equity and climate alignment

Trust and perceived value are shaped by what is deployed (shared versus private), where it operates, and how transparently it performs. Governments can institutionalise trust by routinely publishing disengagement and collision data, such as those reported by the California DMV, and by disclosing test locations through platforms like the NHTSA AV TEST Initiative. Independent safety audits should accompany each phase-gate so that public dashboards capture both inputs (exposure, operational design domain, fleet size) and outcomes (incidents per 1,000 km, mean time between disengagements) [47, 54]. The U.S. DOT's AV TEST Initiative illustrates how consistent and accessible performance data can help build public trust.

AV deployment can also be made more politically and socially acceptable when aligned with sustainability and equity objectives. In Oslo, AVs have been introduced into low-emission zones and underserved transit areas, allowing local governments to advance both climate goals and equitable mobility [55]. In Singapore, AV corridors are being developed as part of broader 'car-lite' strategies designed to complement rather than compete with public transport.

Policy pathway: Mandate independent safety audits with public reporting, prioritise deployments in underserved areas, and integrate AV strategies within low-carbon mobility frameworks.

4.5 Sequencing policy packages (COM-B integrated)

Effective strategies for AV adoption combine interventions across capability, opportunity, and motivation. Early implementation should focus on AV-ready street upgrades, public demonstrations, and transparent reporting dashboards. The mid-phase should integrate AVs into Mobility-as–a-Service (MaaS) platforms, establish open APIs and V2X systems, and introduce professional competency certification.

During scale-up, policy priorities should shift towards pricing and curb management, linked to SDG-based performance indicators such as mode share, vehicle kilometres travelled, and CO_2 per passenger-kilometre. **Table 2** synthesises global findings into a coherent set of policy pathways, drawing on examples from diverse urban contexts.

The main insight for policymakers is that capability, opportunity, and motivation are interdependent. Progress in one domain can be undermined if the others are neglected. For instance, advanced AV infrastructure will have limited value if public trust remains low or if regulators lack the expertise to manage complex mixed-traffic conditions.

COM-B domain	Sub-theme	Evidence base	Policy pathway	Example implementations
Capability	Public Knowledge and Digital Literacy	Nordhoff et al. [19]; Fonzone et al. [22]; Zhang et al. [49].	Embed AV literacy programmes into sustainable mobility campaigns, with community workshops and interactive trials.	*SOHJOA Finland* ran public engagement events with live AV rides; the *UK SCALE project* provided guided tours and Q&A sessions for local residents.
Capability	Professional Training for Planners and Operators	Milakis et al. [46]	Introduce AV competency frameworks into national transport curricula, supported by PPP-based professional training.	*Singapore Land Transport Authority*'s AV training for bus operators; *EU AVENUE project*'s training modules for city planners.
Opportunity	Physical Infrastructure Upgrades	DfT [10]; Fagnant and Kockelman [50]	Adopt AV-ready infrastructure standards in road codes, requiring consistent markings, upgraded signage, and V2X integration.	*Melbourne Connected Corridors* upgraded road markings and installed C-ITS beacons; *Japan's Smart Intersection programme* integrated AV sensor networks.
Opportunity	Digital Infrastructure and Data Sharing	Taamneh and Makahleh [12]; Wong et al. [56].	Establish open mobility data standards and shared V2X platforms to facilitate AV–infrastructure coordination.	*Barcelona City OS* platform sharing AV data feeds; *US Smart Columbus* project's open-data portal for connected mobility.
Motivation	Public Trust and Safety Perceptions	Nordhoff et al. [17]; Nordhoff et al. [20].	Implement transparent safety reporting and public dashboards on autonomous vehicle (AV) incident data.	California DMV *publishes AV disengagement and collision reports;* examples include trials that publish high-level safety summaries.
Motivation	Environmental and Social Value Alignment	Acheampong and Cugurullo [47]; Schaller [57].	Align AV deployment with low-carbon mobility targets, integrating them into public transport networks.	*Oslo's zero-emission transport plan,* incorporating AV feeder services; *Singapore's AV corridors* linked to MRT stations.

Table 2.
Policy pathways for autonomous vehicle adoption in urban mobility (structured using the COM-B framework).

5. Critical discussion and implications for policy and practice

The worldwide evidence based on AVs and, more specifically, on the introduction of AS in urban environments is now both large and diverse. The findings of the systematic review that inform this chapter, therefore, represent a wide-ranging and reliable picture of peer-reviewed academic evidence on AV adoption pathways that has been published to date, over the 2003–23 period. However, drawing policy-relevant lessons from the review findings presented in this chapter is a somewhat more challenging task, requiring subjective judgements to be made by the author about the meaning of the evidence. As such, this chapter briefly reflects on key themes within three related areas: (i) the extent to which pathways to current AV deployment are likely to prove realistic; (ii) the key implications for governance and multi-level coordination; and (iii) the conditions that would need to be met for AV adoption pathways to align with wider sustainability and climate change goals.

5.1 Reconciling technological readiness with policy ambition

While trials like SCALE in Birmingham, CAVForth in Edinburgh, and Milton Keynes' StreetCAV have proven technically possible, academic research has identified a continuing 'mismatch' between levels of technological readiness and policy readiness [12, 46]. Timelines in many national AV strategies for planned AV deployments rarely account for the experimental and often cyclical nature of technology refinement, public buy-in, and regulatory calibration. The COM-B pathways highlighted in Section 4, around building capability and public trust, for example, also indicate that rolling out without continued engagement can damage public confidence and heighten safety concerns [17, 19].

Policy should be adaptive, adjusting timelines to operational learning and public expectations. Examples from countries like Singapore and Finland show that small-scale, publicly transparent pilot phases can provide a more sustainable basis for long-term roll-out than national targets.

5.2 Governance complexity and the need for multi-level coordination

The AV adoption is not just a transport engineering problem but a multisector governance issue. The global evidence synthesis has highlighted the policy pathway towards policy coherence at municipal, regional, and national government levels, each with its own distinct but aligned responsibility [47, 58]. The local government may be responsible for aspects of the street network, curb space, and local public transport integration, while the national government sets regulations, safety, and data governance rules.

In practice, there is evidence from Europe, North America, and East Asia that incoherent policy approaches between levels of government can hold back or derail AV policy and project plans. For instance, there have been cases in the United States where cities have taken the lead in enabling AV pilots, but their state-level regulators have followed slowly, leading to legal uncertainty and, thus, reticence around scaling up AV projects. Japan has a relatively harmonised national–local policy approach for AVs through the promotion of AV deployment in smart city investment zones [59]. Evidence from recent simulation-based studies indicates that realising such benefits in practice depends on supportive and coordinated

policy frameworks rather than technical performance alone [60]. This justifies a number of governance-related pathways to be incorporated into **Table 2** (in the Opportunity domain), since AV infrastructure build-out and data-sharing and privacy policies require a long-term intergovernmental partnership approach.

5.3 Public acceptance as a dynamic, context-dependent process

Acceptance is not fixed, and it can change with familiarity, over time, through lived experience, and through trust-building activities [19, 22]. Acceptance of AVs, as is well documented in the behavioural literature, may have significant 'trial effects', that is, a change in public attitudes after user experience, but such effects may wear off in the absence of reinforcing or follow-on activities. For example, both the Finnish (SOHJOA) and UK trials (SCALE) have reported an increase in acceptance after the trials, although it is not clear how long such effects last or how much overpromising on the features of the technology or underplaying known limitations can backfire. This could be especially the case in early adopter contexts.

The COM-B model's Motivation pathways speak to this, highlighting transparency and safety reporting, as well as setting an appropriate environmental frame, as critical. The implication for policy is that acceptance cannot be built on one-off activities but needs to be regularly measured and appropriately targeted to manage issues as they arise.

5.4 Aligning AV policy pathways with sustainability and climate goals

One of the clearest messages in the international literature is that AVs are not a sustainability win by default [57]. Without specific design and policy, their deployment could add to VKT and the transport system's overall congestion, emissions, and resource intensity. The Motivation domain in **Table 2**, therefore, also includes pathways that clearly link AVs to a zero-emission transport strategy and to other components of public transport, such as feeders to public transport stops.

Both Oslo's zero-emission strategy and Singapore's AV corridors are examples of this principle. In Oslo, the city's zero-emission strategy requires that AV pilots be dedicated feeders to public transport, and Singapore's AV corridors connect to MRT stations rather than allowing point-to-point private travel. AV policy is, first and foremost, climate policy, and a large focus must be on making modal shift and decarbonisation clear and active goals in every phase of AV deployment.

5.5 From pathways to practice: Implementation challenges

Where the policy levers are feasible, they are also evidence-based. Not all are universally applicable, however. Constraints range from local authority capacity and fragmented financing to ambiguous long-term business models for commercial AV services. The uptake of AVs is also met with pushback by incumbents, operators' unions, and neighbourhood organisations that might stand to lose jobs or service levels.

Mitigating these risks calls for staged approaches that combine technical pilots with governance and institutional learning. This calls for built-in evaluation from the very start to ensure lessons are learned along the way and shared after the trial ends. The approach taken for the CAVForth trial governance, in which operationally-derived evidence contributed to adapting the Scottish bus service licensing rules, is an example of a policy feedback loop in action.

6. Acronyms and abbreviations

Autonomous vehicle (AV); autonomous shuttle (AS); automated driving system (ADS); behaviour change wheel (BCW); British Broadcasting Corporation (BBC); connected and autonomous vehicle (CAV); cooperative intelligent transport system (C-ITS); Department for Transport (DfT); electric vehicle (EV); focus group discussion (FGD); global positioning system (GPS); human–machine interface (HMI); information and communications technology (ICT); Intergovernmental Panel on Climate Change (IPCC); low- and middle-income country (LMIC); multi-level perspective (MLP); Paris Agreement (PA); rapid evidence assessment (REA); Society of Automotive Engineers (SAE); Sustainable Development Goals (SDGs); Theory of Planned Behaviour (TPB); Technology Acceptance Model (TAM); Transport for West Midlands (TfWM); United Nations (UN); University of Birmingham (UoB); United States (US).

7. Conclusions and forward-looking recommendations

Autonomous vehicle deployment is a socio-technical transition, not merely a technical upgrade. AV adoption will require a system-wide, multi-scalar approach. A policy coordination mechanism must combine technical and institutional innovation with infrastructure planning and investment, behavioural change management, and climate sustainability pledges.

Drawing on the global evidence synthesis (Section 4) and methodological learnings (Section 2), the section below highlights five key messages emerging from the evidence review and reflection. The adoption of AVs will not be an automatic process; it will be determined by design choices made by policymakers, transport operators, technology developers, manufacturers, and users. AV integration into the mobility ecosystem has often been 'messier' than anticipated. It is not a linear technological 'disruption'. In cities where AV adoption has made greater progress, such as in Singapore's structured trials and Lyon's AS in the Confluence district, there has been a judicious combination of clear governance structures, step-wise pilots, and built-in loops of learning and adaptation. The fact that progress has been slow and even regressive in some cases does not mean that AVs should not or cannot be adopted. It means that progress requires carefully planned and well-managed processes.

Public trust depends on reliability, safety, and transparent communication. Autonomous vehicle services are not just judged by their technological readiness but also by how they communicate operational protocols to the public and passengers. For example, the findings of Nordhoff et al. [17] and Fonzone et al. [22] show that participants in AV trials were significantly more likely to use the service again if they received adequate information before their ride and if the ride experience met their expectations. Passengers were also sensitive to how operators responded to their grievances and complaints.

Autonomous vehicles can be climate- and equity-friendly, or they can be not; it all depends on design choices. AV systems have the potential to increase mobility emissions (if they induce travel demand) or increase mobility exclusion (if they are only deployed in affluent neighbourhoods). These worst-case scenarios can be avoided by designing and implementing AV services as part of a broader Sustainable Urban Mobility Plan (SUMP) or in alignment with the Sustainable Development

Goals (SDGs), while using the SUMP performance and climate indicator checklist, along with the Paris Agreement framework, to track progress.

7.1 The strategic imperative

The policy pathways identified are not plug-and-play solutions and need to be sequenced, contextualised and evaluated on the ground. In the early stages of roll-out, priorities should include efforts to integrate AVs into existing transport systems so that they complement, rather than compete with, public transport and active modes [42]. Mid-development stage policies should respond to scaling issues, for example, through interoperability standards or with digital infrastructure. Longer-term strategies need to ensure that AV governance is institutionalised, aligned with urban planning, climate adaptation, and investment.

Across the various international case studies, a key message that emerged is the importance of having structured feedback loops between trials, research, and policy design. To this end, monitoring and evaluation need to be built in from the outset, as the UK Future Transport Zones evaluation framework suggests [10].

7.2 Policy recommendations

Drawing on the evidence discussed in this chapter, several practical steps can support more effective and equitable AV adoption. These steps need to be clear, actionable, and backed by examples of successful applications. **Table 3** summarises the chapter's findings into clear recommendations for decision-makers, with key actions, lead actors, priorities, and real-world examples showing how they can be applied.

Recommendation (What)	Key action (How)	Lead actors (Who)	Deployment priority*	Example implementation
Embed AVs within sustainability strategies	Integrate AV planning into Sustainable Urban Mobility Plans (SUMPs) and link it to climate targets.	Transport ministries; metropolitan planning authorities	**Short term** (1–2 yrs)	Singapore's AV trials are integrated into the Land Transport Master Plan.
Cultivate public trust and transparency	Publish real-time safety data; organise co-design workshops with residents.	City governments, AV operators, civil society groups	**Short term**	Helsinki's Robo-Bus trials with public dashboards
Coordinate multi-level governance	Create inter-agency AV taskforces; harmonise vehicle certification and data-sharing standards.	National transport regulators; city councils	**Medium term** (3–5 yrs)	EU's CCAM Partnership governance model
Advance AV-ready infrastructure	Upgrade road markings, digital mapping, and 5 G coverage in trial corridors.	Infrastructure agencies; telecom providers	**Medium term**	South Korea's AV-ready 'K-City' test bed
Promote equity and access	Prioritise deployment in underserved areas; integrate AV fares into public transport ticketing systems.	Local authorities; transit agencies	**Medium term**	Detroit's neighbourhood AV shuttle programme.

Recommendation (What)	Key action (How)	Lead actors (Who)	Deployment priority*	Example implementation
Anchor AVs to climate accountability	Conduct lifecycle carbon impact assessments; incentivise shared-ride AV services.	Climate agencies; urban transport planners	**Medium term**	Lyon Confluence AV project with mode-shift targets.
Secure sustainable finance models	Implement public–private partnership frameworks; test demand-based pricing.	Transport ministries; investors; technology partners	**Long term** (5 + yrs)	Dubai RTA–Cruise LLC partnership.

**Priorities are indicative and should be adapted based on local readiness and capacity.*

Table 3.
Strategic recommendations for sustainable AV integration in urban mobility.

7.3 Forward look

Implemented with equity and inclusion in mind, these actions can help cities move from pilots to resilient, climate-aligned mobility systems. As previous transport innovations have shown, be it electric buses in Shenzhen or bus rapid transit in Bogotá, it is not the technology in and of itself that is transformative. Rather, it is the interplay between the technology, policy frameworks, and people that determines whether an innovation is worth it.

In the coming decade, AV policy and strategy will increasingly become entangled with other aspects of urban policymaking, be it housing and growth, climate resilience and adaptation, or digital and data governance. Policymakers and city leaders who prepare now for AVs to be one part of the urban transformation agenda have an opportunity to steer AVs towards sustainable solutions.

Acknowledgements

The author would like to acknowledge the School of Engineering at the University of Birmingham for its academic support, research resources, and guidance throughout the development of this work.

Conflict of Interest

The author declares no conflict of interest.

Notes/thanks/other declarations

The author wishes to express sincere gratitude to Dr. Emma Ferranti and Dr. Dilum Dissanayake for their invaluable guidance, constructive feedback, and encouragement throughout the research process.

Author details

Hisham Y. Makahleh
School of Engineering, University of Birmingham, Birmingham, UK

*Address all correspondence to: hxm298@bham.ac.uk

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] SAE International. Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles [Internet]. 2021. Available from: https://www.sae.org/standards/content/j3016_202104/ [Accessed: 2025-Febraury-13]

[2] NHTSA. Automated Vehicles for Safety [Internet]. 2023. Available from: https://www.nhtsa.gov/vehicle-safety/automated-vehicles-safety [Accessed: 2025-April-12]

[3] NHTSA. Levels of Automation [Internet]. 2023. Available from: https://www.nhtsa.gov/document/levels-automation [Accessed: 2025-April-12]

[4] Zenzic. Self-driving shuttle route goes live in Solihull [Internet]. 2025. Available from: https://zenzic.io/news/self-driving-shuttle-route-goes-live-in-solihull/ [Accessed: 2025-April-12]

[5] ADAS & Autonomous Vehicle International. SCALE self-driving shuttle trial begins in Birmingham, UK [Internet]. 2025. Available from: https://www.autonomousvehicleinternational.com/news/mobility-solutions/scale-self-driving-shuttle-trial-begins-in-birmingham-uk.html [Accessed: 2025-June-22]

[6] Innovate UK. SCALE [Internet]. 2025. Available from: https://iuk-business-connect.org.uk/projects/connected-automated-mobility/scale/ [Accessed: 2025-April-13]

[7] ZENZIC. SCALE [Internet]. 2025. Available from: https://zenzic.io/innovation/deployment/scale/ [Accessed: 2025-April-14]

[8] Sunderland Our Smart City. 2023: Our year in smart city achievements [Internet]. 2023. Available from: https://www.sunderlandoursmartcity.com/2023-our-year-in-smart-city-achievements/ [Accessed: 2025-April-15]

[9] UK Department for Transport. Code of Practice: Automated Vehicle Trialling. London, UK: Department for Transport; 2023

[10] DfT. Implementation and Process Evaluation: Wave 1 Report National Evaluation of Future Transport Zones [Internet]. 2022. Available from: https://assets.publishing.service.gov.uk/media/66feb0f630536cb927482be2/dft-ftz-evaluation-ipe-wave-1.pdf [Accessed: 2025-April-13]

[11] Ohmio. The Future of Autonomous Transport [Internet]. 2025. Available from: https://www.ohmio.com/ [Accessed: 2025-June-13]

[12] Taamneh MM, Makahleh HY. The prospects of adopting electric vehicles in urban contexts: A systematic review of literature. Transportation Research Interdisciplinary Perspectives. 2025;**31**:101420

[13] Bankole SO, Donaldson D, Dissanayake D, Ferranti E, "Electric mobility in low- and middle-income countries: Preparedness from the consumer point of view," in IEEE PES/IAS PowerAfrica, Marrakech, Morocco, 2023

[14] Bankole SO, Dissanayake D, Donaldson DL, Ferranti E. Can electric shared mobility increase the effectiveness of feeder systems to bus

rapid transit stations in African cities? A systematic literature review. Transportation Research Procedia. 2025;**89**:414–438

[15] Makahleh HY. Traffic management implications of overtaking assistance automated vehicles mixed with human-driven vehicles. Advances in Traffic and Transportation Research. 2024;**2**(1):1–11

[16] Makahleh HY, Makahleh GY. Traffic management implications of cooperative automated vehicles mixed with regular vehicles on motorways. Modern Transportation. 2024;**13**(1):13184

[17] Nordhoff S, D. Winter J, Madigan R, Merat N, V. Arem B, Happee R. User acceptance of automated shuttles in Berlin-Schöneberg: A questionnaire study. Transportation Research Part F: Traffic Psychology and Behaviour. 2018;**58**:843–854

[18] Makahleh HY, Badrawi HA, Abdelfatah A. Assessing the impacts of autonomous vehicles for freeway safety. In: 10th World Congress on New Technologies (Newtech'24). Barcelona, Spain: Avestia Publishing; 2024. DOI: 10.11159/icceia24.153

[19] Nordhoff S, Winter JD, Kyriakidis M, Arem BV, Happee R. Acceptance of driverless vehicles: Results from a large cross-national questionnaire study. Journal of Advanced Transportation. 2018;**2018**:5382192. DOI: 10.1155/2018/5382192

[20] Nordhoff S, Kyriakidis M, Arem BV, Happee R. A multi-level model on automated vehicle acceptance (MAVA): A review-based study. Theoretical Issues in Ergonomics Science. 2019;**20**(6):682–710

[21] Fonzone A, Fountas G, Downey L. Automated bus services – To whom are they appealing in their early stages? Travel Behaviour and Society. 2024;**34**:100647

[22] Fonzone A, Fountas G, Downey L, Olowosegun A. How autonomous bus trials affect passengers' views: Exploring the gap between pre-ride expectations and real word experience. Transportation Research Part F: Traffic Psychology and Behaviour. 2025;**112**:115. DOI: 10.1016/j.trf.2025.07.021

[23] Nordfjærn T, Egset KS, Mehdizadeh M. "Winter is coming": Psychological and situational factors affecting transportation mode use among university students. Transport Policy. 2019;**81**:45–53

[24] Blumenfeld M, Roberts C, Schmid F. A systems approach to developing a new metro for megalopoleis. Proceedings of the Institution of Civil Engineers - Transport. 2016;**169**(5):249–261

[25] Blumenfeld M, Roberts C, Schmid F, "An operational strategy to increase average door-to-door speeds of metro systems in megalopoleis," in Transforming the Future of Infrastructure through Smarter Information: Proceedings of the International Conference on Smart Infrastructure and Construction, 27–29 June 2016, Cambridge, UK, ICE Publishing, 2016, p. 735–740

[26] Ferranti EJS, Oberling DF, Quinn AD. Transport resilience to weather and climate: An interdisciplinary view from Rio de Janeiro. Proceedings of the Institution of Civil Engineers - Urban Design and Planning. 2022;**175**(3):103–121

[27] Ferranti E, Andres L, Denoon-Stevens SP, Melgaço L, Oberling D, Quinn A. Operational challenges and mega sporting events legacy: The case of BRT systems in the global south. Sustainability. 2020;**12**(4):1609

[28] IPCC. Climate Change 2021: The Physical Science Basis. Cambridge, United Kingdom: Cambridge University Press; 2021

[29] IPCC. Climate Change 2022: Impacts, Adaptation and Vulnerability [Internet]. 2022. Available from: https://www.ipcc.ch/report/sixth-assessment-report-working-group-ii/ [Accessed: 2024-December-28]

[30] United Nations. THE 17 GOALS [Internet]. 2025. Available from: https://sdgs.un.org/goals [Accessed: 2025-April-14]

[31] Diba DS, Gore N, Pulugurtha SS. Integrating autonomous shuttles: Insights, challenges, and strategic solutions from practitioners and industry experts' perceptions. Future Transportation. 2025;**5**(1):9

[32] Makahleh HY, Taamneh MM, Dissanayake D. Promoting sustainable transport: A systematic review of walking and cycling adoption using the COM-B Model. Future Transportation. 2025;**5**(3):79

[33] Bastola A, Wang H, Boroujeni SPH, Brinkley J, Moshayedi AJ, Razi B. Driving toward inclusion: A systematic review of AI-powered accessibility enhancements for people with disability in autonomous vehicles. IEEE Access. 2025;**13**:61384–61415

[34] Janatabadi F, Ermagun A. Empirical evidence of bias in public acceptance of autonomous vehicles. Transportation Research Part F: Traffic Psychology and Behaviour. 2022;**84**:330–347

[35] Othman K. Exploring the implications of autonomous vehicles: A comprehensive review. Innovative Infrastructure Solutions. 2022;**7**:165

[36] Wiedyanoe S, Fonzone A, Cowie J, Utomo D. Exploring policy interventions to support the introduction of autonomous vehicles in Indonesia. Jurnal Ilmu Kepolisian. 2024;**18**(2):163–176

[37] Rahman MM, Thill J-C. Impacts of connected and autonomous vehicles on urban transportation and environment: A comprehensive review. Sustainable Cities and Society. 2023;**96**:104649

[38] Tao T, Cao J. Examining motivations for owning autonomous vehicles: Implications for land use and transportation. Journal of Transport Geography. 2022;**102**:103361

[39] Falagas ME, Pitsouni EI, Malietzis GA, Pappas G. Comparison of PubMed, Scopus, Web of Science, and Google Scholar: Strengths and weaknesses. The FASEB Journal. 2008;**22**(2):338–342

[40] Makahleh HY, Ferranti EJS, Dissanayake D. Assessing the role of autonomous vehicles in urban areas: A systematic review of literature. Future Transportation. 2024;**4**(2):321–348

[41] UNFCC. The Paris Agreement [Internet]. 2015. Available from: https://unfccc.int/process-and-meetings/the-paris-agreement [Accessed: 2024-December-28]

[42] Soteropoulos A, Berger M, Ciari F. Impacts of automated vehicles on travel

behaviour and land use: An international review of modelling studies. Transport Reviews. 2019;**39** (1):29–49

[43] Petticrew M, Roberts H. Systematic Reviews in the Social Sciences: A Practical Guide. New Jersey, U.S: Wiley; 2006

[44] Petticrew M. Time to rethink the systematic review catechism? Moving from 'what works' to 'what happens'. Systematic Reviews. 2015;**4**:36

[45] Oliver K, Lorenc T, Innvær S. New directions in evidence-based policy research: A critical analysis of the literature. Health Research Policy and Systems. 2014;**12**:34

[46] Milakis D, van Arem B, van Wee B. Policy and society related implications of automated driving: A review of literature and directions for future research. Journal of Intelligent Transportation Systems. 2017;**21** (4):324–348

[47] Acheampong RA, Cugurullo F. Capturing the behavioural determinants behind the adoption of autonomous vehicles: Conceptual frameworks and measurement models to predict public transport, sharing and ownership trends of self-driving cars. Transportation Research Part F: Traffic Psychology and Behaviour. 2019;**62**:349–375

[48] Michie S, Stralen MMV, West R. The behaviour change wheel: A new method for characterising and designing behaviour change interventions. Implementation Science. 2011;**6**(1):42

[49] Zhang Z, Liu J, Qian X, Guo S, Yang C, Jones S. Envisioning shared autonomous vehicles (SAVs) for 374 small and medium-sized urban areas in the United States: The roles of road network and travel demand. Journal of Transport Geography. 2025;**127**:104302

[50] Fagnant DJ, Kockelman K. Preparing a nation for autonomous vehicles: Opportunities, barriers and policy recommendations. Transportation Research Part A: Policy and Practice. 2015;**77**:167–181

[51] Coppola P, Silvestri F. 1 - Autonomous vehicles and future mobility solutions. In: Autonomous Vehicles and Future Mobility. Amsterdam, The Netherlands: Elsevier; 2019. p. 1–15

[52] MaaS MiddleEast. The 6 levels of driving automation explained [Internet]. 2024. Available from: https://maas-middleeast.com/the-6-levels-of-driving-automation-explained/ [Accessed: 2025-April-11]

[53] Lavieri PS, Bhat CR. Modeling individuals' willingness to share trips with strangers in an autonomous vehicle future. Transportation Research Part A: Policy and Practice. 2019;**124**:242–261

[54] Kyriakidis M, Happee R, Winter JD. Public opinion on automated driving: Results of an international questionnaire among 5000 respondents. Transportation Research Part F: Traffic Psychology and Behaviour. 2015;**32**: 127–140

[55] Pöllänen E, Read GJM, Lane BR, Thompson J, Salmon PM. Who is to blame for crashes involving autonomous vehicles? Exploring blame attribution across the road transport system. Ergonomics. 2020;**63**(5): 525–537

[56] Wong WF, Fuchs S. Multimodal transport networks. FRB Atlanta. 2022;13

[57] SCHALLER. The New Automobility: Lyft, Uber and the Future of American Cities. New York, USA: Schaller Consulting; 2018

[58] Stilgoe J, Cohen T. Rejecting acceptance: Learning from public dialogue on self-driving vehicles. Science and Public Policy. 2021;**48** (6):849–859

[59] Raimbault J, Batty M, "Estimating public transport congestion in UK urban areas with open transport models," in 29th GISRUK, Cardiff, Wales, UK, 2021

[60] Makahleh HY, Noaman M, Abdelfatah A. Evaluating the impact of autonomous vehicles on signalized intersections' performance. Smart Cities. 2025;**8**:181. DOI: 10.3390/smartcities8060181

Chapter 3

Cooperative Driving and Collective Navigation Architectures for CCAVs: Contemporary Techniques, Simulators, Datasets, and Research Directions

Kenan Ahiska

Abstract

As vehicle-to-vehicle and vehicle-to-infrastructure technologies evolve, connected and cooperative autonomous vehicles (CCAVs) become a feasible solution for traffic problems with their shared and collective navigation and collaborative driving policies to globally optimize safety and efficiency. This chapter covers the architectures in autonomous driving and autonomous navigation of CCAVs. Multi-agent reinforcement learning-based autonomous driving techniques and deep-learning-based end-to-end cooperative driving solutions are investigated. Intermediate fusion schemes for autonomous navigation, and in particular transformer-based collective navigation architectures of CCAVs, are examined. Popular simulators and datasets used in the development and benchmarking of the autonomous driving and navigation architectures of CCAVs are analyzed. Future research directions are discussed.

Keywords: connected and cooperative autonomous vehicles, cooperative driving, end-to-end autonomous driving, multi-agent reinforcement learning, collective perception, collective navigation, transformer-based intermediate fusion, simulator, dataset

1. Introduction

Autonomous vehicles (AVs), with limited or no human control in driving, represent the current and transformative change in automotive technologies. Using autonomous driving or autonomous vehicles eliminates human-driven risk factors and makes it possible to mitigate traffic congestion, increase accessibility, improve road safety, and provide energy-efficient driving [1]. In the context of autonomous vehicles, the control decision of the vehicle is made according to the inputs from the on-board sensors of the vehicle, such as cameras, LiDAR, etc. The driving

pipeline consists of perception, planning, and control parts, and in autonomous vehicles, deep learning-based techniques are used either in the perception section of the pipeline or replace the whole pipeline in an end-to-end approach.

Nevertheless, single-vehicle autonomous driving can fail to satisfy safety concerns due to its limited perception range and incapability to acquire information about the road, traffic, and other agents in the neighborhood. Connected and cooperative vehicles (CCAVs) is an integration of AVs to share sensor inputs and decisions through vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), or vehicle-to-everything (V2X) technologies. CCAVs benefit significantly from extended and collective navigation solutions, as well as collaborative decision-making in the planning and control of the vehicles. CCAVs can be considered a solution to improve traffic safety and energy-efficient driving, with a joint performance of perception, communication, computing, and control [2].

Autonomy of CCAVs, similar to the autonomy of AVs, can be considered to achieve three main tasks: perception/navigation, planning, and control; however, in the CCAV context, collaboration is possible: collective perception/navigation, cooperative planning, and cooperative control. The autonomous driving of CCAVs aims at achieving cooperation in all or some parts of this modular pipeline. The autonomous navigation of CCAVs means achieving a collective perception/navigation solution in the first module of the pipeline. Autonomy in CCAVs is not just about sharing information between vehicles but realizing collective perception and behavior for harmony and safety in traffic.

Deep learning-based solutions in cooperative driving of CCAVs relax the precise system modeling and high computational power requirements of the conventional control techniques used in the modular pipeline solutions for autonomous driving of CCAVs [3]. Multi-agent reinforcement learning (MARL) has been shown to be successful in optimizing collective decision-making and has been studied for autonomous driving of CCAVs [4]. End-to-end autonomous driving approaches, where the raw sensor data are directly mapped to control signals of vehicles in a CCAV group, is another contemporary method in autonomous driving of CCAVs, and it is especially good at aiming to optimize the whole pipeline into a driving policy in harmony [5].

Collective navigation tackles the problems of single-agent perception regarding occlusions, sparse observations at far distances, or limited sensor range, and it provides a robust online mapping solution. Either the raw sensor data, features extracted from these data, or the navigation solution, such as poses of surrounding objects, are shared between vehicles and infrastructure. Sharing raw sensor data necessitates high communication costs, while sharing navigation solutions results in poor-quality context [6]. Collective navigation tries to fuse data and generate a scene from the observations of the same scene from multiple viewpoints with different types of sensors. Considering the image patches as words and benefiting from attention mechanisms, transformer-based collective navigation solutions are successful at solving this heterogeneous multi-view sensor fusion problem [7].

The development and benchmarking of algorithms designed for autonomous driving or navigation require multi-view and multi-modal data. Real-world datasets are available but limited. Simulated datasets are often used, and simulators with different capabilities are employed to generate these datasets. Simulators have varying properties and strengths in specific test scenarios or interfaces tailored for specific algorithms. Adverse weather conditions and communication limits often

create a gap between real-world data and simulated data, which is an important issue for researchers.

This chapter, in a very summarized manner, provides the current trends in cooperative driving and collective navigation of CCAVs. In Section 2, cooperative driving architectures are investigated, including those based on MARL in Section 2.1 and end-to-end autonomous driving schemes for CCAVs in Section 2.2. In Section 3, collective navigation architectures, in particular intermediate fusion schemes, are examined. Transformer-based collective navigation solutions are studied in Section 3.2, while more general deep-learning-based schemes for intermediate fusion are covered in Section 3.1. In Section 4.1, the most popular simulators used in the CCAV context are investigated, while in Section 4.2, real-world and simulated datasets used for benchmarking the algorithms are analyzed. The chapter concludes with Section 5, where research directions are discussed.

2. Cooperative driving of connected and cooperative autonomous vehicles

The cooperative driving of CCAVs can be summarized as making joint optimal driving policies based on a collective navigation solution shared among the collaborating agents in the neighborhood using inter-vehicle communication and the infrastructure [8]. A hierarchical solution, namely the pipeline of perception, planning, and control modules, is a straightforward solution for cooperative driving [9]; nevertheless, this solution requires precise modeling and substantial computational power. Hence, for real-time applications, it is often infeasible [3].

Reinforcement learning (RL) is very successful in sequential decision-making, and Multi-agent reinforcement learning (MARL) extends these capabilities into making joint optimal decisions for multiple agents. In Section 2.1, recent studies on cooperative driving using MARL in scenarios where cooperation is essential are presented.

End-to-end cooperative driving maps the raw sensor input from different vehicles and infrastructure into control commands for these vehicles directly using V2V and V2I communication. Compared to single-agent end-to-end autonomous driving, cooperative solutions do not suffer from occlusions or multi-agent intersection-related problems and jointly plan the trajectories and policies of the agents. End-to-end approaches eliminate the limits on scalability and adaptability of modular pipelines [5]. Recent works on deep learning-based end-to-end cooperative driving solutions are detailed in Section 2.2.

2.1 Multi-agent reinforcement learning for cooperative driving

In this section, Multi-agent reinforcement learning (MARL) applications for cooperative driving are investigated. In cooperative driving with MARL, each vehicle is considered an agent and learns from its interactions with the environment not only to travel safely but also to cooperate with other vehicles and the infrastructure. A categorization in terms of the dimension of cooperative motion can be made: one-dimensional (lateral control, longitudinal control), two-dimensional (lane changing), or three-dimensional (time-limited motions such as on-ramp merging, traffic signal control, unsignalized intersections) [10]. Below, selected recent studies on these scenarios are listed.

For the CCAV platooning problem (one-dimensional) in [11], a long short-term memory (LSTM)-based robust communication protocol is used as a MARL approach with individual and global rewards, achieving stable platooning control. For the same problem, in [12], the following vehicles are considered as a collection, and a distributed proximal policy optimization (DPPO)-based MARL approach with a quadratic reward function is employed to overcome the drawbacks of centralized optimization in high-mobility urban traffic scenarios.

For the cooperative lane change problem (two-dimensional) in [13], a zero-sum deep Q-network (DQN)-based MARL approach is used to achieve harmonious driving, where a balance between individual and overall efficiency is achieved using limited sensor data. For the same problem, in [14], MARL is based on the multi-agent advantage actor-critic (MA2C) framework, where a new design for local reward is proposed as a parameter-sharing mechanism. The reward function is multi-objective, including fuel efficiency, safety, and driving comfort, and successful cooperative lane changing was achieved.

For the traffic signal control problem (three-dimensional), in [15], a decentralized coordination multi-agent DQN is proposed to overcome issues related to the dimensionality and nonstationarity of the environment. A CCAV state space decomposition into independent and coordinated parts is constructed, and explicit identification and dynamic adaptation of agent coordination during the learning process are achieved. For the same problem, in [16], a cooperative group-based multi-agent Q-learning for ATSC (CGB-MATSC) is employed to improve the learning process, where the joint state representation for close agents is grouped with k–NN, a pheromone-based strategy is created to match with local green-wave flow, and the reward is discounted spatially.

For the on-ramps merging problem (three-dimensional) in [17], together with an action masking scheme, parameter sharing and local rewards are used to achieve cooperation in the MA2C framework. Potential collisions are avoided preemptively using a priority-based safety supervisor. For the unsignalized intersections problem (three-dimensional) in [18], QMIX, a value decomposition-based MARL approach, is proposed, where an end-to-end learning scheme for autonomous learning of the complex scenarios is achieved with an adaptive curriculum through self-play training.

2.2 End-to-end deep learning approaches for cooperative autonomous driving

In this section, for connected and cooperative autonomous vehicles, end-to-end deep learning-based cooperative driving approaches are examined. For a single autonomous vehicle, end-to-end autonomous driving approaches train neural networks that map the raw sensor data directly to the driving commands [19]. The single-vehicle end-to-end autonomous driving approaches cannot eliminate problems related to occlusions and multi-agent intersections. End-to-end cooperative autonomous driving, which is also the scope of this section, overcomes these issues.

Using V2V communication, end-to-end self-driving performance can be enhanced. In [20], between two cooperative self-driving vehicles, image data were shared, and for the lane change maneuver, the steering angle is controlled. Convolutional neural network (CNN), long short-term memory (LSTM), and fully connected (FC) layers are concatenated to produce image inputs for the steering angle commands. The tests are performed on the Udacity dataset.

Using a similar network architecture, in [21], the end-to-end cooperative autonomous driving problem is solved for CCAV platoons, not only for the following vehicle but also for the leading one in challenging urban environments. In this paper, instead of sharing a high-level image stream, the states of the vehicles are shared. The network takes the state of the other vehicle and ego-sensor data and generates control commands, either in the case of the leading vehicle or the following vehicle. The tests are performed on Town01 and Town02 of the CARLA simulator.

CooperNaut [22] is an end-to-end V2V cooperative autonomous driving architecture. It generates features from point clouds produced by different vehicles using decentralized fusion to improve perception and employs a CNN network to optimize planning and control outputs. As a pioneering study addressing this problem, it exhibits relatively poor trajectory planning performance and lacks solutions for safety and interpretability, which are especially important in urban environments. The paper conducted its simulations using the AutoCastSim tool, which is also introduced in the paper.

UniV2X [23] is an end-to-end cooperative autonomous driving architecture using V2V and V2I collaboration. The proposed pipeline includes agent perception, object detection, and tracking, as well as motion forecasting seamlessly. Considering effectiveness, reliability, and transmission-friendliness, a sparse-dense hybrid transmission framework and cross-view data interaction are implemented for spatial awareness and scene coverage. The method is based on deep learning models, resulting in poor performance in cases of semantic richness and heterogeneous multi-perspective inputs. The tests are performed on DAIRV2X dataset.

V2X-VLM [24] is another end-to-end cooperative autonomous driving approach proposed to use semantic alignment by unifying heterogeneous multi-modal data within a large vision-language model (VLM) backbone. Higher performance in trajectory planning and collision avoidance has been achieved. Interpretable and context-aware planning was proposed using the knowledge distillation and contrastive learning capabilities of the method. Tests were performed on the DAIR-V2X dataset.

SEAL [5] is an extension to V2X-VLM, including adaptive complex weather modeling. For adverse weather conditions, a scalable and photo-realistic data generation infrastructure is proposed to ease the training, and for these conditions, a gated multi-scenario adaptive attention (GMSAA) mechanism is built to modulate feature representations dynamically. The proposed method uses a multi-task scenario-aware contrastive learning (MSCL) objective to enforce separation between different long-tail scenarios. The tests are performed on DAIR-V2X and V2X-Real datasets, used together with GPT-4.0 for adverse weather condition adjustments.

In **Figure 1**, the differences and improvements from the traditional pipeline to the contemporary end-to-end deep learning-based cooperative driving architectures for CCAVs are presented.

3. Collective navigation of connected and cooperative autonomous vehicles

As V2V and V2I communication capabilities improve rapidly, collective navigation solutions, where the vehicles share their navigation data – either raw sensor input or navigation solution – become feasible [25]. An overview of collective

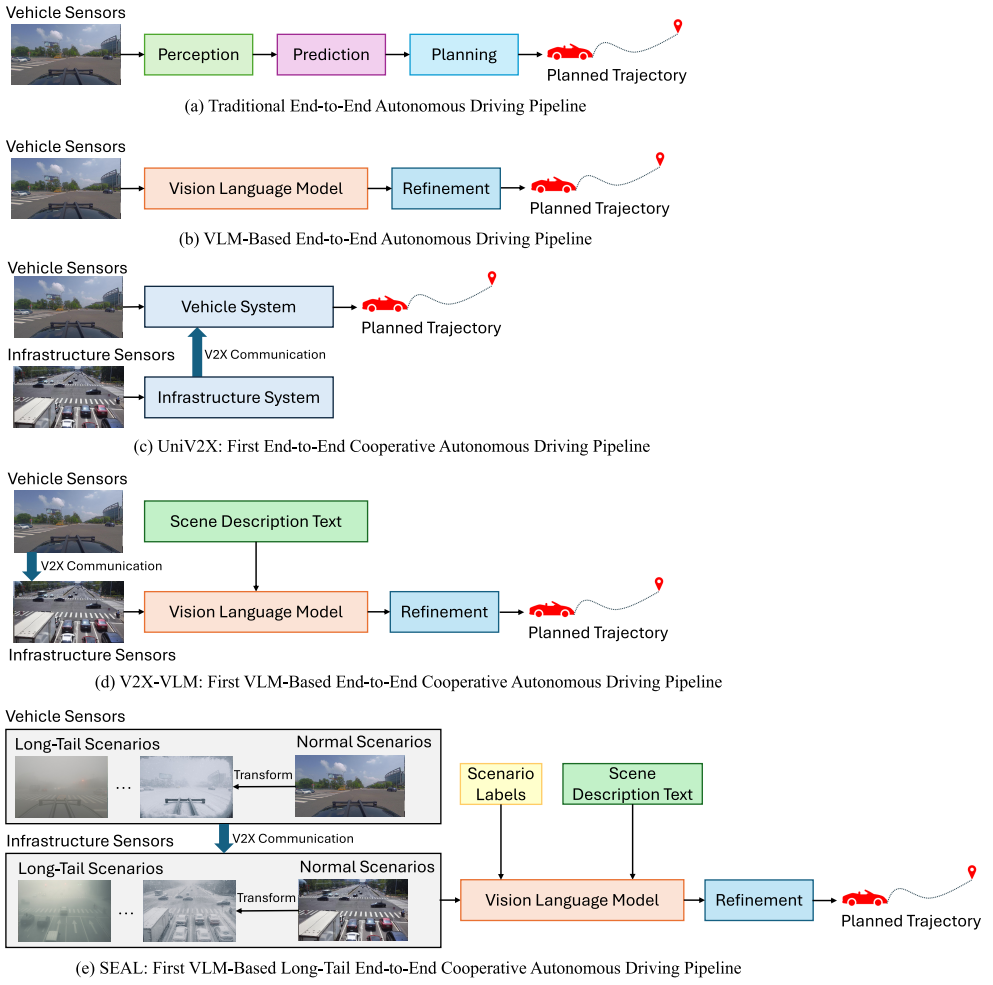


Figure 1.
Evolution of the end-to-end cooperative driving architectures for CCAV: (a) Traditional pipeline, (b) VLM-based framework (single autonomous vehicle), (c) Univ2x [23] cooperative end-to-end autonomous driving without semantic alignment, (d) V2X-VLM [24] cooperative end-to-end autonomous driving with semantic alignment and heterogeneous data, and (e) SEAL [5] cooperative end-to-end autonomous driving with semantic alignment and heterogeneous data enhanced for complex weather conditions [5].

navigation in connected and cooperative autonomous vehicles is presented in **Figure 2**. There are three strategies for collective navigation: early fusion, intermediate fusion, and late fusion.

In early fusion, the raw sensor data (images or point cloud) are shared between vehicles. A comprehensive and holistic perception is formed [27, 28] either using a centralized approach [29], or a hetero-modal (LiDAR and RGB images) ego-perception can be used in fusion [30]. However, early fusion necessitates a large transmission bandwidth.

In late fusion, detection outputs (perception results such as bounding box positions) are shared between the vehicles [31, 32]. The scheme simply involves merging different sensor outputs at the decision level [33, 34]. Although practical

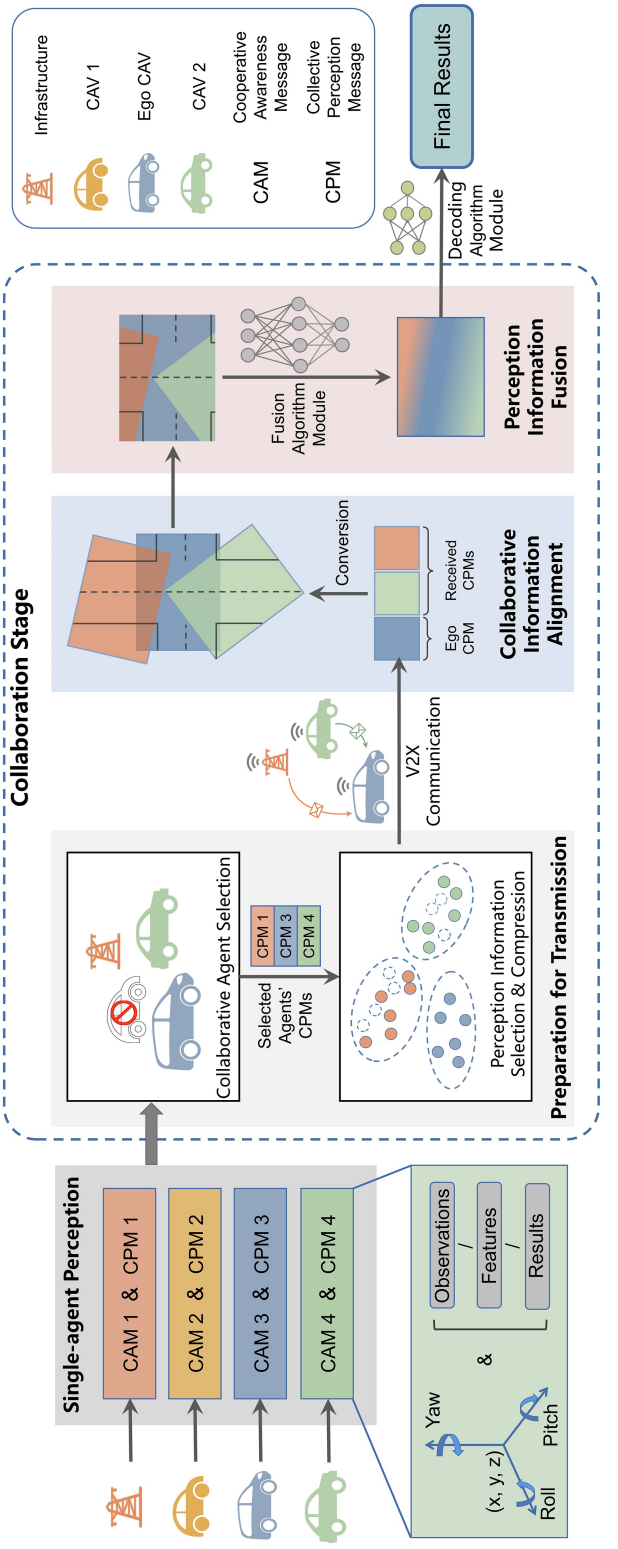


Figure 2.
Overview of collective navigation in connected and cooperative autonomous vehicles [26].

and flexible, late fusion often encounters association problems, resulting in error accumulation and poor-quality output context [35].

In intermediate fusion, as an option providing a balance between context quality (performance) and transmission bandwidth, intermediate neural features are extracted and shared between the vehicles. Intermediate fusion appears to be the main scheme in the collective navigation of CCAVs. In the following subsections, contemporary intermediate fusion architectures and transformer-based intermediate fusion architectures are investigated in more detail.

3.1 Intermediate fusion architectures

Intermediate fusion has emerged as a particularly effective compromise between communication cost and perceptual accuracy, wherein each vehicle encodes its raw sensor data into intermediate features, which are then transmitted to neighboring vehicles for fusion. This approach avoids the heavy bandwidth demands of raw data transmission (as in early fusion) while providing richer contextual understanding than the object-level decisions used in late fusion. Recent research has explored different architectures for intermediate fusion, including spatial alignment techniques, attention mechanisms, and graph-based learning strategies. In **Table 1**, four prominent works that propose or evaluate such fusion mechanisms are compared.

Paper/ method	Fusion level	Fusion mechanism	Data type shared	Bandwidth efficiency	Performance impact	Unique strength
V2VNet [35]	Intermediate fusion	Feature-level fusion using spatial transformation and encoder-decoder CNN	Compressed deep feature maps	High efficiency	Improved detection under occlusion and extended range.	Good trade-off between accuracy and bandwidth.
OPV2V [36]	All levels benchmarked	Benchmarks 16 pipelines; proposes Attentive Intermediate Fusion.	LiDAR point clouds (simulated and compressed)	Evaluated under compression constraints	Enables benchmarking of fusion strategies and robustness.	Provides a large-scale open dataset and an Attentive Fusion baseline.
F-Cooper [37]	Intermediate Feature Fusion	Shares compact BEV features; merges with ego vehicle.	Compact 3D point cloud features	Low latency (71 ms)	10% gain at 20 m, up to 30% at longer ranges.	Focus on real-time feasibility for edge computing.
DiscoNet [38]	Learned graph-based fusion	Teacher-student setup: learned collaboration graph with matrix-valued attention.	Pose-aware attention graph over shared features	Efficient due to selective collaboration	Near teacher-level performance with reduced communication.	Uses matrix-valued attention to learn adaptive inter-agent importance.

Table 1.
Comparison of intermediate fusion architectures.

V2VNet [35] employs a spatial-aware graph neural network to combine the shared neural features. It uses compressed feature maps, ego-centric spatial alignment, and learned attention fusion. The method balances accuracy and bandwidth, handles occlusions, and extends the detection ranges, whereas it also requires accurate spatial registration and comes with a moderate compute cost.

OPV2V [36] presents the first large-scale open simulated dataset and benchmarks 16 fusion strategies (early, intermediate, late) with various LiDAR detectors, proposing an attentive intermediate fusion method that performs well even under high compression. The paper employs an agent-wise single-head self-attention mechanism to fuse the features.

F-Cooper [37] shares point cloud features between vehicles, generated with a lightweight CNN decoder, and enables real-time edge computing with low latency (71 ms). This framework shows roughly 10% detection gains within 20 meters and up to 30% improvements at longer distances, while preserving privacy.

DiscoNet [38] uses knowledge distillation to improve training by limiting the features to those from the network for early fusion. The method utilizes a teacher–student setup: the teacher has holistic (joint) inputs, while the student uses single-view inputs plus a learned, pose-aware "Collaboration Graph" (DiscoGraph) that highlights important regions via matrix-valued attention. The distilled student (DiscoNet) achieves nearly teacher-level performance with better bandwidth efficiency. The method is evaluated on the V2X-Sim dataset.

3.2 Transformer-based intermediate fusion architectures

Vision Transformers (ViT) consider image patches as visual words, and the self-attention mechanism can then be directly applied to images [39]. Full self-attention brings high computational complexity and performs poorly in long-range sequences. Locality in self-attention overcomes this issue and provides improved flexibility, as proposed in Swin Transformer [40, 41]. Sparse attention [42], pyramidal design [43], and enlarged receptive fields [44] are offered as improvements to attention model architectures.

V2X-ViT [7] lays the foundational work in multi-agent Vision Transformer for V2X communication. It uses two novel attention modules: Heterogeneous Multi-Agent Self-Attention (HMSA) to model interactions across agent types (vehicles and infrastructure) and Multi-Scale Window Attention (MSwin) to capture local and global spatial feature interactions in parallel. The paper addresses challenges such as asynchronous inputs, pose errors, and sensor heterogeneity. The tests are performed on CARLA/OpenCDA datasets.

CoBEVT [45] focuses on cooperative semantic segmentation from a bird's-eye view, employing sparse transformers to efficiently process multi-agent, multi-camera data, enhancing the understanding of spatial environments. CoBEVT exploits sparse attention for efficient, real-time BEV segmentation in cooperative multi-camera settings. The fused axial attention (FAX) module captures both local and global spatial interactions across cameras and agents efficiently. The paper achieves state-of-the-art (SOTA) performance on OPV2V and nuScenes for BEV semantic segmentation, with real-time inference, and is generalizable to single-agent and LiDAR-based tasks.

CoFormerNet [6] addresses the challenge of spatial discrepancies in LiDAR data between vehicles and infrastructure. It uses affine coordinate transformations to

align feature maps, a multi-head cross-attention mechanism for effective fusion, a unified positional encoding (aligning infrastructure and vehicle coordinates), and spatial-modulated cross-attention (SMCA) with Gaussian masks to focus attention around object queries and mitigate calibration errors. The paper explicitly targets spatial inconsistency, improves bounding-box prediction accuracy, and speeds up training.

HM-ViT [46] introduces a unified multi-agent framework for hetero-model cooperation (e.g., LiDAR + camera) between vehicles, modeling complex inter- and intra-agent relationships. It employs sparse heterogeneous local and global attentions, utilizing a heterogeneous 3D graph Transformer. The paper presents the first framework supporting cross-modal V2V cooperation and demonstrates performance gains on the OPV2V dataset.

A short summary of the comparison of the transformer-based intermediate fusion architectures is presented in **Table 2**.

4. Simulators and datasets

4.1 Simulators

In this section, popular simulators used in studies on CCAV autonomous driving and autonomous navigation are summarized and analyzed. These simulators are used to replicate real-world conditions and serve as safe and cost-effective alternatives to real-world testing [47]. The simulators also provide a learning platform, presenting infrastructure to impose different challenges for CCAV autonomy: various traffic scenarios and challenging agent characters with in a framework encompassing realistic models and sensors, communication infrastructures, and traffic conditions [28]. A summary of the comparison of the popular simulators is presented in **Table 3**.

Car Learning to Act (CARLA) is an open-source urban driving simulator. It has a high-fidelity 3D environment model with realistic weather, lighting, and traffic conditions. CARLA supports multiple autonomous agents, both in vehicle and pedestrian form. The simulator provides multiple sensor suites: LiDAR, RGB

Paper	Data modality	Application focus	Key technique	Strengths
V2X-ViT [7]	Multi-agent imagery	V2X object detection	HMSA and MSwin attention modules	Robust to pose errors and asynchronous heterogeneous inputs
CoBEVT [45]	Camera-based BEV	BEV semantic segmentation	FAX sparse attention across views/agents	SOTA performance; real-time; generalizable
CoFormerNet [6]	LiDAR (infra + vehicle)	Object detection in V2I	SMCA, affine transforms, unified positional encoding	Handles spatial misalignment effectively
HM-ViT [46]	Heterogeneous modalities	V2V object detection	3D graph Transformer for hetero-modal fusion	Cross-modal collaboration innovation

Table 2.
Comparison of transformer-based intermediate fusion architectures.

Simulator	Simulation type	Key features	Connectivity support	CCAV support	Integration-APIs	Use case focus
CARLA [48]	3D, physics-based	Realistic sensors, dynamic weather, urban scenes, ROS/Autoware support	Partial (via ROS or plugins)	Limited (single-agent, extendable via APIs)	Python API, ROS, Autoware	AV research, sensor validation, perception
SUMO [50]	Microscopic traffic simulator	High-speed traffic flow simulation, V2X protocol emulation, signal control	Strong (V2X protocols, TraCI interface)	Yes (multi-agent traffic logic)	TraCI (Python, C++, OMNeT++)	Traffic modeling, network-scale CCAV, V2X
LGSVL (SVL) [54]	3D, physics-based	Accurate sensors, map import (HD maps), Apollo/Autoware-ready	Yes (via ROS Bridge, V2X via extensions)	Yes (multi-agent, ROS-based CCAV)	ROS/ROS2, Apollo, Autoware, Unity backend	AV system integration, CCAV coordination
CityFlow [57]	Microscopic traffic simulator	High-speed multi-intersection traffic simulation, RL integration	Partial (extendable with custom APIs)	Basic (focused on signal-level control)	Python API, open-source for RL agents	RL for signal control, large-scale traffic optimization
Apollo CyberRT [60]	Middleware + Sim tools	Modular real-time robotic framework used with the Apollo simulation platform	Yes (supports V2X modules via CyberRT)	Yes (full CCAV support via Apollo stack)	CyberRT API (C++), ROS-like architecture	Real-time AV systems, V2X middleware, Apollo stack
MetaDrive [62]	3D + procedural driving Sim	Lightweight, procedural scenes, RL multi-agent environments	Partial (via APIs)	Yes	Python API, Stable-Baselines3	RL for driving, multi-agent planning

Table 3.
Comparison of simulators used in CCAV.

cameras, GPS, and IMU. Furthermore, CARLA supports V2V and V2I communication simulation through plugins or extensions [48]. CARLA is widely used to simulate multi-agent scenarios for cooperative perception, collaborative planning, and sensor fusion [36, 49].

Simulation of Urban Mobility (SUMO) is a microscopic traffic simulator. It simulates traffic flows, vehicle routing, and traffic lights through roads, including intersections. SUMO can simulate large-scale road networks and real-world traffic scenarios. It supports communication protocols modeling (e.g., V2X communication with extensions) [50]. SUMO is often combined with CARLA or other simulators to model realistic traffic patterns and evaluate cooperative vehicle behaviors in complex road networks. A hybrid simulation combining CARLA's realistic sensor and environment model with SUMO's traffic management and routing capabilities enables testing collective navigation and cooperative decision-making in dynamic traffic scenarios with realistic multi-agent interactions [51–53].

LGSVL Simulator (now part of SVL Simulator) is an open-source autonomous driving simulator. It features high-fidelity sensor simulation (LiDAR, radar, cameras) and supports multi-agent scenarios with V2X communication. LGSVL integrates with Apollo and Autoware (popular open-source autonomous driving stacks) [54]. The simulator is often used for testing perception, planning, and control in connected vehicle networks with realistic urban and highway maps [55, 56].

CityFlow is a large-scale (city-wide) traffic simulator [57]. It can simulate traffic signal controls and large-scale intersections. It is lightweight and provides data structures efficient for the usage of multi-agent reinforcement learning applications [58, 59].

Apollo Cyber RT is another simulator that uses high-definition maps to simulate cooperative driving scenarios with realistic sensor data and vehicle communications. It simulates sensor fusion and multi-agent localization/decision-making for CCAVs [60, 61].

MetaDrive is a realistic and computationally feasible driving environment generator. It uses procedures for simulations, especially well-performing for high-way merge and intersection cases, and is suitable for generalizable reinforcement learning applications [62].

4.2 Datasets

In this section, popular datasets used in studies on CCAV autonomous driving and autonomous navigation are summarized and analyzed. Among various datasets, those including RGB camera data and publicly available are investigated. There are also datasets that do not include RGB data, such as V2V-Sim [35], V2XSet [7], LUCOOP [63], T&J [64], and CODD [65], and those that are not publicly available, such as DAIR-V2X–C [66], DOLPHINS [67], IRV2V [68], V2X-Seq [69], and V2X-Real [70], often used in the literature. A detailed comparison of the datasets is provided in **Table 4** and **Table 5**.

The COMAP dataset [71] is generated using a co-simulation of CARLA and SUMO with 2 to 20 CCAVs. The vehicles have 360-degree LiDAR (10 Hz, 200k points per second, 80 meter range) and an RGB camera (10 Hz, 800 × 600 pixels). The scenario includes 21 intersections.

The OPV2V dataset [36] is created using a co-simulation of CARLA and SUMO for 2 and 7 CCAVs. The vehicles have 360-degree LiDAR (10 Hz, 1.3 M points per

Dataset	Type	Scenario type	Sensor modalities	scale and key features
COMAP [71]	Simulated (CARLA + SUMO)	Intersection-based multi-agent	LiDAR, RGB cameras	8,668 frames, 227 K annotated 3D boxes, semantic labels, supports varied CCAV configurations.
OPV2V [36]	Simulated (CARLA + OpenCDA)	V2V scenarios, diverse roads	LiDAR + RGB cameras	11,464 frames, 233 K 3D boxes, supports BEV segmentation and object detection with multiple fusion schemes.
V2X-Sim 2.0 [49]	Simulated (SUMO + CARLA)	Multi-agent V2X	RGB, LiDAR, GPS, IMU	100 scenes, 10,000 frames; supports detection, tracking, and segmentation in BEV.
DeepAccident [72]	Simulated (CARLA)	Accident-prone V2X scenarios	Multi-view RGB + LiDAR, V2X infrastructure	57 K frames, 285 K samples, covering detection, tracking, segmentation, motion, and accident prediction.
V2V4Real [70]	Real-world	V2V scenarios, real traffic	LiDAR, RGB cameras, HD maps	20 K LiDAR + 40 K RGB frames, 240 K 3D boxes, supports Sim-to-Real studies.
TUMTraf [73]	Real-world (roadside + onboard)	Intersections, complex maneuvers	Camera, LiDAR, GPS, IMU	2,000 point clouds, 5,000 images, 30 K 3D boxes, HD maps; includes violations, near misses, and U-turns.
AdverCity [74]	Simulated	Adverse weather and lighting	Semantic cameras (likely RGB/LiDAR)	Focus on semantic segmentation in extreme conditions (e.g., fog, rain, night).

Table 4.
Comparison of datasets used in CCAV, part-1.

second, 120 meter range), 4 RGB cameras facing front, left, back, and right (10 Hz, 800 × 600 pixels), GPS, and IMU (10 Hz). There are 73 urban and rural scenarios, including highways.

V2X-Sim 2.0 is an extended version of V2X-Sim [49], generated using a co-simulation of CARLA and SUMO with 2 to 5 CCAVs. The vehicles have 360-degree LiDAR (5 Hz, 200k points per second, 70 meter range) and 6 high-resolution RGB cameras (100 Hz, 1600x900 pixels). The scenario includes 3 CARLA maps with 100 intersections.

The DeepAccident dataset [72] is generated using CARLA, simulating 12 types of accidents. In the scenarios, two CCAVs collide, and two other CCAVs are following. All vehicles have LiDAR (10 Hz, 70 meter range) and six RGB cameras (10 Hz, 1600 × 900 pixels).

The V2V4Real dataset [70] is a real-world dataset recorded in 10k frames (10 Hz) along 347 km of highway and 63 km of urban roads, including intersections. There are two vehicles equipped with monocular cameras facing front and back (CCAV 1: 2064x1544 px, CCAV 2: 1280x720 px), a LiDAR (200 meter range), GPS, and IMU.

The TUMTraf V2X Collective Perception dataset [73] is real-world data collected at a large four-way intersection with one autonomous vehicle and one road side unit. The latter has a LiDAR (120 meter range) and four RGB cameras (1920x1200 px), while the vehicle has a LiDAR (200 meter range), an RGB camera (1920x1200 px), GPS, and IMU.

Dataset	Strengths	Weaknesses	Typical applications	Distinctive focus, context
COMAP [71]	Efficient synthetic co-simulation (CARLA + SUMO). Multi-modal (images & point clouds) with segmentation.	Synthetic only (sim-to-real gap). Smaller scale.	Collective perception, fusion experiments, multi-agent perception benchmarking.	Lightweight synthetic generator for collective multi-agent perception (urban scenes).
OPV2V [36]	Open benchmark + fusion pipeline; multiple fusion strategies and metrics are provided.	Primarily simulated; earlier dataset (less real-world variety).	V2V fusion algorithm benchmarking (feature/early/late fusion).	One of the early standard benchmark and pipeline offerings for V2V cooperative perception.
V2X-Sim 2.0 [49]	Large, flexible synthetic V2X suite supporting multi-agent/multi-task research.	Synthetic data (sim-to-real gap).	V2X cooperative perception, multi-agent tasks, multi-modality research.	Comprehensive synthetic V2X family designed for various cooperative paradigms (V2V, V2I, V2X).
DeepAccident [72]	Large set of accident and near-accident scenarios, multi-view V2X recordings; supports motion and accident prediction tasks.	Synthetic accident-centric scenes (require adaptation).	Safety evaluation, accident prediction, V2X-enabled risk forecasting.	Focused on generating explicit accident scenarios and labels to enable accident prediction research.
V2V4Real [70]	Large-scale *real-world* multi-modal V2V dataset (LiDAR, RGB, HDMaps); annotated 3D boxes and tracks over long driving routes.	Real collection typically covers cooperating vehicle pairs (not dense fleets); annotation effort limits some breadth.	Real-world cooperative 3D detection, cooperative tracking, Sim2Real studies.	One of the first large real-world V2V cooperative-perception datasets (fills the sim-to-real gap).
TUMTraf [73]	High-quality roadside/infrastructure data; overhead LiDAR + camera with precise tracks.	Roadside-centric viewpoint (less ego-vehicle sensor realism).	RSU-assisted perception, long-range tracking, infrastructure-vehicle fusion.	Emphasizes infrastructure/roadside sensing for persistent multi-object tracking and V2X research.
AdverCity [74]	Synthetic multi-modal CP dataset explicitly built for adverse weather and glare; featuring many weather conditions and annotations.	Synthetic data (sim-to-real gap). Newer dataset (fewer external benchmarks so far).	Robust collaborative perception in adverse weather, domain-robustness, nighttime/glare handling.	First open synthetic CP dataset targeting adverse weather and glare scenarios (CARLA + OpenCDA).

Table 5.
Comparison of datasets used in CCAV, part-2.

The AdverCity dataset [74] is generated using CARLA with OpenCDA and 3 CCAVs. The vehicles are equipped with a LiDAR (10 Hz, 1.2 million points per second, 200 meter range), 4 RGB cameras (10 Hz, 1920x1080 pixels), GPS, and IMU. This dataset includes scenarios across 5 CARLA maps under 11 different weather conditions.

5. Conclusions and future research directions

In this chapter, autonomous driving and autonomous navigation architectures for connected and cooperative vehicles are analyzed. For cooperative driving, multi-agent reinforcement learning-based methods are investigated. Furthermore, end-to-end deep learning-based cooperative driving techniques, where raw sensor data of each agent are merged and joint optimal planning is globally found, are examined. For the modular pipelines, the navigation module of the pipeline for cooperative driving can be executed in cooperation. For intermediate fusion strategies, deep learning-based methods, mainly CNN-based ones, are examined and compared. Transformer-based intermediate fusion architectures are also analyzed. In the last part of this chapter, simulators used in the development and testing of these algorithms are examined; similarly, open-source simulated and real-world datasets are listed and compared.

Regarding MARL studies for cooperative autonomous driving of CCAVs, studies generally overlook the noisy and challenging communication between vehicles and bandwidth limits [75], which require more attention. Considering the data shared among the agents in MARL-based cooperative driving, security and privacy issues arise, especially since the proposed methods are generally centralized training and decentralized execution. The lack of real-world MARL datasets necessitates the use of simulated datasets during development. Augmenting available single-agent data for offline MARL data generation is also an open area [76]. Similarly, the extension of reinforcement learning with human feedback in autonomous driving [77] to multi-agent problems can be further studied.

End-to-end cooperative autonomous driving studies on safety-critical scenarios, such as emergencies and changing infrastructure capabilities, are limited and can be studied further to achieve more robust and reliable solutions. Furthermore, communication through limited bandwidths and noisy channels, as well as improvements to these systems, such as selected shared features, token-based fusion, or dynamic and adaptive compression, are future research areas [5]. Last but not least, more real-world datasets for end-to-end cooperative driving applications are required to further develop and compare novel techniques.

Intermediate collective navigation of CCAVs is mainly studied on single-modal data sharing, although multi-modal approaches available in the literature are limited. The privacy and security of the shared data are also concerns that need to be addressed. Similar to cooperative autonomous driving, communication limitations and adaptability need to be examined in cooperation with the collective navigation solutions.

Author details

Kenan Ahiska
Department of Electrical and Electronics Engineering, Middle East Technical University, Ankara, Türkiye

*Address all correspondence to: kahiska@metu.edu.tr

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] Bi J, Zhang X, Yuan H, Zhang J, Zhou M. A hybrid prediction method for realistic network traffic with temporal convolutional network and LSTM. IEEE Transactions on Automation Science and Engineering. 2021;**19**(3):1869–1879

[2] Li B, Zhuang W, Zhang H, Sun H, Liu H, Zhang J, et al. Traffic-Aware Ecological Cruising Control for Connected Electric Vehicle. IEEE Transactions on Transportation Electrification 2023;**9**:2075–2086

[3] Liu W, Hua M, Deng Z, Meng Z, Huang Y, Hu C, et al. A Systematic Survey of Control Techniques and Applications in Connected and Automated Vehicles. IEEE Internet of Things Journal 2023;**10**:21892–21916

[4] Ning Z, Xie L. A survey on multi-agent reinforcement learning and its application. Journal of Automation and Intelligence. 2024;**3**(2):73–91

[5] You J, Li P, Jiang Z, Huang Z, Gan R, Shi H, et al. SEAL: Vision-Language Model-Based Safe End-to-End Cooperative Autonomous Driving with Adaptive Long-Tail Modeling. arXiv Preprint arXiv 2025

[6] Li B, Zhao Y, Tan H. CoFormerNet: A Transformer-Based Fusion Approach for Enhanced Vehicle-Infrastructure Cooperative Perception. Sensors. 2024;**24**(13):4101. Available from: https://www.mdpi.com/1424-8220/24/13/4101

[7] Xu R, Xiang H, Tu Z, Xia X, Yang MH, Ma J V2x-vit: Vehicle-to-everything cooperative perception with vision transformer. In: European conference on computer vision. Springer; 2022

[8] Bazzan A, Klügl F. Multi-agent Systems for Traffic and Transportation Engineering. Hershey, PA. IGI Global; 2009

[9] He X, Lou B, Yang H, Lv C. Robust Decision Making for Autonomous Vehicles at Highway On-Ramps: A Constrained Adversarial Reinforcement Learning Approach. IEEE Transactions on Intelligent Transportation Systems. 2023;**24**(4):4103–4113

[10] Hua M, Qi X, Chen D, Jiang K, Liu ZE, Sun H, et al. Multi-Agent Reinforcement Learning for Connected and Automated Vehicles Control: Recent Advancements and Future Prospects. IEEE Transactions on Automation Science and Engineering. 2025;**22**:16266–16286

[11] Peake A, McCalmon J, Raiford B, Liu T, Alqahtani S Multi-agent reinforcement learning for cooperative adaptive cruise control. In: 2020 IEEE 32nd International Conference on Tools with Artificial Intelligence (ICTAI). IEEE; 2020. p. 15–22

[12] Shi H, Chen D, Zheng N, Wang X, Zhou Y, Ran B. A deep reinforcement learning based distributed control strategy for connected automated vehicles in mixed traffic platoon. Transportation Research Part C: Emerging Technologies. 2023;**148**:104019

[13] Wang G, Hu J, Li Z, Li L. Harmonious lane changing via deep reinforcement learning. IEEE Transactions on Intelligent

Transportation Systems. 2021;**23** (5):4642–4650

[14] Zhou W, Chen D, Yan J, Li Z, Yin H, Ge W. Multi-agent reinforcement learning for cooperative lane changing of connected and autonomous vehicles in mixed traffic. Autonomous Intelligent Systems. 2022;**2**(1):5

[15] Wu Y, Chen H, Zhu F. DCL-AIM: Decentralized coordination learning of autonomous intersection management for connected and automated vehicles. Transportation Research Part C: Emerging Technologies. 2019;**103**: 246–260

[16] Wang T, Cao J, Hussain A. Adaptive Traffic Signal Control for large-scale scenario with Cooperative Group-based Multi-agent reinforcement learning. Transportation Research Part C: Emerging Technologies. 2021;**125**:103046

[17] Chen D, Hajidavalloo MR, Li Z, Chen K, Wang Y, Jiang L, et al. Deep multi-agent reinforcement learning for highway on-ramp merging in mixed traffic. IEEE Transactions on Intelligent Transportation Systems 2023;**24**: 13246–13257

[18] Antonio GP, Maria-Dolores C. Multi-Agent Deep Reinforcement Learning to Manage Connected Autonomous Vehicles at Tomorrow's Intersections. IEEE Transactions on Vehicular Technology. 2022;**71**(7): 7033–7043

[19] Hu Y, Yang J, Chen L, Li K, Sima C, Zhu X, et al. Planning-oriented autonomous driving. In: Proceedings of the IEEE/CVF conference on computer vision and pattern recognition; 2023. p. 17853–17862

[20] Valiente R, Zaman M, Ozer S, Fallah YP Controlling Steering Angle for Cooperative Self-driving Vehicles utilizing CNN and LSTM-based Deep Networks. In: 2019 IEEE Intelligent Vehicles Symposium (IV); 2019. p. 2423–2428

[21] Huch S, Ongel A, Betz J, Lienkamp M. Multi-Task End-to-End Self-Driving Architecture for CAV Platoons. Sensors. 2021;**21**(4):1346

[22] Cui J, Qiu H, Chen D, Stone P, Zhu Y. Coopernaut: End-to-end driving with cooperative perception for networked vehicles. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition; 2022. p. 17252–17262

[23] Yu H, Yang W, Zhong J, Yang Z, Fan S, Luo P, et al. End-to-end autonomous driving through V2X cooperation. arXiv preprint arXiv:240400717. 2024

[24] You J, Shi H, Jiang Z, Huang Z, Gan R, Wu K, et al. V2X-VLM: End-to-End V2X Cooperative Autonomous Driving Through Large Vision-Language Models. Transportation Research Part C: Emerging Technologies. 2026;**183**:105457

[25] Guo Y, Ma J, Leslie E, Huang Z. Evaluating the effectiveness of integrated connected automated vehicle applications applied to freeway managed lanes. IEEE Transactions on Intelligent Transportation Systems. 2020;**23**(1):522–536

[26] Huang T, Liu J, Zhou X, Nguyen DC, Azghadi MR, Xia Y, et al. V2X Cooperative Perception for Autonomous Driving: Recent Advances and Challenges. arXiv Preprint arXiv 2024

[27] Hu H, Liu Z, Chitlangia S, Agnihotri A, Zhao D Investigating the Impact of Multi-LiDAR Placement on Object Detection for Autonomous Driving. In: 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR); 2022. p. 2540–2549

[28] Chen S, Chen Y, Zhang S, Zheng N. A Novel Integrated Simulation and Testing Platform for Self-Driving Cars With Hardware in the Loop. IEEE Transactions on Intelligent Vehicles. 2019;**4**(3):425–436

[29] Arnold E, Dianati M, de Temple R, Fallah S. Cooperative Perception for 3D Object Detection in Driving Scenarios Using Infrastructure Sensors. IEEE Transactions on Intelligent Transportation Systems. 2022;**23** (3):1852–1864

[30] Gao H, Cheng B, Wang J, Li K, Zhao J, Li D. Object Classification Using CNN-Based Fusion of Vision and LIDAR in Autonomous Vehicle Environment. IEEE Transactions on Industrial Informatics. 2018;**14** (9):4224–4231

[31] Rawashdeh ZY, Wang Z Collaborative automated driving: A machine learning-based method to enhance the accuracy of shared information. In: 2018 21st International Conference on Intelligent Transportation Systems (ITSC). OPTorganization; 2018. p. 3961–3966

[32] Rauch A, Klanner F, Rasshofer R, Dietmayer K Car2X-based perception in a high-level fusion architecture for cooperative perception systems. In: 2012 IEEE Intelligent Vehicles Symposium; 2012. p. 270–275

[33] Zeng W, Wang S, Liao R, Chen Y, Yang B, Urtasun R. DSDNet: Deep Structured Self-driving Network. In: Computer Vision – ECCV 2020: 16th European Conference, Glasgow, UK, August 23–28, 2020, **Proceedings, Part XXI**. Berlin, Heidelberg: Springer-Verlag; 2020. p. 156–172

[34] Melotti G, Premebida C, Gonçalves N Multimodal Deep-Learning for Object Recognition Combining Camera and LIDAR Data. In: 2020 IEEE International Conference on Autonomous Robot Systems and Competitions (ICARSC); 2020. p. 177–182

[35] Wang TH, Manivasagam S, Liang M, Yang B, Zeng W, Urtasun R V2vnet: Vehicle-to-vehicle communication for joint perception and prediction. In: Computer Vision–ECCV 2020: 16th European Conference, Glasgow, UK, Proceedings, Part II 16. Springer

[36] Xu R, Xiang H, Xia X, Han X, Li J, Ma J. Opv2v: An open benchmark dataset and fusion pipeline for perception with vehicle-to-vehicle communication. In: 2022 International Conference on Robotics and Automation (ICRA). IEEE; 2022

[37] Chen Q, Ma X, Tang S, Guo J, Yang Q, Fu S. F-cooper: Feature based cooperative perception for autonomous vehicle edge computing system using 3D point clouds. In: Proceedings of the 4th ACM/IEEE Symposium on Edge Computing; 2019. p. 88–100

[38] Li Y, Ren S, Wu P, Chen S, Feng C, Zhang W. Learning Distilled Collaboration Graph for Multi-Agent Perception. Advances in Neural Information Processing Systems. 2021;**34**:28861–28873

[39] Dosovitskiy A, Beyer L, Kolesnikov A, Weissenborn D, Zhai X, Unterthiner

T, et al. An image is worth 16x16 words: Transformers for image recognition at scale. arXiv preprint arXiv:201011929. 2020

[40] Liu Z, Lin Y, Cao Y, Hu H, Wei Y, Zhang Z, et al. Swin transformer: Hierarchical vision transformer using shifted windows. In: Proceedings of the IEEE/CVF International Conference on Computer Vision; 2021. p. 10012–10022

[41] Liu Z, Ning J, Cao Y, Wei Y, Zhang Z, Lin S, et al. Video swin transformer. arXiv preprint arXiv:210613230. 2021

[42] Dong X, Bao J, Chen D, Zhang W, Yu N, Yuan L, et al. Cswin transformer: A general vision transformer backbone with cross-shaped windows. arXiv preprint arXiv:210700652. 2021

[43] Wang W, Xie E, Li X, Fan DP, Song K, Liang D, et al. Pyramid vision transformer: A versatile backbone for dense prediction without convolutions. In: Proceedings of the IEEE/CVF International Conference on Computer Vision; 2021. p. 568–578

[44] Min J, Zhao Y, Luo C, Cho M Peripheral Vision Transformer. arXiv preprint arXiv:220606801. 2022

[45] Xu R, Tu Z, Xiang H, Shao W, Zhou B, Ma J. CoBEVT: Cooperative Bird's Eye View Semantic Segmentation with Sparse Transformers. In: Liu K, Kulic D, Ichnowski J, editors. Proceedings of The 6th Conference on Robot Learning. vol. 205 of Proceedings of Machine Learning Research. PMLR; 2023. p. 989–1000

[46] Xiang H, Xu R, Ma J. HM-ViT: Hetero-modal Vehicle-to-Vehicle Cooperative Perception with Vision Transformer . In: 2023 IEEE/CVF International Conference on Computer Vision (ICCV). Los Alamitos, CA, USA: IEEE Computer Society; 2023. p. 284–295

[47] Samak TV, Samak CV, Li B, Krovi V. When Digital Twins Meet Large Language Models: Realistic, Interactive, and Editable Simulation for Autonomous Driving. arXiv Preprint. 2025

[48] Dosovitskiy A, Ros G, Codevilla F, Lopez A, Koltun V. CARLA: An open urban driving simulator. In: Conference on robot learning. PMLR; 2017. p. 1–16

[49] Li Y, Ma D, An Z, Wang Z, Zhong Y, Chen S, et al. V2X-Sim: Multi-Agent Collaborative Perception Dataset and Benchmark for Autonomous Driving. IEEE Robotics and Automation Letters 2022;**7**:10914–10921

[50] Lopez PA, Behrisch M, Bieker-Walz L, Erdmann J, Flötteröd YP, Hilbrich R, et al. Microscopic Traffic Simulation using SUMO. In: 2018 21st International Conference on Intelligent Transportation Systems (ITSC). IEEE Press; 2018. p. 2575–2582

[51] Li P, Kusari A, LeBlanc DJ. A Novel Traffic Simulation Framework for Testing Autonomous Vehicles Using SUMO and CARLA. arXiv Preprint. 2021

[52] Yilmaz-Niewerth S, Häbel R, Friedrich B. Developing a comprehensive large-scale co-simulation for replication of automated driving in urban traffic scenarios. Transportation Research Procedia. 2024;**78**:522–529. 25th Euro Working Group on Transportation Meeting

[53] Azfar T, Ke R. Traffic Co-Simulation Framework Empowered by Infrastructure Camera Sensing and

Reinforcement Learning. Journal of Intelligent Transportation Systems. 2025. p. 1–19. DOI:10.1080/15472450.2025.2559410

[54] Rong G, Shin BH, Tabatabaee H, Lu Q, Lemke S, Možeiko M, et al. LGSVL Simulator: A High Fidelity Simulator for Autonomous Driving. In: 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC); 2020. p. 1–6

[55] Sun Y, Poskitt CM, Sun J, Chen Y, Yang Z. LawBreaker: An Approach for Specifying Traffic Laws and Fuzzing Autonomous Vehicles. In: Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering. ASE ´22. New York, NY, USA: Association for Computing Machinery; 2023

[56] Li C, Sifakis J, Yan R, Zhang J. Rigorous Simulation-based Testing for Autonomous Driving Systems – Targeting the Achilles' Heel of Four Open Autopilots. arXiv Preprint arXiv. 2024

[57] Zhang H, Feng S, Liu C, Ding Y, Zhu Y, Zhou Z, et al. CityFlow: A Multi-Agent Reinforcement Learning Environment for Large Scale City Traffic Scenario. In: The World Wide Web Conference. WWW ´19. New York, NY, USA: Association for Computing Machinery; 2019. p. 3620–3624

[58] Feng Q, Ablavsky V, Sclaroff S. CityFlow-NL: Tracking and Retrieval of Vehicles at City Scale by Natural Language Descriptions. arXiv Preprint arXiv. 2021

[59] Wu J, Ran Y, Lou Y, Shu L. CenLight: Centralized traffic grid signal optimization via action and state decomposition. IET Intelligent Transport Systems. 2023;**17**(6): 1247–1261

[60] Huang X, Cheng X, Geng Q, Cao B, Zhou D, Wang P, et al. The ApolloScape Dataset for Autonomous Driving. In: 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW); 2018. p. 1067–10676

[61] Ning M, Yang Y, Shu K, Huang S, Zhong J, Salehi M, et al. CoInfra: A Large-Scale Cooperative Infrastructure Perception System and Dataset in Adverse Weather. arXiv Preprint arXiv 2025

[62] Li Q, Peng Z, Feng L, Zhang Q, Xue Z, Zhou B. MetaDrive: Composing Diverse Driving Scenarios for Generalizable Reinforcement Learning. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2023;**45**(3):3461–3475

[63] Axmann J, Moftizadeh R, Su J, Tennstedt B, Zou Q, Yuan Y, et al. LUCOOP: Leibniz University Cooperative Perception and Urban Navigation Dataset. In: 2023 IEEE Intelligent Vehicles Symposium (IV); 2023

[64] Chen Q, Tang S, Yang Q, Fu S. Cooper: Cooperative perception for connected autonomous vehicles based on 3d point clouds. In: 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS). IEEE; 2019

[65] Arnold E, Mozaffari S, Dianati M. Fast and Robust Registration of Partially Overlapping Point Clouds. IEEE Robotics and Automation Letters. 2021;**6**(2):1385–1392

[66] Yu H, Luo Y, Shu M, Huo Y, Yang Z, Shi Y, et al. Dair-v2x: A large-scale

dataset for vehicle-infrastructure cooperative 3d object detection. In: IEEE/CVF Conference on Computer Vision and Pattern Recognition; 2022

[67] Mao R, Guo J, Jia Y, Sun Y, Zhou S, Niu Z. DOLPHINS: Dataset for Collaborative Perception enabled Harmonious and Interconnected Self-driving. In: Proceedings of the Asian Conference on Computer Vision; 2022. p. 4361–4377

[68] Wei S, Wei Y, Hu Y, Lu Y, Zhong Y, Chen S, et al. Asynchrony-Robust Collaborative Perception via Bird's Eye View Flow. arXiv E-prints. 2023;**36**:28462–28477

[69] Yu H, Yang W, Ruan H, Yang Z, Tang Y, Gao X, et al. V2X-Seq: A Large-Scale Sequential Dataset for Vehicle-Infrastructure Cooperative Perception and Forecasting. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2023

[70] Xu R, Xia X, Li J, Li H, Zhang S, Tu Z, et al. V2V4Real: A Real-world Large-scale Dataset for Vehicle-to-Vehicle Cooperative Perception. In: IEEE/CVF CVPR; 2023

[71] Yuan Y, Sester M. COMAP: A Synthetic Dataset for Collective Multi-Agent Perception of Autonomous Driving. The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences. 2021;**43**:255–263

[72] Wang T, Kim S, Ji W, Xie E, Ge C, Chen J, et al. DeepAccident: A Motion and Accident Prediction Benchmark for V2X Autonomous Driving. arXiv preprint arXiv:230401168. 2023

[73] Zimmer W, Wardana GA, Sritharan S, Zhou X, Song R, Knoll AC TUMTraf V2X Cooperative Perception Dataset. arXiv preprint arXiv:240301316. 2024

[74] Karvat M, Givigi S. Adver-City: Open-Source Multi-Modal Dataset for Collaborative Perception Under Adverse Weather Conditions. arXiv Preprint arXiv. 2025

[75] Wang R, He X, Yu R, Qiu W, An B, Rabinovich Z Learning efficient multi-agent communication: An information bottleneck approach. In: International Conference on Machine Learning. PMLR; 2020. p. 9908–9918

[76] Reuse M, Simon M, Sick B About the Ambiguity of Data Augmentation for 3D Object Detection in Autonomous Driving. In: 2021 IEEE/CVF International Conference on Computer Vision Workshops (ICCVW); 2021. p. 979–987

[77] Yuan Y, Hao J, Ma Y, Dong Z, Liang H, Liu J, et al. Uni-RLHF: Universal Platform and Benchmark Suite for Reinforcement Learning with Diverse Human Feedback. arXiv Preprint arXiv. 2024

Chapter 4

Perspective Chapter: Vehicle Platoon String Stability through the Lens of O-RAN – Opportunities, Challenges and Future Directions

Emad El-Din Mazied and Hesham A. Rakha

Abstract

Vehicle platooning enhances fuel efficiency, reduces travel time, and improves road safety, while enabling automation across various use cases, including logistics, agriculture, and manufacturing. *String stability* is key to platoon control, modeled within the framework of a wireless networked control system (WNCS). It prevents the amplification of disturbances along the vehicle formation and ensures cooperative and safe operations. This chapter provides a comprehensive overview of vehicle platoon control in the context of Open Radio Access Network (O-RAN) design as a communication infrastructure for platoon string stability, highlighting how O-RAN's open, programmable, and intelligent architecture enables the integration of sensing, communication, computing, and control functions within intelligent transportation systems (ITS) to achieve a string-stable platoon. The discussion explores how O-RAN's disaggregated architecture, edge intelligence, and AI-powered xApps and rApps can support multi-agent control frameworks for maintaining string stability, considering wireless communication constraints. Furthermore, the chapter addresses the opportunities, technical challenges, and research directions associated with O-RAN-enabled platoon control, including coordination across heterogeneous infrastructures, trade-offs between latency and reliability, data privacy, and human–vehicle interaction. Through this lens, O-RAN is presented to realize cooperative, reliable, and road user-accepted vehicular control systems.

Keywords: vehicle platoon, string stability, wireless networked-control system, O-RAN, ISCCC, multi-agent communication-control co-design

1. Introduction

Vehicle platooning – a line (string) of successive vehicles traveling in a single lane, where each vehicle follows an acceleration and spacing profile relative to the leading

vehicle at the head of the platoon – has demonstrated gains in fuel efficiency, reduced delivery times, enhanced safety through shockwave damping, and notable socioeconomic benefits [1]. A vehicle platoon can be viewed as a vehicular cyber-physical system (VCPS), whose control, expressed in terms of string stability, is modeled within the framework of a wireless networked control system (WNCS) [2]. In this context, the quality of control (QoC) interplays with the quality of service (QoS) of the underlying wireless communication network, where maintaining reliability metrics – packet drop rate (PDR), delay, and jitter – below predefined thresholds is essential to achieving desired control performance.

Recent advances in wireless network architectures, particularly Open Radio Access Networks (O-RAN) [3], introduce an open, programmable, disaggregated, and intelligent framework that can bridge wireless network functions and intelligent transportation system (ITS) control functions to achieve robust, string-stable platoons. This chapter builds upon these developments to explore how O-RAN's openness and AI-driven control can enhance platoon stability by introducing guidelines for designing a multi-agent communication–control framework that integrates sensing, communication, and computing with platoon control, inspired by the research presented by Zhai et al. and Cheng et al. [4, 5].

Although O-RAN offers considerable opportunities for platoon control, it remains in its infancy and is subject to inherent limitations. While a growing body of literature examines O-RAN's role in supporting vehicular communications, for example, [6] – a comprehensive overview of how O-RAN's intelligent and multi-agent control capabilities—such as AI-powered xApps and rApps can be integrated into ITS for vehicle platoon control across different use cases (logistics, agriculture, and industry) is still missing. Therefore, this chapter provides an overview that highlights opportunities and challenges from various design perspectives, as well as the research directions associated with O-RAN-enabled platoon control. These include coordination across heterogeneous infrastructures, trade-offs between latency and reliability, data privacy, and human–vehicle interaction, all of which are critical for incorporating O-RAN into string-stability control of vehicular platoons[1].

This chapter introduces O-RAN as an enabling technology for developing robust string-stability platoon control that integrates sensing, communication, and computation into the platoon control process. The integration occurs at the system level, where string-stability platoon control is modeled as a multi-agent feedback control system, and the vehicle platoon is represented as a WNCS. In this framework, vehicle dynamics (e.g., velocity), which represent the control-loop output, are fed back to vehicle control agents and to integrated sensing, communication, and computing resource management agents, which use this information to determine sensing ranges and communication constraints required for reliable wireless transmission.

Within this context, the chapter analyses string-stability platoon control through the WNCS abstraction, where the openness and intelligence of O-RAN enable a methodological framework for integrating sensing, communication, computation, and control to synthesize a robust platoon control system. The core concept underlying this methodology is that robust vehicle control depends on understanding, anticipating, and predicting future events in the presence of variations in the surrounding ITS environment. Accordingly, real-time data are

[78] Throughout this chapter, *platoon control* and *string stability* are used interchangeably to refer to the control of inter-vehicle dynamics within a platoon.

collected, analyzed, and used to produce accurate, timely control actions while tuning wireless communication parameters to ensure reliable message exchange.

O-RAN supports this integrated methodology by enabling vehicle sensors to communicate with O-RAN rApps deployed at the edge, where data can be processed and analyzed in real time to support accurate control decisions. More specifically, O-RAN enables this integrated perspective through its openness, which supports the rapid development of control logic via xApps and rApps; its intelligence, which facilitates the deployment of multi-agent AI/ML algorithms; and its edge computing capabilities, which provide the computational resources required to execute these algorithms and dynamically tailor resources through O-RAN system management and orchestration.

In this sense, the chapter focuses on the design of robust string-stability platoon control through an integrated sensing, communication, computation, and control (ISCCC) approach enabled by O-RAN technologies.

Figure 1 visualizes the methodological structure of this chapter through a layered architecture. At the system layer, the O-RAN system integrates sensing, communication, and computation to support the control layer, whose core component is a multi-agent string-stability control system. This control layer operates within the system layer and leverages the integrated system capabilities to realize robust platoon control. The system layer further supports diverse applications at the application layer, including platoons of tractors in Agriculture 4.0, platoons of automated guided vehicles in Industry 4.0, and platoons of trucks in logistics.

In this sense, **the key contributions of this chapter are as follows:**

- Provide a comprehensive overview of string stability in the context of a WNCS.
- Leverage models and formulations from the literature to establish design guidelines for ISCCC-based string-stability controllers suitable for intelligent vehicle platoons.

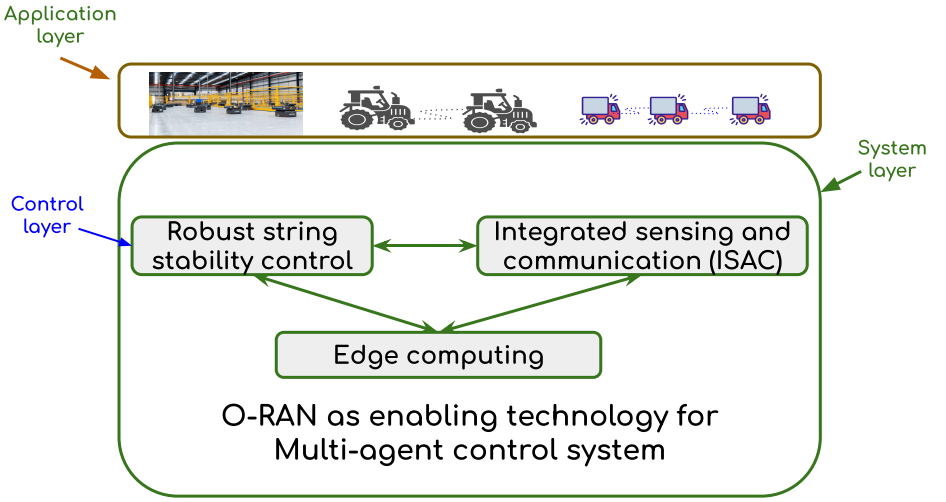


Figure 1.
O-RAN-based integrated sensing, communication, and computation for string stability control: control, system, and application layers.

- Examine the capabilities of O-RAN in supporting the proposed control framework, emphasizing its openness, disaggregation, and intelligence as enablers for adaptive platoon control.

- Address the opportunities and technical challenges of incorporating O-RAN into platoon control, with particular attention to coordination across heterogeneous infrastructures, communication–control co-design, and human-centered design considerations.

The rest of this chapter is organized as follows: First, we discuss the motivation for vehicle platooning, its definition, components, and string-stability models. Next, we present platoon control as a network-controlled system and outline guidelines for developing AI-powered multi-agent control frameworks. We then examine the integration of sensing, communication, and computing enabled by O-RAN within the platoon-control context. Subsequently, we discuss the opportunities offered by O-RAN for platoon control, the remaining challenges, and directions for future research. Finally, the chapter concludes with key insights and implications.

2. Vehicle platooning and string stability: An overview

In this section, we provide an overview of vehicle platooning and string stability, outlining their definitions, evolution, and key design requirements. We then present a generic framework, leveraging cutting-edge research on string stability for platoon control that ensures string stability and highlights essential design considerations.

2.1 Motivations

Fuel consumption accounts for nearly half of logistics expenses, influencing the pace of global economic growth [7–9]. It is also a major contributor to air pollution, responsible for approximately one-quarter of global carbon dioxide (CO_2) emissions and linked to an estimated 4.2 million premature deaths per year [9, 10]. In addition, unsafe road conditions cause approximately 1.35 million traffic fatalities each year, disproportionately affecting vulnerable road users [9, 10].

To address the persistent challenges of road safety and fuel consumption in transportation systems, recent advances in car-following theory [11], control theory for adaptive cruise control (ACC) [12], and the evolution of connected and automated vehicles (CAVs) [11], rooted in integrated wireless sensing and communication, have converged to enable the development of ***vehicle platooning***. Vehicle platooning aims to improve traffic flow efficiency while meeting environmental, economic, and operational requirements. These include gains in fuel efficiency and reduced delivery times, enhanced safety through shockwave damping, and socioeconomic benefits in urban, suburban, and rural contexts, such as minimizing travel time, lowering fuel consumption and emissions, and optimizing the use of limited road capacity [13–15].

2.2 Definition

A vehicle platoon is defined as a line of successive vehicles in a single lane, where each follows an acceleration and spacing-distance profile relative to the leading vehicle at the head of the platoon [12]. The concept originates from car-following theories, which model vehicles traveling sequentially in a lane without overtaking, assuming that each driver (human, autonomous, or hybrid) responds in a specific manner to stimuli from the vehicle ahead. **Figure 2** illustrates an example of two vehicle platoons.

2.3 Vehicle platooning components

The vehicle platoon system comprises six components: node dynamics, information flow topology (IFT), distributed controller, formation geometry, communication infrastructure, and system disturbances. Since covering all components is beyond the scope of this chapter, we focus on two critical elements – communication infrastructure and the distributed controller – highlighting opportunities enabled by next-generation wireless networks. We refer to [2, 16] for detailed surveys of the other components.

2.3.1 Platoon control

The distributed controller coordinates the platoon system to achieve control objectives that encompass both *individual and string stability*. Platoon control synchronizes vehicles at a consensual speed while maintaining safe spacing, thereby increasing capacity, improving safety, and reducing fuel use. *Individual stability* ensures convergence to trajectories but may amplify disturbances as the platoon length grows, leading to stop-and-go waves. *String stability*, in contrast, prevents disturbance amplification along the vehicle string. This chapter emphasizes string stability as the key control objective.

2.3.2 Platoon communication

Platoon performance is constrained by technical limitations of wireless communication systems, such as delay, packet loss, limited bandwidth, and security risks. In this chapter, we highlight emerging O-RAN architectures, which provide openness, disaggregation, and intelligence, enabling vehicle platooning to integrate

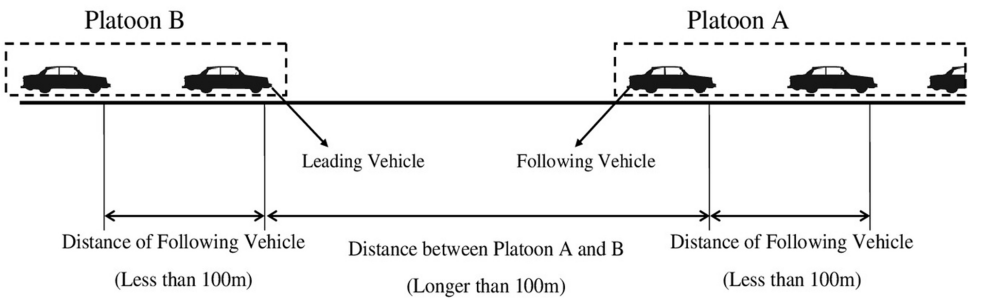


Figure 2.
Vehicle platoon [1].

advances in control theory, wireless communication, and high-performance computing (HPC) within a VCPS framework [16, 17]. **Figure 3** depicts the enabling communication and vehicular technologies.

2.3.3 Platoon use-cases

In this sense, platooning applies across Industry 4.0 (guided vehicles and mobile robots), logistics (trucks), Agriculture 4.0 (tractors), and diverse driving models (human, hybrid, and autonomous). Vehicles exchange control and situational awareness data through Vehicle-to-Vehicle (V2V) and Vehicle-to-Network (V2N) links, while edge servers manage these processes to enable integrated sensing, communication, and computation for robust platoon control, as illustrated in **Figure 4**. In the subsequent sections, we discuss the O-RAN-based vehicle platooning system design and related challenges in more detail.

2.4 Vehicle platoon control: String stability

A vehicle platoon consists of at least two closely spaced vehicles traveling at a desired cruising velocity while maintaining a specified inter-vehicle distance. Platoon control enables tighter formations, reducing congestion, aerodynamic drag, and fuel consumption [2]. However, tight formations introduce a major challenge – ***string instability*** – where disturbances in system states amplify along the vehicle string. Such instability can induce traffic jams (e.g., stop-and-go waves) even

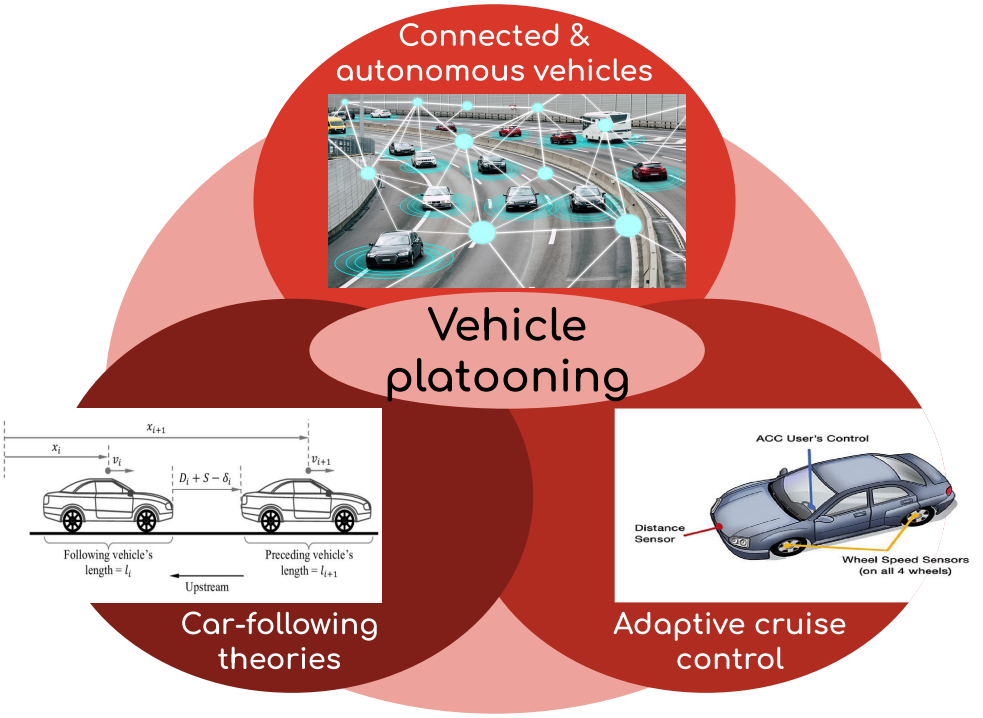


Figure 3.
Enabling technologies.

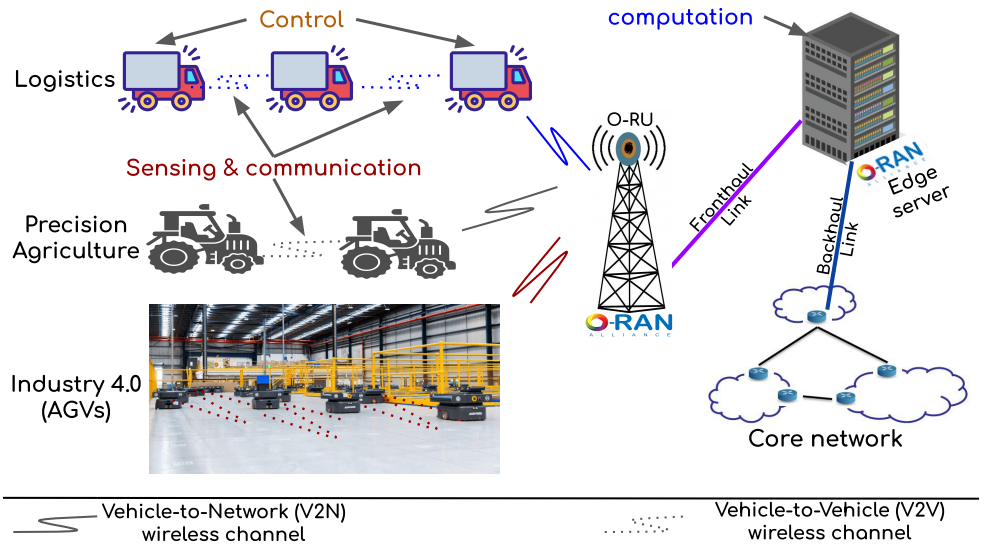


Figure 4.
Platoon components and use cases.

without bottlenecks, thereby undermining the benefits of platoon control [2]. In this context, a vehicular platoon is modeled as a cascaded system of autonomous and connected elements (i.e., automotive subsystems), making ***string stability*** a fundamental system property.

A platoon is string-stable if disturbances are not amplified as they propagate along the string. Four major disturbance types are typically considered in modeling and analysis: (i) initial condition perturbations for the leading vehicle; (ii) initial condition perturbations for all vehicles; (iii) external disturbances for the leading vehicle with zero initial condition perturbations; and (iv) external disturbances for all vehicles with zero initial condition perturbations. A vehicle string is stable if, for any bounded initial disturbances, all position fluctuations remain bounded and approach zero as time tends to infinity. Several definitions of string stability exist in the literature, depending on the disturbance type and modeling approach [2].

In this chapter, we adopt disturbance string stability (DSS), which considers the input-to-state stability (ISS) case because it is more practical, accommodates all four disturbance types, and captures real-world scenarios involving unmodeled dynamics [2, 18]. Accordingly, we consider a platoon of automatically heterogeneous controlled vehicles represented as an autonomous cascaded interconnection. The overall dynamics of this interconnected system can thus be expressed through the following cascaded state-space formulation [18]:

$$\begin{aligned} \dot{x}_0(\theta) &= f(x_0(\theta), u(\theta), \omega_0(\theta)), \\ \dot{x}_v(\theta) &= f(x_v(\theta), x_{v-1}(\theta), \omega_v(\theta)), \quad v \in \mathcal{V} \\ y_v(\theta) &= h(x_v(\theta)), \end{aligned} \tag{1}$$

where $\mathcal{V} = 1, 2, \ldots, N$ denotes the set of follower vehicles; $x0(\theta)$ represents the state of the leading vehicle subsystem ($v0$) as a function of the independent variable θ (which may denote time t or space s)[2]; $xv(\theta)$ denotes the state of the follower vehicle subsystem $v \in \mathcal{V}$; $u(\theta)$ is the external input signal; $yv(\theta)$ is the output signal of vehicle $v \in \mathcal{V}$; and $\omega_v(\theta)$ represents the external disturbance acting on the system. The function $f(\cdot)$ denotes the state transition function that captures the system dynamics among interconnected vehicles and is assumed to be continuously differentiable and globally Lipschitz in its arguments (i.e., globally Lipschitz in (x, ω) and (x, u, ω)). Likewise, $h(\cdot)$ denotes the output function mapping states to outputs, which is continuously differentiable and globally Lipschitz in its argument (x).

In this context, the platoon system defined in 1 is said to be disturbance string stable (DSS) if the equilibrium point $x_v(\theta) = 0$[3], for all $v \in \mathcal{V}$, satisfies the following condition "there exist a class $\mathcal{KL}$ function β, a class $\mathcal{K}$ function σ, and positive constants $k_1, k_2 \in \mathbb{R}^+$" such that, for any initial condition $x_v(0)$ and additive disturbance $\omega_v(\theta)$, $v \in \mathcal{V}$, the following property holds:

$$\sup_v |x_v(\theta_0)| < k_1, \sup_v \| \omega_v(\theta)\|_\infty < k_2, \tag{2}$$

This inequality ensures that the influence of both the initial conditions and external disturbances on each vehicle's output remains bounded and does not amplify along the string as θ evolves. In other words, the system is said to exhibit DSS when local deviations – whether due to initial state errors or external perturbations – decay or remain uniformly bounded throughout the entire platoon, ensuring smooth and coordinated motion among all vehicles.

For the system described in 1, when the condition in 2 holds, the solution $x_v(\theta)$, $v \in \mathcal{V}$, exists for all $\theta \geq \theta_0$ and satisfies the following property:

$$\sup_v \left|x_v(\theta)\right| \leq \beta\left(\sup_v \left|x_v(\theta_0)\right|, \theta - \theta_0\right) + \sigma\left(\sup_v |\omega_v|_\infty^{[\theta_0, \theta]}\right), \quad \forall v \in \mathcal{V} \tag{3}$$

In addition to the above properties, for ISS compatibility, the vehicle platooning system must ensure that the state transition function f has a bounded input–state gain, so that perturbations in neighboring states or disturbances remain bounded. This condition can be defined as follows:

$$|x_v(\theta)| \leq \beta\left(x_v(\theta_0), \theta - \theta_0\right) + \gamma\left(|x_{v-1}|_\infty^{[\theta_0, \theta]}\right) + \sigma\left(|\omega_v|_\infty^{[\theta_0, \theta]}\right), \forall \theta \geq \theta_0 \tag{4}$$

If the platoon system considers $\dot{x}_v(\theta) = f(x_v(\theta), y_{v-1}(\theta), \omega_v(\theta))$, where $y_v(\theta) = h(x_v(\theta))$, then the corresponding ISS–DSS compatibility property for the output mapping can be expressed as follows:

$$|y_v(\theta)| \leq \beta_y(x_v(\theta_0), \theta - \theta_0) + \gamma_y\left(|y_{v-1}|_\infty^{[\theta_0, \theta]}\right) + \sigma_y\left(|\omega_v|_\infty^{[\theta_0, \theta]}\right), \forall \theta \geq \theta_0 \tag{5}$$

Table 1 summarizes the parameters of the string stability model.

According to the above discussion, obtaining string stability is crucial for maintaining safe and secure formations; failure to do so jeopardizes road safety due to instability in the chain of vehicles. Consequently, research on string stability focuses on designing controllers to ensure a string-stable platoon. The following

[2] θ is the independent variable, which can represent time t or space s.

[3] This means that when all states and disturbances are zero, the system remains at rest.

Symbol	Definition	Symbol	Definition
$\mathcal{V}$	Set of following vehicles	$\cdot_0$	Subscript denotes the leading vehicle
$\cdot_v$	Subscript denotes a following vehicle	θ	Independent variable (space or time)
u	System control input	ω	External disturbance
y	System output	$f(\cdot)$	State transition is a continuously differentiable and globally Lipschitz function in its arguments.
$h(\cdot)$	Mapping states to outputs is a continuously differentiable and globally Lipschitz function in its arguments.	$\sup_D(\cdot)$	Supremum (least upper bound) of the norm of the Jacobian of $\cdot$over a domain D
k	Positive constant $\in \mathbb{R}^+$	β	Function of $\mathcal{KL}$ class
σ	Functions of $\mathcal{K}$ class	γ	Functions of $\mathcal{K}$ class

Table 1.
String Stability model definition.

sections discuss the principles of string stability controller design in the era of next-generation wireless networks that leverage openness, disaggregation, and intelligence in open programmable radio access networks (RANs), where sensing, communication, and computation are integrated to achieve robust platoon control (string stability). Furthermore, they highlight the opportunities, challenges, and future research directions associated with each design aspect within this integrated framework of sensing, communication, computation, and control.

3. Network controlled platoon system

As introduced in Section 2, a vehicle platoon is a controlled VCPS, where platoon control is achieved by interconnecting platoon components that interact through a wireless communication infrastructure. In this VCPS, sensing, communication, and computing are integrated to enhance platoon controller design by enabling reliable and low-latency information exchange among networked entities such as vehicles, network components, and road infrastructure units [19–24]. In the following, we discuss the design of string stability controllers in the context of network-controlled systems, thereby establishing the control-theoretic foundation of the introduced methodology by analyzing string-stability platoon control as a multi-agent feedback control problem.

In this context, each vehicle controller is manifested as an agent that cooperates with other agents to regulate inter-vehicle spacing and velocity while maintaining string stability. Existing string-stability models and control formulations in the literature are reviewed and interpreted from a multi-agent perspective. These models provide the analytical basis for embedding learning-assisted and adaptive control interventions, particularly when control loops are closed over wireless communication links.

3.1 Vehicle platoon as a WNCS

As shown in **Figure 4**, vehicle platoon control is considered a WNCS in the context of the VCPS, which includes vehicles with onboard sensors, actuators, and

controllers communicating wirelessly. Sensors (e.g., radar, camera, GPS) measure the vehicle's own state – speed, acceleration, spacing distance – and the relative state of neighboring vehicles. Actuators (e.g., throttle, brake, steering) execute commands from the controller. Controllers may be implemented locally within each vehicle (e.g., cooperative ACC) or partially centralized at an edge or cloud entity for higher-level coordination [25].

Information exchange among platoon vehicles is based on vehicle-to-vehicle (V2V) and vehicle-to-network (V2N) communications. Although there are two wireless infrastructures – (i) IEEE 802.11p/DSRC and (ii) cellular V2X (C–V2X) – this chapter considers only C–V2X. In C–V2X, V2V communication occurs via the sidelink interface (PC5) in Mode 4 to support direct message exchange between neighboring vehicles for local platoon stabilization. V2N links connect vehicles to network infrastructure such as road-side units (RSUs) or edge servers for global coordination and network management.

The WNCS-based platoon operates as a closed-loop system: sensors monitor system-state variations and send measurements wirelessly to controllers; controllers compute control actions and send commands wirelessly to actuators; actuators execute the commands, closing the control loop [20]. In this sense, vehicular platooning integrates physical processes, communication infrastructure, and control logic.

Consequently, communication and control components are interdependent. Dynamic wireless conditions, such as fading, packet loss, and delay, affect the QoC. Inaccurate measurements can lead to deviations from the planned control action, while network-induced delays create discrepancies between actual and predicted states. Error-control mechanisms, such as forward error correction (FEC) and retransmission, reduce packet loss but incur delay, introducing reliability–latency trade-offs.

Given these interdependencies, the WNCS-based platoon design must account for the limitations of wireless communication networks, the characteristics of the wireless channel (e.g., sidelink), and the controller design to ensure the robustness of the platoon control and maintain the stability of the string.

3.2 WNCS-based string stability controller

In WNCS-based platoon control, the design of string stability controllers accounts for the complexities of the platoon's subsystems, including vehicle dynamics, wireless communication constraints, network access, wireless sensing, and resource-constrained computing entities (e.g., edge servers). **Figure 5** illustrates the information exchange between vehicle controllers over sensing and communication channels, where the sensing and communication capabilities of the WNCS contribute to achieving string stability control objectives.

The platoon operates by integrating WNCS entities, which include sensing, communication, and computation, to achieve a string-stable platoon. A hierarchical control scheme is considered, comprising distributed local controllers in each vehicle that manage ACC [26].

In this system, we consider a delay-based spacing policy for the string stability control design, as described in [18]. The control objective is to optimally regulate the inter-vehicle spacing by tracking the reference velocity ν_{ref} determined by the vehicle's ACC process.

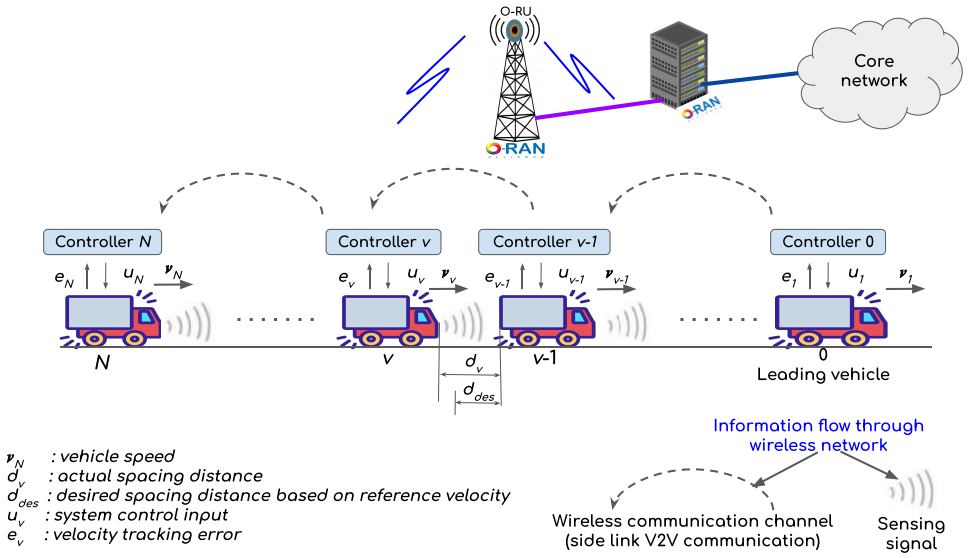


Figure 5.
Information exchange in WNCS-based vehicle platoon.

The vehicle dynamics are expressed in terms of the longitudinal position of each vehicle $v \in \mathcal{V}$ and its velocity ν, which satisfy the kinematic relations according to the analysis introduced in [18] as follows.

$$\dot{Z}_v(\theta) = h(\xi_v(\theta)),$$

$$\dot{\xi}_v(\theta) = f(\xi_v(\theta)) + g(\xi_v(\theta))\, u_v(\theta) + p(\xi_v(\theta))\, \omega_v(\theta) \tag{6}$$

In 6, the function $\xi(\theta)$ represents a general description of the vehicle dynamics, which may include the engine, drivetrain dynamics, and low-level control systems [18]. The variable θ, as defined in Section 2, is an independent variable that represents either space or time. If $\theta = t$ (time domain), then $Z_v(\theta) = s_v(t)$ denotes the position of vehicle v at time t, and the kinematic relation with velocity is given by $\nu_v(t) := h(\xi_v(t))$. Conversely, if $\theta = s$ (space domain), then $Z_v(\theta) = t_v(s)$ denotes the time at which vehicle v is at position s, and the kinematic relation with velocity is expressed as $\nu_v(s) := \frac{1}{h(\xi_v(s))}$. The functions h, f, g, and p are assumed to be sufficiently smooth, continuous, differentiable, and globally Lipschitz functions in their arguments.

In this sense, to achieve the control objective of tracking the reference velocity ν_{ref}, the controller introduces a velocity tracking error $e_v(\theta)$, which needs to be minimized to ensure robust platoon control in the context of a WNCS system. Accordingly, the kinematic relations in 6 can be rewritten in their linear form as follows [18].

$$\dot{Z}_v(\theta) = e_{1,v}(\theta) + h(\xi_v(\theta)),$$

$$\dot{e}_v(\theta) = \mathrm{A} e_v(\theta) + \mathrm{B} u_v(\theta) + \rho(\xi_v(\theta))\, \omega_v(\theta) \tag{7}$$

where $e_v = [e_{1,v}, \cdots e_{N-1,v}]^T$.

Since we consider a WNCS-based platoon, external disturbances may arise from vehicle dynamics, unreliable communication, or sensing imperfections that cause delays or the loss of critical information required for control decision-making [19, 22, 26]. Accordingly, $\omega_v(\theta)$ accounts for ω_v^{cont}, ω_v^{ISAC}, and ω_v^{comp}, representing disturbances in control, integrated sensing and communication, and resource-constrained computing systems, respectively. These factors may lead to processing delays or information loss that affect control performance.

Recent studies on controller design have shown promising results in integrating multi-agent reinforcement learning (MARL) with Proportional-Integral-Derivative (PID) control, which can be applied to vehicle platoon control to address system complexity, nonlinearity, and uncertainties arising from rapid variations in system states over time [4, 27].

Figure 6 illustrates the MARL-based PID control, where disturbances from the integrated sensing and communication system are considered. Deep reinforcement learning (DRL) agents, as described in [4], can be trained to map the system state (e.g., e_v for control, or PDR, latency, signal-to-noise ratio (SNR), velocity, and distance for the ISAC system state).

As shown in **Figure 6**, the velocity error vector is computed from the reference signal ν_{ref} and the measured vehicle velocity. This error represents the system state, which is mapped to an optimal action according to the trained DRL policy. The resulting action determines the PID gain vector that specifies the parameters k_p, k_i, and k_d, used to generate the control input u_v for the ACC process, which is also affected by the external disturbance ω_v^{cont}. Due to space limitations, we refer to [4, 27] for a detailed analysis of this control process.

Furthermore, incorporating ISAC-related disturbances into the string stability control framework can enhance its performance. In this context, the DeModulation Reference Signal (DMRS) sensing technique for ISAC in 5 G-A and 6 G systems can be leveraged to estimate the maximum sensing range and trackable velocity using radar-based sensing [28, 29]. The DMRS-based velocity and distance estimations are

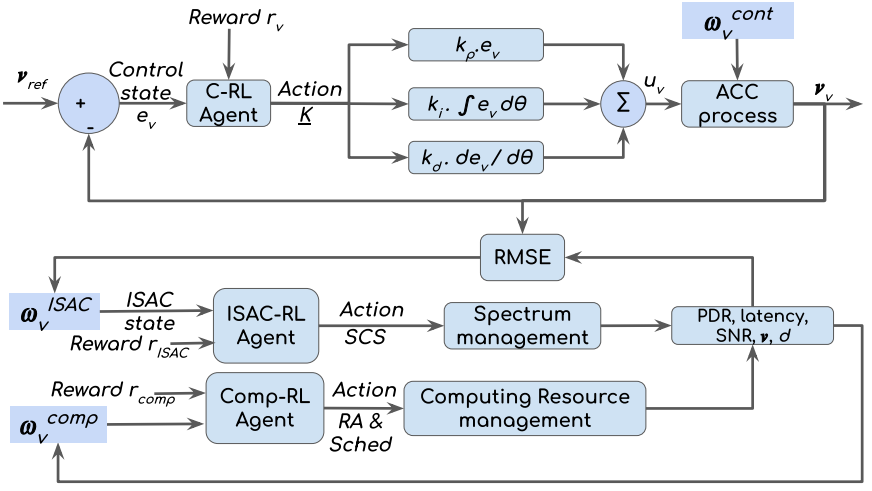


Figure 6.
MARL-based PID controller for string-stable platoon.

compared with measured values using root mean square error (RMSE), which contributes to disturbance estimation alongside PDR, latency, and SNR in sidelink communication. Based on the ISAC system state, a trained ISAC-RL agent determines the optimal subcarrier spacing and 5 G radio spectrum numerology pattern to improve wireless channel reliability, minimize PDR, RMSE (for velocity and distance), and latency, and maximize SNR [30].

Likewise, the computing agent accounts for disturbances arising from computational performance, which also affect the overall system behavior. This includes the processing of radio communication functions and sensing signal data at the vehicular local computing nodes, as well as at centralized edge servers that handle offloaded tasks from the vehicle platoon [31, 32].

The following section discusses this proposed string stability control framework through the lens of O-RAN networks, highlighting key opportunities, challenges, and directions for future research.

4. String stability in open and intelligent WNCS

In earlier sections, we discussed the control foundation of the proposed methodology, including the components of vehicle platoons, their control mechanisms, and a framework for controller design within a WNCS, in which wireless communication is a key enabler. Building on this control framework, this section examines how string-stability platoon control is implemented at the system level when the vehicle platoon is modeled as a WNCS. In this context, communication delays, packet losses, sensing uncertainties, and computational constraints directly affect control performance. Accordingly, this section reviews O-RAN architectural components – including the RAN Intelligent Controller (RIC), xApps, rApps, and edge computing infrastructure – as system-level enablers that provide programmability, intelligence, and resource orchestration required to operationalize ISCCC within a WNCS.

O-RAN represents an open and intelligent Wireless Network Control System (WNCS) for ITS, transforming traditional wireless networks into use-case–centric platforms across transportation, health, agriculture, and other domains. Its key enablers – virtualization, disaggregation, open interfaces, and intelligence – collectively enable flexibility, scalability, interoperability, and cost efficiency. Virtualization decouples hardware from software, allowing RAN functions to run as open software on general-purpose hardware. Disaggregation separates the base station into open radio (O–RU), distributed (O–DU), and centralized (O–CU) units, with control (CU–CP) and user (CU–UP) planes enabling efficient deployment of RAN functions. Open interfaces standardize interconnections to support multi-vendor interoperability, while the RIC, in its non-RT and near-RT forms, hosts AI/ML applications for intelligent optimization and orchestration of RAN resources [3].

We refer the reader to [3, 33] for detailed discussions on O-RAN's architecture, evolution, and enabling technologies. In this section, we examine O-RAN as a network infrastructure for WNCS-based vehicle platoons and analyze its contribution to the string-stability control framework introduced in Section 3 through the lens of open, programmable, disaggregated, intelligent, and virtualized wireless networks.

4.1 O-RAN vehicular networks

O-RAN is still in its infancy, and its integration into vehicular networks remains largely unexplored. Few research efforts in the literature highlight the potential benefits of using O-RAN to support various applications in C–V2X, one of which is improving the reliability of wireless links that are essential for vehicle platoons, as discussed in Section 3.

Linsalata et al. [6] support the system-layer perspective introduced in this chapter for robust string-stability platoon control. In their work, the O-RAN near-real-time RIC is leveraged to implement an xApp for V2V relay selection when sidelink channels fail to meet reliability requirements for information exchange. This approach illustrates how O-RAN system-level intelligence can be integrated into a WNCS to support the control layer by adapting communication decisions in response to reliability constraints, which is essential for maintaining string stability in platoon control scenarios.

Likewise, Yoo et al and Lee et al. [34, 35] provide a system-layer perspective, which we introduce in this chapter, where the ISAC framework is integrated with O-RAN's open and programmable architecture, particularly at the network edge (near-RT RIC), to support joint sensing and resource allocation processing, which can be leveraged in the proposed string stability controller. These studies collectively indicate that O-RAN can serve as an intelligent and programmable network infrastructure that supports integrated sensing, communication, and computing for platoon control.

4.2 ISAC as a service

O-RAN's openness, disaggregation, and intelligence operational concepts can be leveraged to offer ISAC for platoon control as a service [36], supporting the leasing concept inspired by resource sharing in cloud computing, where various use cases of vehicle platoons utilize resources for a specific period (service lifetime) before releasing them for other use cases. This concept is introduced in the context of O-RAN design as network slicing, where on-demand virtual networks are created, instantiated, managed, and operated to support a specific use case (vehicle platoon control) for a defined lifetime (slice time), and then terminated at the end of that slice time. In this sense, ISAC is managed by O-RAN's computational resources (xApps and near-RT RIC) for ISAC's spectrum resource allocation to support platoon control. The discussion of the technical details of this design is beyond the scope of this chapter, but we refer to [37, 38] for further details.

4.3 Intelligent digital twin string stability control

As O-RAN offers programmability, resource and function virtualization, and intelligent agents that enable their incorporation into vehicle platoon control design, recent advances in ITS control have introduced a digital twin framework to augment the MARL-PID control framework [5], thereby supporting our perspective on the control-layer design for vehicle platoon control. The digital twin was originally developed to replicate physical and dynamic processes in a virtual environment to predict the behavior of a system under various operational conditions and gain sufficient information [39]. Recent advances in ITS control adopt the digital twin to

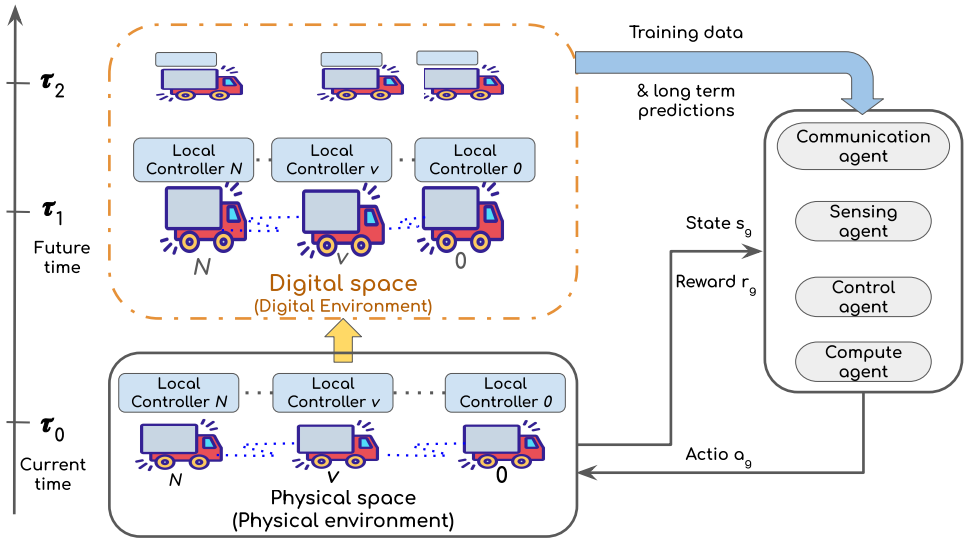


Figure 7.
Digital twin framework for ISCCC-based platoon control.

augment platoon control [5] by introducing a second-level global controller for the overall system, where one of the global control functions is vehicular network relay selection, as introduced in [6].

Figure 7 illustrates a digital twin framework that leverages O-RAN capabilities to deploy a global controller at the near-RT RIC[4]. In this framework, the overall system is replicated through multiple differentiated digital domains – including the road environment, transportation infrastructure, vehicle dynamics, vehicle sensors, vehicle controllers, spectrum virtualization, and computational resources – which collectively virtualize system behavior over time. The resulting predictions and state information are disseminated to a global MARL controller, which coordinates local platoon controllers to achieve robust, string-stable platoon operation, consistent with the system-layer methodological framework illustrated in **Figure 1**.

5. Opportunities, challenges, and future directions

In the following, we discuss research perspectives and application domains through the lens of the proposed ISCCC methodology, emphasizing how different deployment domains impose distinct constraints on string-stability platoon control. While the underlying control principles remain consistent, application domains such as logistics, agriculture, and industrial automated guided vehicles (AGVs) impose varying requirements on latency, reliability, energy efficiency, scalability, and human interaction. These constraint regimes shape how the multi-agent control layer and the WNCS abstraction are instantiated, and they highlight O-RAN's role as a unifying—but not uniform—enabling framework for adaptive platoon control.

[91] **Figure 7** is inspired by work in [5].

Within this context, O-RAN augments platoon-control design by enabling multi-agent coordination, efficient resource sharing through network slicing, and open software platforms that support portable control applications integrated with underlying system software via xApps. It further provides accessible human–machine interfaces for network monitoring by users with limited digital literacy and facilitates deployment in resource-constrained regions through open-source, interoperable O-RAN solutions. However, these opportunities are accompanied by several technical challenges that researchers in academia and industry are actively investigating.

Accordingly, the related work discussed in the following sections is interpreted through the methodological framework introduced in this chapter and visualized in **Figure 1**, with a particular focus on the system-layer perspective. Specifically, these studies are reviewed with respect to how multiple agents within the system layer interact with one another, how O-RAN-enabled intelligence and orchestration support these interactions, and how the system layer, in turn, enables and constrains the application layer across different deployment domains. Based on this perspective, we outline the identified opportunities, discuss the associated challenges, and highlight directions for future research.

5.1 Multi-agent communication-control co-design

In a vehicle platoon, string stability control interplays with other control agents in the ITS, such as traffic signal control [40] and lane-change maneuver control [41], which, depending on the platoon strategy, can alter the platoon's formation and, in some cases, the leader–follower configuration. Consequently, the dynamic variations in platoon topology require high-frequency, event-triggered information exchange among control agents due to the volume of state changes in the platoon system, as well as a hierarchical controller design (e.g., a global controller and distributed local controllers).

5.1.1 Opportunities

By leveraging O-RAN's multi-layer control framework (Non-RT and Near-RT RIC), hierarchical platoon control architectures can be implemented as xApps and rApps[5]. O-RAN offers several opportunities to realize hierarchical controller designs that effectively coordinate these distributed control agents with each other and with the centralized controller through xApps that can potentially migrate or be instantiated on off-the-shelf general-purpose computing devices.

5.1.2 Challenges

Although O-RAN provides these opportunities for multi-agent and hierarchical control design, several key challenges remain to be addressed in the context of vehicle platoon control systems, where communication–control co-design remains a major issue. These include the optimal placement of controllers that communicate wirelessly to exchange control information while ensuring that QoC metrics are coupled with wireless communication metrics (e.g., PDR, jitter, delay);

[92] ːApps are Near-RT RIC functions operating at a latency timescale of 10 ms to 1 s, whereas rApps are Non-RT RIC functions operating at a latency timescale greater than 1 s.

synchronization of control actions for safety-critical applications (e.g., road safety); and the placement of control functions (xApps and rApps) to ensure these applications are achieved in a timely manner.

5.1.3 Future directions

The aforementioned challenges open new directions for future research in controller design and function placement within the context of communication–control co-design [42], where platoon string stability requires timely and reliable control actions. Three major research directions emerge from these challenges:

- **Communication–control synchronization:** this represents a complex network problem with strict synchronization requirements that may benefit from applying results from random graph theory [43], particularly for synchronizing distributed control actions in wireless communication environments with inherent limitations, where retransmissions due to channel impairments need to be managed to support vehicle platooning safety-critical applications.

- **O-RAN controller placement problem:** research in [44, 45] can be extended to incorporate control and road safety performance metrics as design constraints for the controller placement problem that would run communication network and ITS control functions.

- **Coordinated ITS and network function placement:** the placement of network and ITS control functions across roadside and O-RAN wireless network infrastructures is crucial for safety-critical applications. Unlike O-RAN RIC controller placement, which focuses on deploying O-RAN network functions, this coordination problem involves determining where to host ITS control functions and wireless network functions across heterogeneous infrastructures – either on O-RAN edge servers within the O-RAN domain or on ITS computational units, such as roadside units (RSUs). Selecting the appropriate infrastructure elements for processing these functions and enabling real-time relaying between them is essential to ensure timely and reliable control actions. This interplay between function placement and inter-infrastructure coordination opens a promising direction for future research in string stability control design.

5.2 Efficient resource sharing

As discussed earlier, the vehicle platoon is a ubiquitous model in various ITS environments and application domains such as logistics (trucks) and industry, that is, Autonomous Guided Vehicles (AGVs) and mobile robots, as well as agriculture (tractors). This makes the platoon one of the O-RAN use cases that does not operate continuously. Therefore, efficient resource-sharing mechanisms are required so that network and ITS resources can be shared effectively among multiple use cases.

5.2.1 Opportunities

O-RAN introduces the concept of network slicing, where on-demand virtual networks can be instantiated to support multiple use cases (e.g., logistics, industry,

and agriculture) with unique service requirements (e.g., latency and PDR) over a defined period (slice lifetime). Network slicing ensures performance isolation, meaning that degradation in one slice does not affect the performance of other active slices. In this sense, O-RAN can offer slicing services tailored to various vehicle platoon scenarios, as illustrated in **Figure 4**.

5.2.2 Challenges

The key challenge in deploying vehicle platoons within network slicing is tailoring heterogeneous resources (computing, network, wireless spectrum, and ITS entities) to support multiple use cases while ensuring performance isolation. This challenge encompasses a massive set of resource allocation and scheduling problems. Several critical issues remain to be addressed in the context of vehicle platoon control systems, where coordination among wireless spectrum, heterogeneous computing architectures, and network resources is essential.

These challenges include coordinated resource allocation and scheduling problems, in which coordination between ITS and O-RAN resource allocation is required to enable efficient resource sharing across multiple use cases, as well as numerology optimization for ISAC operations.

5.2.3 Future directions

The aforementioned challenges open new directions for future research in spectrum numerology optimization for ISAC and coordinated resource allocation and scheduling in the context of vehicle platoon string stability control:

- **Coordinated resource allocation:** This represents the end-to-end allocation of distributed and heterogeneous resources (network, computing, and ITS units) for vehicle platoon network slicing. Building on the theoretical contributions presented in [46], where notions of timing graphs have been adopted to develop robust coordinated resource allocation mechanisms for heterogeneous resources, ITS resources (e.g., RSUs), 5 G spectrum resources for V2N communication, edge computing resources (FPGA, CPU, and GPU), and transport network elements (front-haul and back-haul links, switches, and routers) need to be allocated in a coordinated manner to meet the strict timing requirements of the vehicle platoon slice. In this sense, the slice can be treated as a supply chain in which distributed resources must be shared to support a coordinated chain of network and ITS functions, following the theoretical foundations introduced in [47].

- **Coordinated scheduling:** Analogous to coordinated resource allocation, coordinated scheduling is essential for online resource sharing. This problem can be explored by extending research in coordinated supply chain scheduling, where the scheduling of multiple manufacturing operations [23, 48, 49] parallels the coordination of network and ITS scheduling in vehicle platoon control slicing design.

- **Numerology optimization for ISAC to support vehicle platoon control:** The accuracy of environmental sensing is closely coupled with the reliability of the

sidelink communication channel (V2V). A trade-off exists between radar and 5 G NR spectrum utilization, making numerology optimization—a process of allocating physical radio resource blocks according to subcarrier spacing patterns—crucial for ISAC operations in vehicle platoon slicing [38].

5.3 Security and privacy

Analogous to all CPS systems that rely on software and networked infrastructures to manage their control framework, O-RAN–based vehicle platoon control systems – viewed as moving-target systems – are vulnerable to several types of cyberattacks, including Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS). Nevertheless, the openness and disaggregation of the O-RAN architecture, the heterogeneity of resources, and the distribution of functions and control entities add further dimensions to the security and privacy problem. In this context, ITS data are exchanged among various entities to support intelligent decision-making, thereby expanding the attack surface. Therefore, rethinking countermeasures for security threats and maintaining data privacy in ITS have become mandatory design requirements.

5.3.1 Opportunities

The O-RAN Alliance is advancing security protocols for several O-RAN components, for example, open interfaces. The O-RAN threat model shows more than 160 distinct threats targeting O-RAN interfaces, network functions, and other architectural elements [50]. New threats have been identified against shared O–RUs, cached application data, AI/ML modules, local O-RU user management, and other O-RAN entities. These ongoing developments provide an opportunity to extend O-RAN's security architecture toward securing safety-critical vehicular control systems.

5.3.2 Challenges

Several challenges remain in securing O-RAN and ITS for vehicle platoon deployment. One major concern is *side-channel attacks* arising from the shared use of heterogeneous resources (computing, network, spectrum, and ITS entities). These attacks exploit information leakage at the hardware, software, or network levels, potentially exposing sensitive control data. For example, hardware vulnerabilities such as Specter and Meltdown allow attackers to exploit speculative execution to access privileged memory and extract sensitive data across virtual machines [51]. In multi-tenant environments, an attacker may execute a malicious xApp co-residing on the same physical infrastructure (InP) as the victim, leading to cross-InP[6] attacks. Likewise, the heterogeneity of both O-RAN and ITS resources exacerbates the threat, making data and control exchanges more vulnerable to privacy breaches.

5.3.3 Future directions

To mitigate information leakage, side-channel attacks, and privacy risks in O-RAN–based vehicular platoon systems, we highlight a few directions for future research:

[95] nP refers to any physical infrastructure in the O-RAN-based ITS system, such as vehicle control software system, RSU, wireless channel, edge server, etc.

- **Side-channel attacks:** Side-channel attacks can occur at multiple layers – hardware, operating systems, spectrum, ITS entities, or network resources. In vehicle platoons, as noted earlier, the timing dimension is critical because resource scheduling directly affects control synchronization. We argue that coordinated, timing-aware scheduling countermeasures can help quantify and mitigate information leakage across heterogeneous domains. The scheduling-aware defense mechanism introduced in [52] illustrates the use of scheduling techniques to defend against cache-level prefetching side-channel attacks. Extending this concept, coordinated supply chain scheduling approaches [48] could be adapted to O-RAN-based VCPS to systematically quantify information leakage and develop effective timing-based defenses against side-channel attacks in the vehicle platoon.

- **Privacy of ITS and O-RAN users:** Differential privacy has recently been explored for vehicle platoon control as a VCPS, e.g., [53, 54]; however, it focuses on a single infrastructure domain, for example, the wireless communication domain, where protecting sensitive information during inter-vehicle exchanges remains a challenge in real-time, resource-constrained environments. Nevertheless, integrating differential privacy frameworks across ITS and O-RAN entities in vehicle platoon systems represents a promising direction for future research.

5.4 Deployment in resource-constrained regions

VCPS is a mobile system that operates across various regions, many of which are rural and have limited communication and energy infrastructure. These limitations directly affect the availability of communication and computing resources, as well as the electrical power required to support CV2X communications, which are essential for vehicle platoon control operations. Two potential alternatives for enhancing connectivity in such scenarios include the use of non-terrestrial wireless networks – such as drones and satellites. However, managing these heterogeneous wireless access technologies remains challenging. O-RAN can interoperate with community networks characterized by constrained energy and communication resources. Recent advances demonstrate the successful deployment of open-source solutions, such as MAGMA, to extend coverage in resource-constrained regions, as shown in Peru [55].

5.4.1 Opportunities

O-RAN can interoperate with open-source community network systems, such as MAGMA [55], through coordinated network control planes to extend coverage into rural regions. The flexibility and portability of community network platforms (e.g., MAGMA) enable them to incorporate partial O-RAN functionalities required to interface with major O-RAN systems and their open interfaces. These systems also provide user-friendly management interfaces suitable for moderately skilled operators. Furthermore, they support remote management and require low computational power, enabling continuous operation with an uninterruptible power supply (UPS) attached to a local computing unit that hosts the community network with O-RAN functionality.

5.4.2 Challenges

Several key challenges arise when extending O-RAN functionality to community networks. First, community network platforms such as MAGMA have recently demonstrated the ability to extend core network capabilities to the wireless edge. In contrast, O-RAN focuses on RAN capabilities. Integrating these two domains requires rethinking the control and user-plane interface design to ensure seamless operation. Second, the limited and unstable energy supply in rural areas constrains both network availability and edge computing performance. Third, heterogeneity across communication interfaces and devices increases the complexity of maintaining interoperability and end-to-end QoS guarantees under fluctuating energy and connectivity conditions.

5.4.3 Future directions

The successful deployment of community networks to support vehicle platoon services in resource-constrained regions requires extending community network research and implementation to encompass access-network functionalities in addition to core-network capabilities. Future work should focus on developing lightweight, interoperable interfaces between the community network and O-RAN components, while accounting for energy diversity, intermittent connectivity, and the coexistence of other wireless access technologies that interoperate with CV2X, such as DSRC and non-terrestrial communication systems. Such integration would enable distributed RAN control and localized edge intelligence in rural regions, supporting resilient and energy-efficient vehicle platoon communication services.

5.5 Human-vehicle interaction

In ITS, vehicles are viewed as automotive systems that integrate dynamic sensing, communication, and computing. One of the major design considerations in vehicle platoon control is the human factor [56], where understanding human perception and reaction is essential for road safety. Assisted and semi-automated systems remain largely human-operated or hybrid, as fully automated platoons are still limited to industrial and agricultural use cases. Nevertheless, operators interact with AI/ML-enabled systems to configure and manage autonomous vehicles [57]. Therefore, understanding and modeling human behavior remain central to the design of safe platoons.

5.5.1 Opportunities

O-RAN and ITS research offer opportunities to integrate human-centered intelligence into vehicular networks [6]. O-RAN can enable adaptive human–vehicle interaction mechanisms – for instance, by supporting proactive risk assessment and driver intention recognition through AI-powered xApps. Likewise, O-RAN and 5 GAA are working on the development of interoperable systems that leverage contextual sensing data (e.g., DMRS-based sensing) to enhance driver assistance, trust, and safety awareness in platoons [58].

Nevertheless, leveraging these opportunities for platoon control depends on addressing the human factors involved in vehicle–network interaction. In practice,

integrating human drivers and operators into AI-powered O-RAN systems introduces behavioral and cognitive challenges that can influence system reliability and safety.

5.5.2 Challenges

Because the driver-hiring process does not require specific IT qualifications, human–vehicle interaction poses key challenges for vehicle platoon control in O-RAN-enabled ITS environments. The first challenge is drivers' limited digital literacy, which can hinder effective engagement with O-RAN-based ITS interfaces and reduce situational awareness. Moreover, accurately modeling driver behavior – while accounting for cultural, cognitive, and physiological factors – is a complex task that directly affects cooperative control performance. Furthermore, incorporating human-intention data into platoon control loops introduces challenges related to latency, privacy, and computational complexity, owing to the need for real-time data collection and processing. Finally, maintaining operator trust in AI-driven platoon systems requires intuitive human–machine interfaces designed to clearly convey system states and control decisions, which are essential for fostering user confidence and reliable interaction [58].

Addressing these challenges requires a holistic, user-centric ITS network design. In this context, low digital literacy and trust gaps can be mitigated through human-centered frameworks that quantify drivers' perceptions, acceptance, and interactions with advanced vehicular systems. Likewise, the complexity of driver modeling and real-time intention tracking requires adaptive network intelligence capable of learning and responding to human behavior. These needs open avenues for further research that leverages behavioral science, intelligent control, and O-RAN capabilities to develop safer and more intuitive platoon systems.

5.5.3 Future directions

Given the challenges mentioned above, enhancing drivers' awareness and acceptance in ITS environments is a key design objective for O-RAN-based vehicle platoons. Therefore, we argue that adopting the *Technology Acceptance Model* (TAM) can provide valuable insights into user behavior, trust, and intention to adopt novel ITS and O-RAN technologies, as well as how drivers interact with emerging automated systems [59]. Quantitative and qualitative research should be conducted in real-world road trials to measure and model drivers' behavior and their interactions with other ITS and O-RAN entities. In this sense, the performance of integrating O-RAN within ITS can be evaluated by assessing how O-RICs (e.g., Near-RT RIC) leverage collected driver-behavior data for adaptive control decisions. For instance, research on fusing stochastic driver models [60] with real-time edge intelligence to capture driver behavior and interactions with ITS components can be extended to O-RAN-based platoon control systems, thereby enabling proactive and safety-aware platoon management. Such human-centered integration will be crucial for advancing cooperative, reliable, and road user-accepted vehicular control systems.

Table 2 summarizes our discussion of the opportunities that O-RAN presents for string stability, the associated challenges, and how these technical challenges shape directions for future research.

Design consideration	Opportunities	Challenges	Directions
Communication-control co-design	O-RAN multi-layer control framework (near-RT RIC and non-RT RIC)	Controller placement and communication-control synchronization	Research on random graphs for synchronization, controller placement, and coordinated function placement, e.g., [43, 44].
Resource sharing	Network slicing	Coordinated resource allocation and scheduling	Rethinking timing graph and coordinated supply chain management in the context of network slicing, resource sharing, as well as numerology optimization for ISAC-based vehicle platoon, e.g., [38, 46–48].
Security	Developing open interfaces, threat models, and risk analysis	Side-channel attacks and privacy breaches	Revisiting timing-aware coordinated scheduling countermeasures against side-channel attacks and differential privacy algorithms for O-RAN-ITS data privacy, e.g., [52, 53].
Resource-constrained regions	Open-source, low-cost, and portable software solution	Network interfaces design and energy limitations	Interoperable interfaces and dynamic spectrum management, e.g., [55].
Human-machine interaction	AI-powered xApps for proactive risk assessment and driver intention recognition	Limited digital literacy, modeling driver behavior, and incorporating human intention data into the control loop.	Leverage TAM and behavior models for human-vehicle interaction, e.g., [56, 59].

Table 2.
Opportunities, challenges, and future directions.

6. Conclusion

Vehicle platoons have become ubiquitous across multiple domains – logistics, agriculture, and industry – owing to their potential to reduce energy and fuel consumption, shorten travel times, and enhance road safety. *String stability* remains central to platoon control design for achieving these objectives. Recent advances in ITS have introduced string stability in the context of a WNCS, where sensing, communication, and computing are integrated with control mechanisms to ensure robust platoon operation.

This chapter provided a comprehensive overview of string-stability control design, offering guidelines for a multi-agent string-stability framework that leverages recent research advances in platoon control. It also discussed how O-RAN capabilities – such as openness, programmability, disaggregation, and intelligence – can support the proposed integrated multi-agent communication–control framework. Recognizing that O-RAN remains under development, the chapter examined its opportunities, key challenges, and emerging research directions for realizing string-stable platoons in open and intelligent wireless systems.

6.1 Key takeaways

- A research gap exists in the literature on multi-agent communication–control frameworks for string stability that explicitly considers O-RAN design principles.
- Human factors and human–machine interaction are critical to achieving road safety in semi-automated platoons, yet the intersection of O-RAN and ITS from a human-centered perspective remains largely unexplored.
- Coordinated relaying between ITS components (e.g., RSUs) and O-RAN entities is crucial for addressing coverage limitations in resource-constrained regions.

6.2 Limitations and future work

Although this chapter synthesizes current research and proposes a conceptual framework, several limitations remain, opening promising avenues for future research:

- The proposed control framework serves as a set of design guidelines without an implementation prototype, leaving room for validation and experimental evaluation.
- The framework does not capture all potential disturbance models or information-exchange patterns within platoon networks.
- The influence of vehicle routing on platoon control—particularly in coverage-aware and reliability-aware routing—remains unaddressed.
- The concept of *platoon slicing* warrants further investigation, particularly in containerized edge environments where different resource- and function-level virtualization technologies could support platoon control applications.

Addressing these limitations and the broader challenges identified throughout the chapter will advance research on automated and connected vehicles, fostering resilient, intelligent, and human-centered vehicular control systems.

Acknowledgments

Authors acknowledge the use of OpenAI's ChatGPT (GPT-5) as a writing and editing assistant in refining the clarity, grammar, and cohesion of the text. The tool was used solely to improve language presentation and structural flow; all ideas, analyses, and conclusions presented in this chapter are the authors' own.

Abbreviations

ACC	Adaptive Cruise Control
CAVs	Connected and Automated Vehicles

Comp-RL	Computing Reinforcement Learning agent[7]
CPS	Cyber-Physical System
C-RL	Control Reinforcement Learning agent[8]
C-V2X	Cellular-based Vehicle-to-Everything
CU-CP	O-RAN Control Unit of Control Plane
CU-UP	O-RAN Control Unit of User Plane
DDoS	Distributed Denial-of-Service (DDoS)
DMRS	DeModulation Reference Signal
DoS	Denial-of-Service (DoS)
DRL	Deep Reinforcement Learning
DSRC	Dedicated Short Range Communication
DSS	Disturbance String Stability
FEC	Forward Error Correction
IFT	Information Flow Topology
ISAC	Integrated Sensing and Communication
ISAC-RL	ISAC Reinforcement Learning agent[9]
ISCCC	Integrated Sensing, Communication, Computation, and Control
ISS	Input-to-State Stability
ITS	Intelligent Transportation System
IoV	Internet of Vehicles
MARL	Multi-Agent Reinforcement Learning
MEC	Multiple-access Edge Computing
Near RT-RIC	Near Real-Time RIC
O-CU	O-RAN Control Unit
O-DU	O-RAN Distribute Unit
O-RAN	Open Radio Access Network
O-RU	O-RAN Radio Unit
PDR	Packet Drop Rate
QoC	Quality of ControlQoS Quality of Service
rApp	O-RAN Non-RT RIC r Application (r denotes a generic name)
RIC	RAN Intelligent Controller
RMSE	Root Mean Square Error
SCS	Subcarrier Spacing
SNR	Signal-to-Noise Ratio
TAM	Technology Acceptance Model
V2N	Vehicle-to-Network communication
V2V	Vehicle-to-Vehicle communication
VCPS	Vehicular Cyber-Physical System
WNCS	Wireless Networked Control System
xApp	O-RAN near-RT RIC x Application (x denotes a generic name)

[101] Jsed for computing resources decision making.

[8] Used for control actions decision making.

[9] Used for ISAC decision making.

Author details

Emad El-Din Mazied[1,2*] and Hesham A. Rakha[3,4]

1 Computer Science Department, Virginia Tech, Blacksburg, USA

2 Electrical Engineering Department, Sohag University, New Sohag, Egypt

3 Center for Sustainable Mobility, Virginia Tech Transportation Institute, Blacksburg, USA

4 The Charles Edward Via Jr. Department of Civil and Environmental Engineering, Virginia Tech, Blacksburg, USA

*Address all correspondence to: emazied@vt.edu

IntechOpen

© 2026 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] Lee J, Kim JH. Phantom traffic: Platoon formed at low traffic density. Journal of Transportation Engineering, Part A: Systems. 2019;**145**(2):4018082. DOI: 10.1061/JTEPBS.0000206

[2] Feng S, Zhang Y, Li SE, Cao Z, Liu HX, Li L. String stability for vehicular platoon control: Definitions and analysis methods. Annual Reviews in Control. 2019;**47**:81–97. DOI: 10.1016/j.arcontrol.2019.03.001

[3] Wani M, Kretschmer M, Schröder B, Grebe A, Rademacher M. Open ran: A concise overview. IEEE Open Journal of the Communications Society. 2025a;**6**:13–28

[4] Zhai Y, Zhao Q, Han Y, Wang J, Zeng W Intelligent pid controller based on deep reinforcement learning. In: International Conference on Robotics, Control and Automation (ICRCA). 2024a. p. 343–348

[5] Cheng N, Wang X, Li Z, Yin Z, Luan T, Shen X. Toward enhanced reinforcement learning-based resource management via digital twin: Opportunities, applications, and challenges. IEEE Network. 2025;**39**(1):189–196

[6] Linsalata F, Moro E, Gjeci F, Magarini M, Spagnolini U, Capone A. Addressing control challenges in vehicular networks through O-RAN: A novel architecture and simulation framework. IEEE Transactions on Vehicular Technology. 2024;**73**(7):9344–9355

[7] World Bank. Transport overview. September 2025. Avaliable from: https://www.worldbank.org/en/topic/transport/overview [Accessed: 2025-July-24]

[8] Atlas International. The impact of rising fuel costs in logistics. February 2025. Available from: https://www.atlasintl.com/blog/the-impact-of-rising-fuel-costs-in-logistics [Accessed: 2025-July-24]

[9] United Nations. Transport – General fact sheet. Technical report. New York, NY, USA: United Nations; 2021

[10] World Health Organization. Transport and health risks. August 2024. Available from: https://www.who.int/teams/environment-climate-change-and-health/healthy-urban-environments/transport/health-risks [Accessed: 2025-July-24]

[11] Garg M, Bouroche M. Longitudinal car-following control of connected autonomous vehicles in realistic scenarios: A survey. IEEE Transactions on Intelligent Transportation Systems. 2025;**26**(11):1–30

[12] Hao Q, Dong J, Zhao J. Adaptive cruise control algorithm for persistence and security of distributed heterogeneous vehicle platoon based on discrete-time control barrier function. IEEE Transactions on Vehicular Technology. 2025a;**74**(10):1–11

[13] Zhang Y, Chen X, Ma J, Yu L. Environmental impact of autonomous cars considering platooning with buses in urban scenarios. Elsevier Journal of Sustainable Cities and Society. 2024b;**101**:105–106. DOI: 10.1016/j.scs.2023.105106

[14] Sessa C, Alessandrini A, Flament M, Hoadley S, Pietroni F, Stam D. The Socio-Economic Impact of Urban Road Automation Scenarios: CityMobil2 Participatory Appraisal Exercise. Switzerland: Springer International Publishing; 2016. p. 163–186

[15] Brummitt P, Khan M. Truck platooning and its impact on fuel emissions. In: 2022 IEEE Green Technologies Conference (GreenTech). 2022. 130–135 DOI: 10.1109/GreenTech52845.2022.9772028

[16] Jia D, Lu K, Wang J, Zhang X, Shen X. A survey on platoon-based vehicular cyber-physical systems. IEEE Communications Surveys and Tutorials. 2016;**18**(1):263–284

[17] Jia D, Lu K, Wang J. On the network connectivity of platoon-based vehicular cyber-physical systems. Transportation Research Part C: Emerging Technologies. 2014;**40**: 215–230

[18] Besselink B, Johansson K. String stability and a delay-based spacing policy for vehicle platoons subject to disturbances. IEEE Transactions on Automatic Control. 2017;**62**(9): 4376–4391

[19] Wen D, Zhou Y, Li X, Shi Y, Huang K, Letaief K. A survey on integrated sensing, communication, and computation. IEEE Communications Surveys and Tutorials. 2024;**27**(5):3058–3098

[20] Wang Y, Wu S, Lei C, Jiao J, Zhang Q. A review on wireless networked control system: The communication perspective. IEEE Internet of Things Journal. 2023a;**11** (5):7499–7524

[21] Li Q, Chang B, Mei W, Chen Z. Semantic-Based Integrated Sensing, Computing, Communication, and Control for Goal-Oriented Applications. In: In the IEEE Proc. of WCNC'25, pages. IEEE. 2025b. 1–6

[22] Zhou Y, Feng Z, Song Z, Wei Z, Ma D, Meng Z, Cui Y, Pang Y, Zhang P. Integrated sensing, communication, and control driven multi-AGV closed-loop control. IEEE Transactions on Vehicular Technology. 2025a;**74**(7):10853–10868

[23] Chang B, Tang W, Yan X, Tong X, Chen Z. Integrated scheduling of sensing, communication, and control for mmwave/thz communications in cellular connected uav networks. IEEE Journal on Selected Areas in Communications. 2022;**40**(7): 2103–2113

[24] Gharaibeh A, Salahuddin MA, Hussini SJ, Khreishah A, Khalil I, Guizani M, Al-Fuqaha A. Smart cities: A survey on data management, security, and enabling technologies. IEEE Communications Surveys and Tutorials. 2017;**19**(4):2456–2501

[25] Rezaee H, Zhang K, Parisini T, Polycarpou MM. Cooperative adaptive cruise control in the presence of communication and radar stochastic data loss. IEEE Transactions on Intelligent Transportation Systems. 2024;**25**(6):4964–4976

[26] Zhang Y, Xu Z, Wang Z, Yao X, Xu Z. Impacts of communication delay on vehicle platoon string stability and its compensation strategy: A review. Elsevier Journal of Traffic and Transportation Engineering. 2023b;**10** (4):508–529

[27] Jiang K, Hua M, He X, Dong L, Zhou Q, Xu H, Sun C. Improving string

stability in cooperative adaptive cruise control through multiagent reinforcement learning with potential-driven motivation. IEEE Transactions on Artificial Intelligence. 2025a;**6**(5):1114–1127

[28] Chen Y, Guo J, Sun Y, Yao H, Liu Y, He Y. Sensing resource scheduling in 5G vRAN: An elastic approach. ACM Transactions on Internet of Things. 2025b;**6**(3):19:1–19:24

[29] Wei Z, Li F, Liu H, Chen X, Wu H, Han K, Feng Z. A 5G DMRS-based Signal for Integrated Sensing and Communication System. arXiv preprint arXiv:2312.02170, 2023

[30] Campolo C, Molinaro A, Romeo F, Bazzi A, Berthet A. 5G NR V2X: On the Impact of a Flexible Numerology on the Autonomous Sidelink Mode. In: 2019 IEEE 2nd 5G World Forum (5GWF). 2019. p. 102–107

[31] Wu Q, Wang S, Ge H, Fan P, Fan Q, Letaief K. Delay-sensitive task offloading in vehicular fog computing-assisted platoons. IEEE Transactions on Network and Service Management. 2024;**21**(2):2012–2026

[32] Rzig I, Jaafar W, Jebalia M, Tabbane S. Energy-efficient vehicular task offloading using multi-mode MEC and RIS-equipped aerial platforms. IEEE Open Journal of the Communications Society. 2025;**6**:7604–7619

[33] He Y, Yu G, Wang X, Wang Q, Niu Z, Ni W, Liu R. Accountability and reliability in 6G O-RAN: Who is responsible when it fails? IEEE Wireless Communications. 2025c;**32**(2):52–59

[34] Yoo H, Lee S, Kim G, Rhee J, Hong E. Dedicated communication for sensing: A new use case for private 5g and open ran for mmtc. Journal of Communications and Networks. 2025;**27**(3):200–207

[35] Lee C, Oh J, Cho S Joint resource allocation and power efficiency optimization for O-RAN based ISAC. In: 2025 International Conference on Artificial Intelligence in Information and Communication (ICAIIC). 2025. p. 15–17

[36] Dong F, Liu F, Cui Y, Wang W, Han K, Wang Z. Sensing as a service in 6G perceptive networks: A unified framework for ISAC resource allocation. IEEE Transactions on Wireless Communications. 2023;**22**(5):3522–3536

[37] Li Y, Hu F, Liu Y, Zhao J. Hierarchical network slicing resource allocation for ISAC vehicular networks. In: 2024 IEEE/CIC International Conference on Communications in China (ICCC Workshops). 2024c. p. 335–340

[38] Hossain M, Xiang A, Kiani A, Saboorian T, Kaippallimalil J, Ansari N. AI-assisted E2E network slicing for integrated sensing and communication in 6G networks. IEEE Internet of Things Journal. 2024a;**11**(6):10627–10634

[39] Haag S, Anderl R. Digital twin–proof of concept. Manufacturing Letters. 2018;**15**:64–66

[40] Shen L, Liu R, Yao Z, Wu W, Yang H. Development of dynamic platoon dispersion models for predictive traffic signal control. IEEE Transactions on Intelligent Transportation Systems. 2018;**20**(2):431–440

[41] Badnava S, Meskin N, Gastli A, Al-Hitmi M, Ghommam J, Mesbah M, Mnif F. Platoon transitional maneuver control system: A review. IEEE Access. 2021;**9**:88327–88347

[42] Qiao Y, Fu Y, Yuan M. Communication–control co-design in wireless networks: A cloud control AGV example. IEEE Internet of Things Journal. 2023c;**10**(3):2346–2359

[43] Lu J, Chen G. A time-varying complex dynamical network model and its controlled synchronization criteria. IEEE Transactions on Automatic Control. 2005;**50**(6):841–846

[44] Abdel-Rahman M, Mazied E, Hassan F, Teague K, Mackenzie A, Midkiff S, Cardoso K, Nikolopoulos D. On robust optimal joint deployment and assignment of RAN intelligent controllers in O-RANs. IEEE Open Journal of the Communications Society. 2024b;**5**:2358–2376

[45] Mazied A, ElNainay M, Abdel-Rahman M, Midkiff S, Rizk M, Rakha H, MacKenzie A. The wireless control plane: An overview and directions for future research. Journal of Network and Computer Applications. 2019;**126**: 104–122

[46] Baxter A, Keskinocak P, Singh M. Heterogeneous multi-resource planning and allocation under stochastic demand. INFORMS Journal on Computing. 2023;**35**(5): 929–951

[47] Thomas D, Griffin P. Coordinated supply chain management. European Journal of Operational Research. 1996;**94**(1):1–15

[48] Sawik T. Coordinated supply chain scheduling. International Journal of Production Economics. 2009;**120** (2):437–451

[49] Jamrus T, Wang H, Chien C. Dynamic coordinated scheduling for supply chain under uncertain production time to empower smart production for industry 3.5. Computers and Industrial Engineering. 2020;**142** (1063751):1–9

[50] O-RAN Alliance. O-RAN ALLIANCE Security Update 2025. Available from: https://www.o-ran.org/blog/o-ran-alliance-security-update-2025, 2025. [Accessed: 2025-October]

[51] Jon Masters. What are Meltdown and Spectre? Here's what you need to know. Available from: https://www.redhat.com/en/blog/what-are-meltdown-and-spectre-heres-what-you-need-know, 2025. [Accessed: 2025-October]

[52] Schlüter T, Tippenhauer N. A scheduling-aware defense against prefetching-based side-channel attacks. 2024. Avaible from: https://arxiv.org/abs/2410.00452 [Accessed: 2024-September-16]

[53] Basak S, Chatterjee K, Singh A. DPPT: A Differential Privacy Preservation Technique for cyber–physical system. Computers and Electrical Engineering. 2023a;**109**:108661

[54] Zhang K, Li Z, Lin W. Distributed platoon control under quantization: Stability analysis and privacy preservation. 2025b. Available from: https://arxiv.org/abs/2510.05959 [Accessed: 2024-September-16]

[55] Hasan S, et al. Building flexible, low-cost wireless access networks with magma. In: Proc. USENIX NSDI'23. 2023b. p. 1667–1681

[56] Atmaca U, Maple C, Epiphaniou G, Sheik A. Human factors for vehicle platooning: A review. IET Conference Proceedings. 2021;**2021**:33–38

[57] Passalacqua M, Pellerin R, Magnani F, Doyon-Poulin P, Del-Aguila L, Boasen J, Leger P. Human-centred AI in industry 5.0: A systematic review. International Journal of Production Research. 2025b;**63** (7):2638–2669

[58] 5G Automotive Association (5GAA). Creating Trust in Connected and Automated Vehicles: A Human-Centric Perspective on Safety, Security, and Privacy. Technical report. 5G Automotive Association; 2024. [Accessed: 2025-October-11]

[59] Choi J, Ji Y. Investigating the importance of trust on adopting an autonomous vehicle. International Journal of Human-Computer Interaction. 2015;**31**(10):692–702. DOI: 10.1080/10447318.2015.1070549

[60] Hu J, Wang S, Zhang Y, Wang H, Liu Z, Cao G. Safety-aware human-lead vehicle platooning by proactively reacting to uncertain human behaving. Transportation Research Part C: Emerging Technologies. 2025;**170**:104941:1–104941:15

Section 2

Security and Resilience

Chapter 5

Security and Resilience in Autonomous Vehicles: A Proactive Design Approach

Chieh Tsai, Murad Mehrab Abrar and Salim Hariri

Abstract

Autonomous vehicles (AVs) promise efficient, clean, and cost-effective transportation systems, but their reliance on sensors, wireless communications, and decision-making systems makes them vulnerable to cyberattacks and physical threats. This chapter presents novel design techniques to strengthen the security and resilience of AVs. Firstly, we provide a taxonomy of potential attacks across different architectural layers, from perception and control manipulation to vehicle-to-any (V2X) communication exploits and software supply chain compromises. Building on this analysis, we present an AV resilient architecture that integrates redundancy, diversity, and adaptive reconfiguration strategies, supported by anomaly- and hash-based intrusion detection techniques. Experimental validation on the Quanser QCar platform demonstrates the effectiveness of these methods in detecting depth camera blinding attacks and software tampering of perception modules. The results highlight how fast anomaly detection combined with fallback and backup mechanisms ensures operational continuity, even under adversarial conditions. By linking layered threat modeling with practical defense implementations, this work advances AV resilience strategies for safer and more trustworthy autonomous vehicles.

Keywords: autonomous vehicles, cybersecurity, reslient AV, Anomaly detection, resilience AV architecture

1. Introduction

The emergence of autonomous vehicles (AVs) represents a transformative shift in transportation, with the potential to drastically improve road safety, traffic efficiency, and accessibility to mobility [1, 2]. By integrating complex subsystems such as, perception, localization, planning, and control, AVs operate with minimal or no human intervention. These systems rely on a wide range of sensors (e.g., LiDAR, cameras, radar), communication protocols (e.g., V2V [vehicle-to-vehicle], V2I), and artificial intelligence (AI) algorithms to make decisions in real time. However, this increasing system complexity also introduces new vulnerabilities [3, 4]. As AVs become more connected and data-driven, their attack

surface expands, exposing them to a wide range of cyber and physical threats that can compromise safety, reliability, and user trust.

Recent incidents and research have highlighted that autonomous systems are susceptible to adversarial manipulation at multiple layers – from sensor spoofing and GPS interference to model poisoning and control signal injection [5, 6]. These attacks not only pose risks to the integrity and availability of autonomous functions but may also lead to catastrophic physical consequences, including loss-of-life collisions and traffic disruption. Therefore, ensuring the security and resilience of AVs have become a critical research challenge, requiring robust threat modeling, proactive defense mechanisms, and intelligent detection systems capable of responding in real time.

Traditional cybersecurity techniques, while foundational, are often insufficient to address the dynamic and real-time constraints of AVs. A resilience-focused approach – one that utilizes redundancy, diversity, and adaptive response mechanisms – is essential for maintaining critical functionality in the presence of faults or attacks [7, 8]. Moreover, the development of lightweight, real-time anomaly detection systems and self-recovery mechanisms is crucial to support operational continuity under adversarial conditions.

This chapter aims to provide a comprehensive overview of the threat landscape in autonomous systems and explore state-of-the-art methodologies for enhancing their security and resilience. We begin by outlining the motivation for AV-specific security measures, followed by a taxonomy of known attacks and an evaluation of current anomaly detection and mitigation techniques. We then introduce a layered threat modeling framework and propose a set of practical defense strategies, supported by experimental demonstrations using a physical AV platform. Finally, we present an AV resilience architecture that integrates detection, validation, and fallback strategies, paving the way for more robust and trustworthy operations of autonomous systems.

2. Background and related work

2.1 Major AV components

AVs are generally organized into three major components: perception, planning, and control [9, 10]. Planning and control together define how the vehicle determines a feasible path and executes the necessary maneuvers to follow it safely. Perception, however, forms the foundation of this pipeline, as it equips the vehicle with awareness of its surrounding environment [11, 12]. A perception system integrates data from multiple sensors, such as LiDAR, radar, and cameras, enabling the detection, localization, and tracking of objects and road features. The importance of perception lies in its role as the primary source of information for autonomous navigation; without reliable perception, subsequent planning and control processes cannot operate effectively.

2.1.1 Perception system attacks

Recent studies have conducted real-world experiments on remote attacks against these perception sensors [13, 14]. The perception system plays a central role in

autonomous driving, as it integrates a diverse suite of sensors, such as cameras, LiDAR, radar, ultrasonic sensors, GPS, and inertial measurement unit (IMU) to construct an accurate understanding of the surrounding environment. Since each of these components contributes uniquely to situational awareness, the compromise of even a single sensor can degrade perception accuracy and mislead decision-making modules [15].

2.1.2 Perception security

To secure vehicle perception, a robust detection system, along with a mitigation strategy, is crucial. Based on the existing literature [13, 15–19], the current approaches for detecting perception sensor attacks against AVs can be categorized as follows: (i) incorporating redundancy by adding more sensors, (ii) cross-vehicle verification through V2V communication, and (iii) relying on alternative sensors and sensor fusion. Although sensor redundancy improves resilience against random attacks, it is ineffective against intentional attacks specific to a particular sensor, where the attacker has prior knowledge of the sensor. Using intervehicle communications like V2V to compare sensor measurements is ineffective when the victim vehicle is out of the communication range [20, 21]. Multimodal fusion, like combining LiDAR and camera data, has shown promising results in improving robustness under benign conditions but still struggles against coordinated multi-sensor adversarial attacks [22–25].

Recent work has explored adversarial training and certified defense mechanisms for perception models, aiming to improve robustness against crafted perturbations [25, 26]. However, these approaches often incur high computational costs and are limited to specific attack models, making them less practical for real-time autonomous driving [27, 28]. Thus, there remains a critical need for lightweight, adaptable defenses that can operate under diverse and evolving attack scenarios.

Given these limitations of the existing methods, there is a need for a holistic and resilient solution that can comprehensively detect and mitigate attacks without relying on specific sensors, sensor redundancy, or other vehicles and networks.

3. Redefining the AV architecture for threat and resilience modeling

In this work, the AV stack is intentionally redefined to emphasize resilience and security considerations. While conventional AV architectures typically separate the system into perception, planning, and control, here the stack is organized into distinct functional layers that more directly capture the operational roles and potential threat surfaces relevant to our study. Although the overall layered concept is inspired by prior work [29], the specific redefinition presented here is tailored to resilience analysis rather than being intended as a universal AV taxonomy.

- **Driver interface and control system**: provides the human driver with inputs and outputs, including steering feedback, dashboard displays, and manual override functions. This layer forms the boundary between human operators and the autonomous driving system. Modern AVs increasingly emphasize intuitive human–machine interfaces (HMIs), ensuring that drivers can safely monitor vehicle status and intervene during edge cases or system failures.

- **Control layer**: responsible for low-level actuation, such as steering, throttle, and braking, as well as implementing motion control algorithms to execute trajectories generated at higher levels. Advanced architectures often integrate high-frequency feedback loops, redundancy in actuation, and fail-safe control policies to guarantee safety in the presence of disturbances or component failures.

- **Decision-making layer**: manages tactical and strategic planning, including path planning, obstacle avoidance, and maneuver selection. This layer translates high-level goals into executable control commands. Current systems leverage reinforcement learning and optimization-based planners to handle complex traffic scenarios, dynamic obstacles, and rule-based constraints in real-time.

- **Knowledge processing layer (data fusion and interpretation)**: integrates heterogeneous data from multiple onboard sensors and external sources to maintain a coherent representation of the environment and vehicle state. In prior studies, this functionality was often included within the perception layer, but here it is explicitly separated to emphasize its role in resilience and security. Advanced architectures employ AI-driven sensor fusion and map-matching techniques to reduce uncertainty and dynamically adapt to changing conditions, thereby improving the robustness of situational awareness.

- **Perception layer**: processes raw sensor data (camera, LiDAR, radar, GPS, etc.) to perform object detection, tracking, and environmental mapping, which are essential for situational awareness. Recent approaches use deep neural networks for multi-modal perception and adopt adversarially robust methods to reduce susceptibility to spoofing, noise, or environmental disturbances.

- **Communication framework (V2V, V2I, V2C)**: supports information exchange between vehicles, infrastructure, and cloud services, enabling cooperative perception, coordinated maneuvers, and extended situational awareness. With the introduction of 5 G and cellular vehicle-to- any, this layer increasingly underpins cooperative driving, low-latency hazard alerts, and real-time map updates.

- **Cross-layer coordinator**: ensures synchronization, resilience, and consistency across all layers of the AV stack, maintaining reliable operations and overall system coherence. This cross-layer coordination is crucial for fault tolerance and safety assurance, as it enables graceful degradation, redundancy management, and system-wide cybersecurity monitoring.

4. Layer-based attack scenarios

To systematically evaluate threats in AVs, we adapt the IoT threat modeling framework [30] to the AV domain. Each architectural layer is examined in terms of its *core functions*, *attack surfaces*, *impact*, and *mitigation strategies*. This structured approach enables a consistent mapping between functional responsibilities and their associated vulnerabilities. Representative cases derived from this methodology are given in **Table 1**.

Layer	Attack surface (AS)	Impact	Mitigation strategy
Driver interface and control system	Malicious driver input injection; compromised dashboard/override signals.	Unauthorized override of system behavior; driver confusion leading to unsafe maneuvers.	Authenticate commands, ensure secure UI design, and implement redundant safety checks for manual override.
Control layer	Command injection in steering/braking; kernel-level rootkits.	Silent manipulation of vehicle dynamics, risk of collisions.	Runtime integrity monitoring, secure boot, anomaly detection in actuation signals.
Decision-making layer	Tampered ML models; adversarial inputs to the planning module.	Unsafe maneuvers, rule violations, unsafe path selection.	Model validation, adversarial robustness testing, consensus-based decision redundancy.
Knowledge processing layer	Data poisoning; sensor fusion manipulation	Distorted environmental model, leading to misinformed decisions.	Trusted data provenance, anomaly detection in fused data, hash-based detection, back up and fallback.
Perception layer	Sensor spoofing (LiDAR, radar, camera); adversarial image perturbations.	Incorrect object detection, phantom obstacles, missed hazards.	Sensor redundancy, adversarial training, anomaly detection.
Communication framework	V2V/V2I spoofing, replay, DoS, packet manipulation	Loss of situational awareness and degraded coordination between vehicles.	Encryption, authentication protocols, rate-limiting, intrusion detection systems
Cross-layer coordinator	Early-stage poisoning cascading through layers	System-wide compromise, cascading unsafe behavior	Cross-layer consistency checks, layered anomaly detection, resilient failover strategies.

Table 1.
Threat modeling for the proposed AV architecture. Each row summarizes the attack surface, safety impact, and candidate mitigation strategy.

4.1 Layer descriptions

The AV architecture can be conceptualized as a hierarchy of interdependent functional layers, each responsible for specific operations and each presenting unique attack surfaces.

At the top, the **driver interface and control system** links the human operator to the vehicle via dashboards, controls, and manual override mechanisms. Any compromise at this layer may confuse the driver, override legitimate commands, or inject malicious control inputs. Beneath it, the **control layer** governs low-level actuation, including throttle, steering, and braking. Attacks here can silently alter vehicle dynamics, producing deviations that are difficult to detect but potentially dangerous.

Building upward in abstraction, the **decision-making layer** manages tactical and strategic behaviors such as, lane changes, obstacle avoidance, and path planning. Manipulating decision models or outputs may lead to unsafe maneuvers or traffic violations. The **knowledge processing layer**, which fuses multisensor and external data into a coherent world model, is needed to support the decision-making processes. Poisoned streams or corrupted fusion algorithms can distort situational awareness and undermine downstream decisions.

The **perception layer** translates raw inputs from LiDAR, radar, cameras, and GPS into object detections, classifications, and environmental maps. It is especially exposed to spoofing, adversarial perturbations, and physical-world manipulations (e.g., altered traffic signs). Complementing perception, the **communication framework** handles information exchange with other vehicles, infrastructure, and the cloud via V2V, vehicle-to-infrastructure (V2I), and vehicle-to-cloud (V2C) links, respectively. Replay, spoofing, or denial-of-service attacks on this layer can disrupt cooperative driving and erode trust.

Finally, the **cross-layer coordinator** ensures synchronization and resilience across all layers. Because it influences the entire stack, faults or injected errors here can cascade through the architecture, destabilizing the system as a whole.

Together, these layers provide a structured visibility through which attacks can be mapped, analyzed, and countered using the five-step methodology.

In this chapter, we focus primarily on the perception and knowledge processing layers as case studies to demonstrate how resilience and security measures can be integrated into an AV system.

5. Security and resilience methodology

Based on the system architecture and identified mitigation strategies, we present an autonomous vehicle resilient (AVR) architecture in conjunction with targeted threat and intrusion detection techniques to enhance the security and operational robustness of AVs. The overall concept of the AVR architecture is illustrated in **Figure 1**, while the anomaly detection framework is depicted in **Figure 2**. Detailed mechanisms are discussed further in the following section.

5.1 AVR architecture

The **AVR architecture** is designed to operate across all functional layers of the AV stack, providing a systematic framework to anticipate, detect, and recover from failures or attacks. Its resilience is achieved through three complementary functions which are as follows:

- **Redundant functions** – critical modules are backed up by verified, functionally equivalent redundant modules to ensure continuity of operations in the event of component failures or malicious tampering. This approach reduces the risk of single points of failure and provides a safety net for vital system operations.

- **Diversity functions** – by incorporating heterogeneous sensors, algorithms, and models, the system mitigates common-mode failures and increases robustness against attacks that depend on existing vulnerabilities in a single type of module or data source.

- **Shuffle functions** – Periodic reconfiguration of software, communication channels, and system parameters introduces a high degree of ambiguity and, consequently, reduces the likelihood that adversaries can exploit deterministic system behaviors.

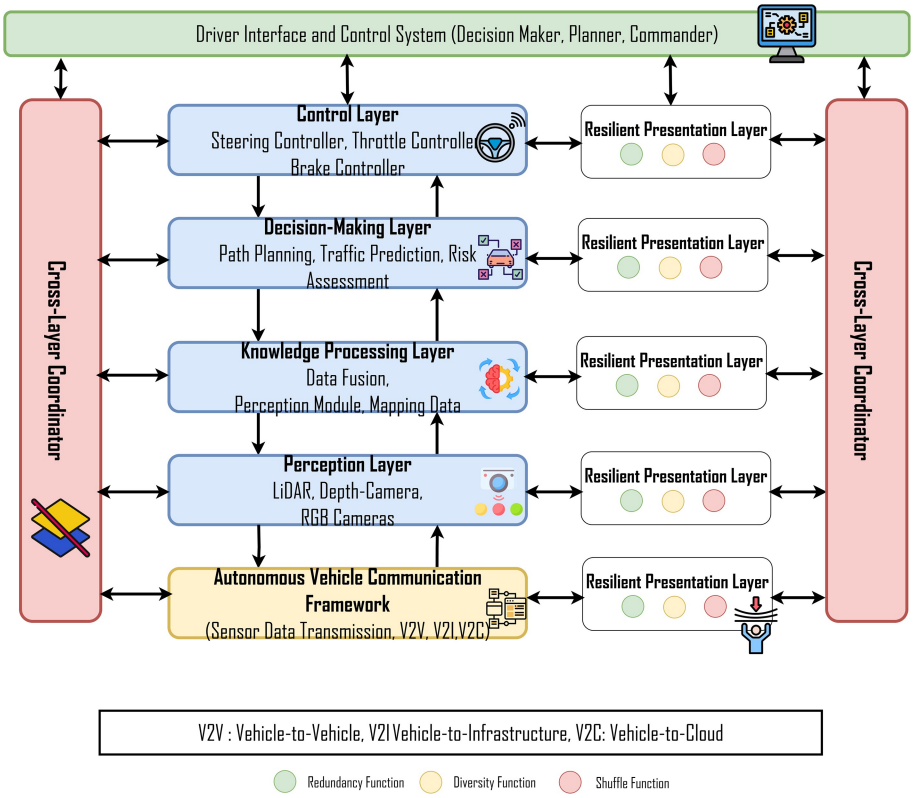


Figure 1.
AVR architecture is across AV functional layers and coordinated by a cross-layer coordinator.

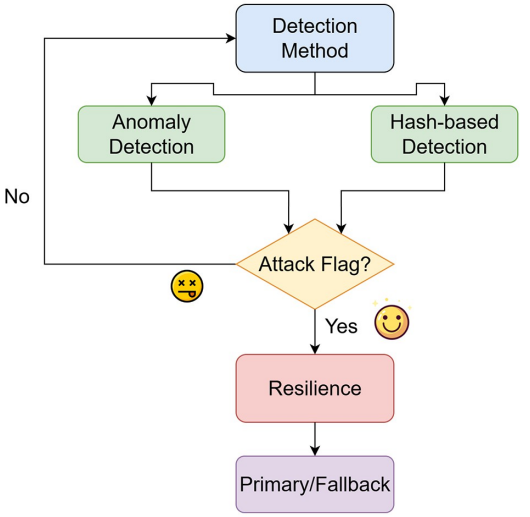


Figure 2.
Intrusion detection techniques: anomaly-based (perception) and hash-based (software/system integrity).

A dedicated **cross-layer coordinator** oversees these functions by monitoring anomalies, enforcing consistency across layers, and triggering dynamic reconfiguration when anomalies are detected. This ensures that multi-stage or stealthy attacks are isolated and mitigated before they can propagate, effectively enhancing overall AV system resilience.

5.1.1 Backup and fallback mechanism

We illustrate the backup and fallback concept through two operational scenarios: a *normal state* and a *failure state*. In the normal state, the **primary module (P)** executes normally, and no intervention is required. The system continues to operate smoothly as long as the detection function $D(\cdot)$ reports no anomalies.

In contrast, the failure state occurs when $D(P) = 1$ signals a compromise or fault in the primary module. At this point, control is immediately transferred to the **fallback module (F)**, which is a verified and trusted redundant module. The transition ensures that the system preserves safety-critical functions even under attack or malfunction.

Figure 3 depicts this mechanism: under normal conditions, the primary module operates, but upon detection of failure, the fallback module takes over seamlessly. This dual-scenario design embodies the redundancy principle of the AVR architecture, as shown in **Figure 1**.

5.2 Intrusion detection techniques

An intrusion detection system (IDS) is used in this work to provide real-time indications of compromises and to trigger resilience responses. We employ two complementary techniques: (i) anomaly-based detection to identify deviations in runtime behavior at the perception level, and (ii) hash-based integrity validation to detect unauthorized modifications to software artifacts (e.g., model weights and configuration files). These are described in the following subsections and together provide both behavioral and software integrity assurance.

5.2.1 Anomaly-based detection

Anomaly-based detection techniques identify unusual or unexpected system behavior that may indicate a cyberattack. They rely on a normal behavior model of

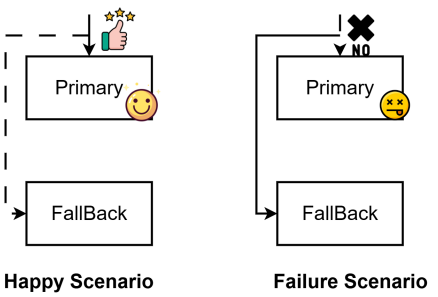


Figure 3.
Two operational scenarios for the backup/fallback mechanism: (1) happy state with primary execution, (2) failure state with automatic switchover to verified fallback.

the whole system or its components. System activities are continuously monitored and compared against the baseline normal behavior model. When instantaneous behavior deviates beyond a predefined normality threshold, it is flagged as anomalous, which may indicate a potential intrusion.

In the context of AVs, anomaly-based intrusion detection depends on accurately characterizing the vehicle's normal operational behavior, which is typically learned through offline modeling and training. If an attacker attacks vehicle components (for example, by injecting malicious data into sensors) that cause the vehicle to behave abnormally, the IDS identifies this deviation and raises an alert. A key strength of anomaly-based IDS is its capability to identify previously unseen attacks better than other detection algorithms; however, developing an accurate normal behavior model is challenging. Inaccuracies in this model can lead to high false-positive or false-negative errors.

To address this, we develop the normal behavior model of AVs using a combination of a mathematical model of the vehicle system, called the autonomous vehicle behavior model (AVBM), and machine learning algorithms. The mathematical model characterizes the instantaneous state of the vehicle, while the learning-based components account for the data-driven variations in normal operation. A simplified overview of the AVBM is illustrated in **Figure 4**, and further details are available in Refs. [31, 32].

5.2.1.1 Anomaly-based intrusion detection methodology

Figure 5 shows a diagram of anomaly-based intrusion detection technique for AVs. We define the anomaly detection approach over a finite set of driving events U. Set U is divided into two subsets: *Normal* driving events N and *Abnormal* driving events A, such that: $N \cup A = U$ and $N \cap A = \varnothing$. A representation map R is used to model U, which maps driving events in U to patterns in U^R. Similarly, N and A driving sets are mapped to N^R and A^R using the representation map R. These can be mathematically expressed as: $U \xrightarrow{R} U^R, N \xrightarrow{R} N^R, A \xrightarrow{R} A^R$, and $N^R \cup A^R = U^R$. A detector D is defined as $D = (f, M)$; where f denotes the normal behavior characterization function expressed as $f: U^R \times M \Rightarrow [0,1]$, and M is denoted as the system memory that stores the normal behavior model extracted from the set of normal driving events N^R. Function f specifies the degree of abnormality of a sample $s \in U^R$ by comparing it with M. The higher the value of $f(s,M)$, the more abnormal the sample is. If the value of $f(s,M)$ exceeds a predefined threshold $\mathbb{T}$, detector D raises an alarm that indicates the occurrence of an abnormal event. Detector D can be mathematically expressed as follows:

$$D(s) = \begin{cases} Abnormal & if \quad f(s,M) > \mathbb{T} \\ Normal & otherwise \end{cases}$$

5.2.2 Hash-based integrity validation

Hash-based integrity validation is used in this work as a lightweight, runtime safeguard for the QCar perception stack [33, 34]. Specifically, the electronic control unit (ECU) periodically computes a cryptographic hash (SHA-256) over a predefined set of integrity-critical artifacts, including the deployed YOLOv8 model weights and associated configuration files (e.g., detection thresholds and

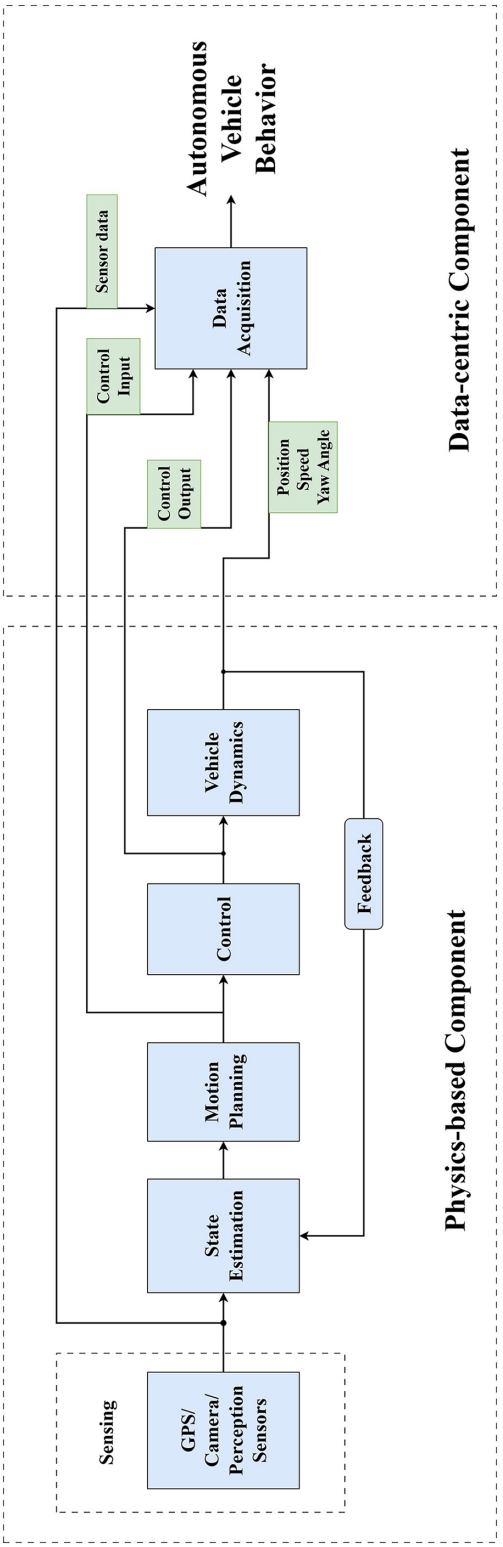


Figure 4.
Simplified AVBM.

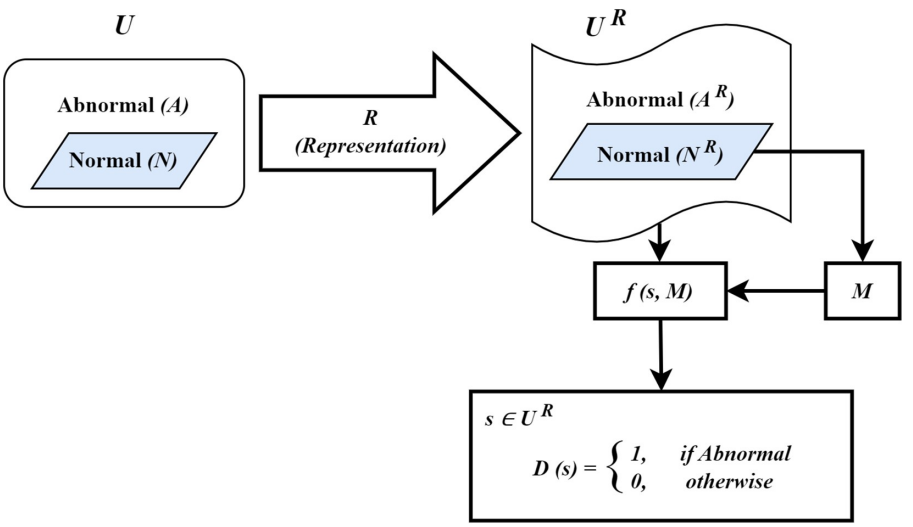


Figure 5.
Anomaly-based intrusion detection methodology.

class-to-label mappings). The computed digest is compared against a trusted baseline hash stored in a protected location.

A hash mismatch is treated as a software-tampering event. Upon detection, the system logs the anomaly (timestamped) and immediately triggers the resilience response: execution is switched to a pre-verified fallback/backup perception module, and trusted files are restored, allowing the vehicle to maintain safety-critical behaviors without requiring a system restart. The fallback remains active in an event-driven manner as long as the integrity violation persists, and normal operation is automatically restored once the expected hash values are re-established.

6. Experimental setup and results

Experiments were conducted using Quanser's QCar self-driving platform, a small-scale, high-fidelity testbed for perception, planning, and control research [35]. The vehicle is equipped with a drive motor, steering servo, four cameras, a 2D LiDAR, an Intel RealSense depth camera, and a 9-axis IMU. An onboard NVIDIA Jetson Orin processor executes control algorithms, receives commands via Wi–Fi from a ground station, and transmits sensor data back for monitoring.

As mentioned in previous sections, our experiments focus on attacks targeting the perception and knowledge processing layers. Perception-layer attacks include sensor-level manipulations, such as laser blinding of the depth camera, which degrades obstacle detection and braking. Knowledge-layer attacks involve software manipulations, including modifications to the YOLOv8 model and configuration files, aiming to compromise data fusion and world-model integrity. These experiments evaluate the effectiveness of resilience mechanisms, including anomaly detection, hash-based integrity validation, and backup/fallback strategies.

Two experimental setups were employed, each corresponding to a distinct threat detection technique, with backup and fallback mechanisms for resilience.

6.1 Anomaly-based intrusion detection setup

6.1.1 Attack experiment

In this experimental setup, we performed a real-world depth camera blinding attack against the onboard depth camera of QCar to degrade obstacle detection and braking capabilities during autonomous driving. A laser blinding attack was performed as explained by Yan et al. [18]. The hardware setup of the attack device consisted of a wide-beam laser controlled by an Arduino, which recorded digital clock timestamps corresponding to the laser's on and off states. The device generated a binary signal, where a value of 1 denoted laser activation and 0 denoted deactivation. Both the QCar and the attack device operated at the same data sampling rate and were initialized simultaneously to ensure temporal alignment. **Figure 6** illustrates the setup used for the anomaly-based intrusion detection experiments.

6.1.2 Data collection: Autonomous vehicle perception (Avp-dataset)

AVBM in **Figure 4** highlights the essential parameters necessary for estimating the present and future states of the vehicle. This helps to model the normal behavior of the vehicle and guides us in collecting data on specific features for our experimental analysis. The autonomous vehicle perception dataset (AVP-dataset) is prepared by incorporating the parameters obtained from the AVBM. The full AVP-Dataset is publicly available at [31, 36].

6.2 Hash-based integrity validation setup

6.2.1 Attack experiment

In this experimental setup, we conducted a *software-based perception tampering attack* on the QCar's onboard NVIDIA Jetson AGX Orin main ECU to evaluate the effectiveness of hash-based integrity validation. The attack scenario is illustrated in **Figure 7**.

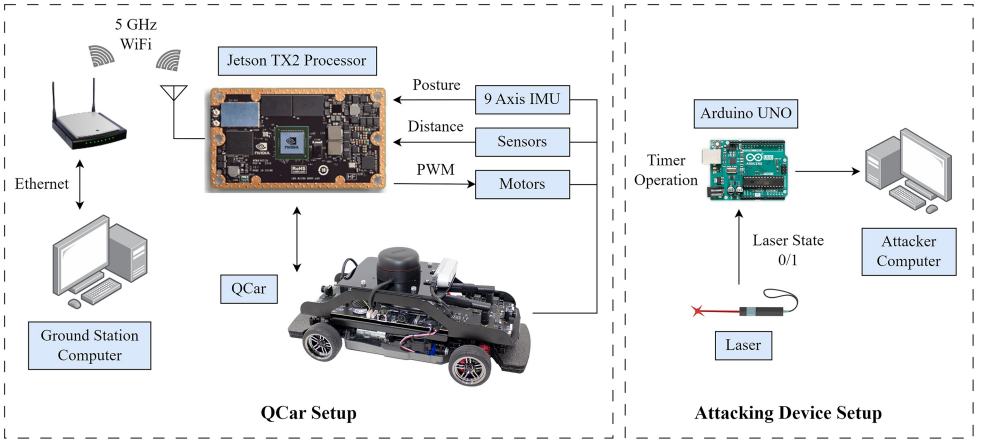


Figure 6.
Setup of the depth camera blinding attack experiment on QCar.

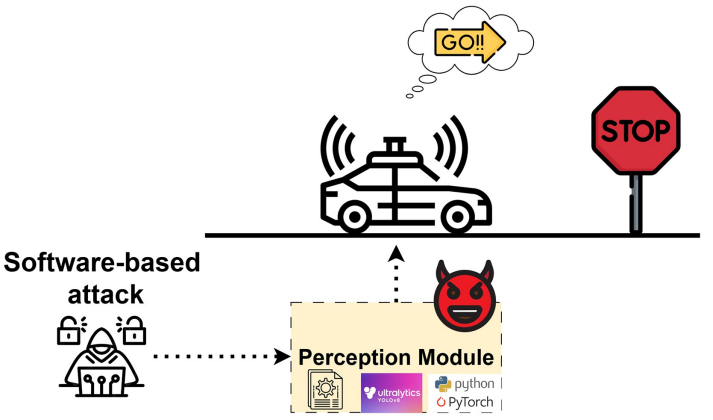


Figure 7.
Software-based attack: ECU perception module compromise on QCar2.

The attack degrades obstacle detection and braking behavior by modifying internal perception parameters at runtime, such as YOLOv8 model configuration files, object detection thresholds, or class-to-label mappings. Unlike physical-layer attacks, this approach does not interfere with sensors directly and instead represents realistic advanced driver-assistance systems (ADAS) and AV threats originating from within the ECU.

To assess robustness and repeatability, five independent software tampering events were triggered under each experimental condition, with each event treated as an individual attack trigger and distributed across multiple autonomous driving runs. No explicit upper limit was imposed on the number of triggers, allowing the system to handle repeated tampering events without requiring a restart or manual intervention.

When an integrity violation is detected, the system does not issue an emergency stop. Instead, it automatically switches to a pre-verified fallback perception module, enabling the vehicle to continue operating while preserving safety-critical functions. The fallback mechanism remains active as long as the abnormal configuration persists and is released once the trusted state is restored. As a result, the vehicle does not unconditionally stop after an attack but continues to drive safely and execute appropriate behaviors, such as stopping for pedestrians or stop signs, based on the fallback perception output.

6.2.2 Data collection: Integrity-validation dataset

Data was collected under normal operation and during software attacks. In the normal scenario, the YOLOv8 model and configuration files remained unaltered, with hashes matching the trusted baseline values. During attacks, modified models or configuration files generated hash mismatches, which were logged by the system. The integrity-validation dataset contains synchronized traces of both normal and attack scenarios, capturing system responses, detection outcomes, and integrity validation results.

6.3 Experimental results

6.3.1 Results: Anomaly-based detection

This experiment evaluates the performance of seven supervised binary classification models, namely random forest (RF), logistic regression (LR), XGBoost (XGB), K-nearest neighbor (KNN), support vector classifier (SVC), multi-layer perceptron (MLP), and naive bayes (NB), using the AVP-Dataset. The evaluation was conducted on the full dataset comprising 88,976 samples, including 45,001 normal instances (50.57%) and 43,975 abnormal instances (49.43%). Classifier performance was assessed using four standard metrics: accuracy, precision, recall, and F1 score. Since the primary objective is to identify abnormal samples, all metrics were computed by treating the abnormal class as the positive class. To ensure unbiased evaluation, a stratified five-fold cross-validation scheme was employed to preserve class balance across folds. In each fold, 80% of the data was used for training, and the remaining 20% was used for testing.

The comparative performance of the evaluated models is summarized in **Table 2**. The results indicate that **RF** achieved the highest accuracy, precision, recall, and F1 score among all classifiers. LR, KNN, and MLP demonstrated competitive performance with comparable F1 scores, following closely behind RF.

6.3.2 Tuning the detection threshold T for anomaly-based detection

In this experiment, we investigated the selection of an appropriate predefined threshold $\mathbb{T}$ for the anomaly behavior analysis framework by examining the predicted probability scores associated with normal and abnormal samples. Since the **RF** model exhibited the strongest overall performance in experiment 2 therefore, it was selected for this experiment. The probability outputs were visualized to identify a suitable separation margin for threshold placement. **Figure 8** illustrates the overlaid probability score distributions for normal and abnormal data, where a clear distinction between the two classes can be observed, as highlighted by the dotted boundaries.

Table 3 reports the corresponding misclassification rates as we widen the decision margin. The results indicate that choosing the threshold $\mathbb{T}$ within the interval of **0.4 to 0.5** provides the most favorable trade-off. In this range, 155 normal samples are incorrectly labeled as abnormal, while no attack samples are misclassified, resulting a false positive rate of 0.0398 (3.98%) and a false negative rate of 0. Thus, setting the predefined threshold $\mathbb{T}$ to a value between 0.4 and 0.5 for the anomaly behavior analysis approach ensures an optimal attack detection capability.

Metrics	RF	LR	XGB	KNN	SVC	MLP	NB
Precision	**0.801**	0.800	0.751	0.793	0.742	0.786	0.692
Recall	**0.894**	0.872	0.876	0.877	0.913	0.874	0.923
F1 Score	**0.845**	0.834	0.809	0.833	0.819	0.828	0.791
Accuracy	**0.838**	0.829	0.795	0.826	0.800	0.820	0.759

Table 2.
Depth camera blinding attack detection performance of different ML models.

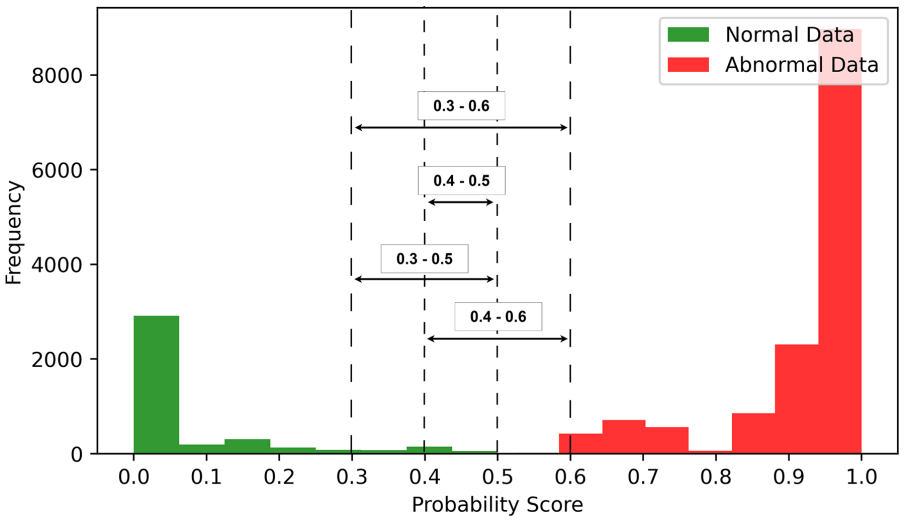


Figure 8.
Distribution of RF abnormal-class probability scores for normal and attack data. The evaluation fold consists of 3,893 normal samples and 13,902 attack samples. An effective detection threshold lies in the range $\mathbb{T} = 0.4–0.5$.

Detection Margin	Normal Data Misclassified	Attack data Misclassified	FP Rate	FN Rate
0.4–0.5	**155**	**0**	**0.0398**	**0**
0.3–0.5	293	0	0.0752	0
0.4–0.6	155	26	0.0398	0.00187
0.3–0.6	293	26	0.0752	0.00187

Table 3.
False positive (FP) and false negative (FN) rates for different detection margins.

6.3.3 Results: Hash-based integrity validation

6.3.3.1 Detection accuracy and timing

We evaluated the hash-based detection mechanism on QCar under varying speeds from **0.5 m/s** to **1.75 m/s,** with update intervals of **1 s**, **3 s**, and **5 s**. Across all configurations, the system achieved a **100% success rate**, demonstrating that hash-based validation reliably detects any modification to the model or configuration, regardless of vehicle speed or update frequency (**Figure 9**).

6.3.3.2 Scalability discussion

In a full-scale vehicle with dozens of concurrent software modules, continuous hashing of all artifacts at high frequency may be impractical. In practice, integrity validation can be scoped to safety-critical artifacts only and executed using staggered schedules or event-driven triggers (e.g., upon update, process restart, or policy-defined checkpoints), which reduces CPU and I/O contention while preserving tamper detection capability.

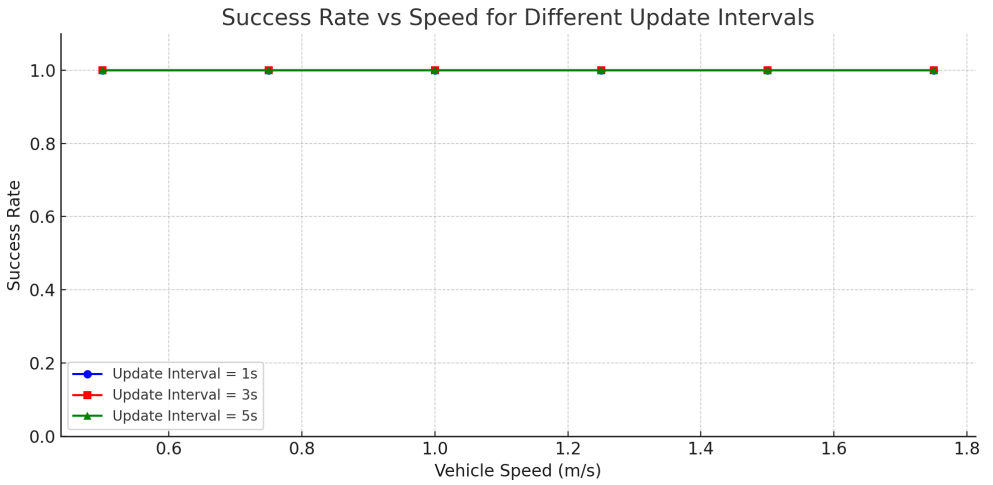


Figure 9.
Success rate of hash-based integrity validation across vehicle speeds (0.5–1.75 m/s) and hash update intervals (1 s, 3 s, and 5 s), showing reliable detection of all software modifications.

6.3.3.3 Resilience results

6.3.3.3.1 System resilience evaluation

Beyond detection, we measured the system's response to attacks, focusing on how backup and fallback mechanisms maintain safe operation. Using hash-based monitoring, the system detected a malicious update within **0.030 s** after its onset at **25.00 s**. The built-in backup mechanisms immediately restored the trusted configuration and model in **0.002 s** (**Figure 10**), preventing any unsafe behavior.

These results emphasize the importance of having robust fallback strategies: in "normal" scenarios where no attack occurs, the backup remains idle but ready, ensuring normal operation is unaffected; in "attack (abnormal)" scenarios with tampering, the fallback enables the system to revert to a safe, trusted state before any compromised module can influence vehicle behavior. This demonstrates that the combination of fast detection and reliable backup is critical for maintaining both safety and operational continuity in autonomous vehicles.

6.3.3.4 Physical validation and behavior analysis

We further validated the proposed resilience mechanisms on the QCar testbed. During normal operation, the vehicle speed stabilized near **0.33 m/s**, corresponding

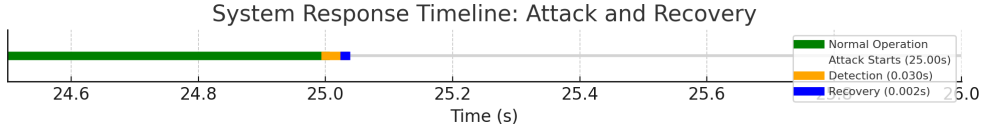


Figure 10.
System response timeline under software tampering. The attack is detected via hash mismatch within 0.030 s after onset, and the trusted configuration is restored within 0.002 s, preventing unsafe vehicle behavior.

DOI: http://dx.doi.org/10.5772/intechopen.1015209

to a low-speed operation on the scaled platform and being qualitatively comparable to approximately **12 km/h** driving in a full-scale vehicle. At **10 s**, a software-tampering attack was introduced; despite this, the vehicle correctly halted at a **STOP** sign at **20 s**, illustrating that the backup and recovery mechanisms successfully maintained functional safety (**Figure 11**).

This physical experiment demonstrates the practical value of the resilience layer: it not only detects attacks but also ensures that the safety-critical behaviors are preserved, preventing unsafe outcomes even under real-world attack conditions.

7. Conclusion

As AVs become integral to the future of transportation systems, it becomes critically important to enhance the security and resilience of AVs. This chapter has addressed the multifaceted vulnerabilities that AVs face, stemming from their dependency on complex sensor systems, wireless networks, and decision-making processes. By categorizing potential threats across various architectural layers, we have highlighted several ways in which these vehicles can be compromised, as well as how these threats can be detected and mitigated.

The introduction of an AV resilient architecture, characterized by redundancy, diversity, and adaptive reconfiguration, offers a robust framework to tolerate AV attacks. The integration of innovative intrusion detection techniques, such as

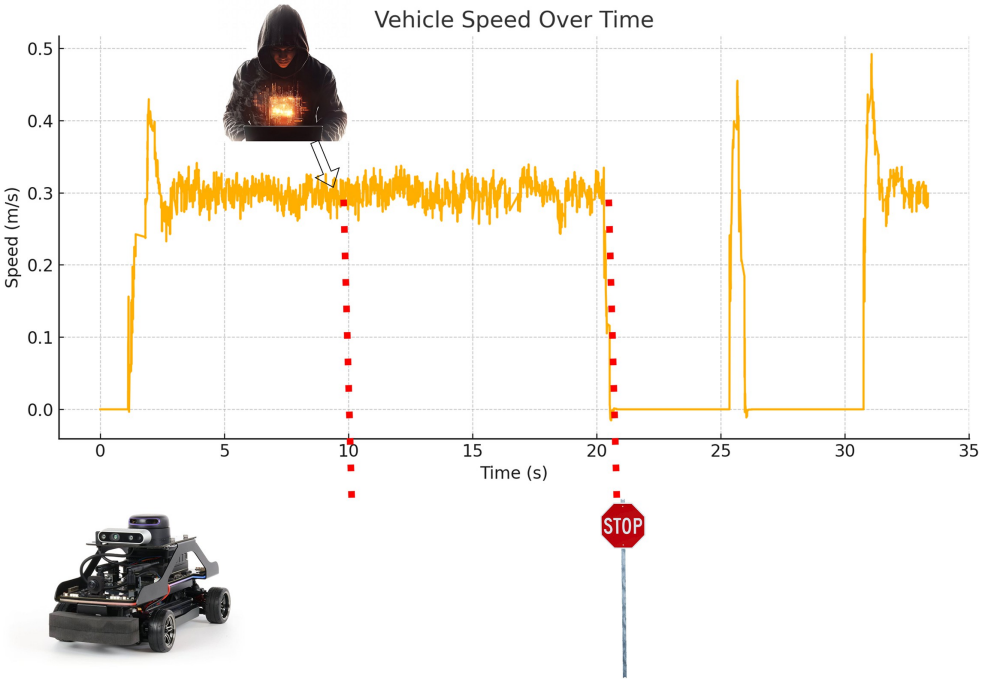


Figure 11.
QCar speed profile during ECU tampering. After the attack is injected at 10 s, the vehicle continues operating under the fallback perception module and correctly stops at a STOP sign at 20 s, demonstrating preserved safety behavior without an emergency halt.

anomaly detection and hash-based verification, further enhances the security and protection of AV operations. The successful experimental validation conducted on the Quanser QCar platform exemplifies the practical effectiveness of these strategies in real-world scenarios, particularly in thwarting depth camera blinding attacks and software tampering.

Ultimately, this work establishes a critical link between threat modeling and the implementation of practical defense mechanisms, paving the way for more resilient AV systems. As we advance toward a future where AVs play an essential role in our transportation landscape, it is imperative that we continue to refine and evolve these security and resilience measures. By prioritizing resilience, we not only enhance the safety and trustworthiness of AVs but also contribute to the broader goal of creating intelligent transportation systems that can adapt to ever-evolving challenges in our complex digital world.

Acknowledgments

This work was supported in part by the National Science Foundation (NSF) projects under Grant 1624668, Grant 1921485, Grant 1303362 (Scholarship-for-Service), Grant 2413009, and the WISPER Center. It was also supported by the 2025 Technology and Research Initiative Fund/National Security Systems Initiative, administered by the University of Arizona, Office of Research and Partnerships, funded under Proposition 301, the Arizona Sales Tax for Education Act, in 2000. Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of the NSF.

Conflict of Interest

The author declares no conflict of interest.

Security and Resilience in Autonomous Vehicles: A Proactive Design Approach
DOI: http://dx.doi.org/10.5772/intechopen.1015209

Author details

Chieh Tsai[1], Murad Mehrab Abrar[2] and Salim Hariri[1*]

1 Department of Electrical and Computer Engineering, University of Arizona, Tucson, USA

2 Department of Mechanical Engineering, University of Washington, Seattle, USA

*Address all correspondence to: hariri@arizona.edu

IntechOpen

© 2026 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] Litman T. Autonomous vehicle implementation predictions. 2017

[2] Shladover SE. Connected and automated vehicle systems: Introduction and overview. Journal of Intelligent Transportation Systems. 2018;**22**(3):190–200

[3] Petit J, Shladover SE. Potential cyberattacks on automated vehicles. IEEE Transactions on Intelligent Transportation Systems. 2014;**16**(2):546–556

[4] Checkoway S, McCoy D, Kantor B, Anderson D, Shacham H, Savage S, Koscher K, Czeskis A, Roesner F, Kohno T. Comprehensive experimental analyses of automotive attack surfaces. In: 20th USENIX security symposium (USENIX Security 11); 2011

[5] Cao Y, Xiao C, Cyr B, Zhou Y, Park W, Rampazzi S, Chen QA, Kevin F, Morley Mao Z. Adversarial sensor attack on lidar-based perception in autonomous driving. In: Proceedings of the 2019 ACM SIGSAC conference on computer and communications security, 2019; p. 2267–2281

[6] Shepard DP, Bhatti JA, Humphreys TE. Drone Hack: Spoofing attack demonstration on a civilian unmanned aerial vehicle. GPS World. 2012;**23**(8):30–33

[7] Sterbenz JPG, Hutchison D, Çetinkaya EK, Jabbar A, Rohrer JP, Schöller M, Smith P. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Computer Networks. 2010;**54**(8):1245–1265

[8] Ganin AA, Mersky AC, Jin AS, Kitsak M, Keisler JM, Linkov I. Resilience in intelligent transportation systems (its). Transportation Research Part C: Emerging Technologies. 2019;**100**:318–329

[9] Pendleton SD, Andersen H, Xinxin D, Shen X, Meghjani M, Eng YH, Rus D, Ang MH. Perception, planning, control, and coordination for autonomous vehicles. Machines. 2017;**5**(1):6

[10] Ulbrich S, Reschka A, Rieken J, Ernst S, Bagschik G, Dierkes F, Nolte M, Maurer M. Towards a functional system architecture for automated vehicles. arXiv preprint arXiv:1703.08557. 2017

[11] Huang K, Shi B, Xiang L, Xin L, Huang S, Yikang L. Multi-modal sensor fusion for auto driving perception: A survey. arXiv preprint arXiv:2202.02703. 2022

[12] Wang Z, Wu Y, Niu Q. Multi-sensor fusion in automated driving: A survey. Ieee Access. 2019;**8**:2847–2868

[13] Petit J, Stottelaar B, Feiri M, Kargl F. Remote attacks on automated vehicles sensors: Experiments on camera and lidar. Black Hat Europe. 2015;**11**(2015):995

[14] Yuan X, Han X, Deng G, Jiwei L, Liu Y, Zhang T. Sok: Rethinking sensor spoofing attacks against robotic vehicles from a systematic view. In: 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P). IEEE, 2023; p. 1082–1100

[15] Ivanov R, M Pajic, and I Lee. Attack-resilient sensor fusion for

safety-critical cyber-physical systems. ACM Transactions on Embedded Computing Systems (TECS). 2016;**15** (1):1–24

[16] Shin H, et al. Illusion and dazzle: Adversarial optical channel exploits against lidar-based perception in autonomous vehicles. In: IEEE Symposium on Security and PrivacyWorkshops; 2017

[17] Wenyuan X, Yan C, Jia W, Xiaoyu J, Liu J. Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles. IEEE Internet of Things Journal. 2018;**5** (6):5015–5029

[18] Yan C, Wenyuan X, Liu J. Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. Def Con. 2016;**24** (8):109

[19] Liu J, Park J-M. "seeing is not always believing": Detecting perception error attacks against autonomous vehicles. IEEE Transactions on Dependable and Secure Computing. 2021;**18**(5):2209–2223

[20] Milaat FA, Liu H. Decentralized detection of gps spoofing in vehicular ad hoc networks. IEEE Communications Letters. 2018;**22**(6):1256–1259

[21] Oligeri G, Sciancalepore S, Ibrahim OA, Di Pietro R. Gps spoofing detection via crowd-sourced information for connected vehicles. Computer Networks. 2022;**216**:109230

[22] Qi CR, Liu W, Chenxia W, Hao S, Guibas LJ. Frustum pointnets for 3d object detection from rgb-d data. In: Proceedings of the IEEE conference on computer vision and pattern recognition, 2018; p. 918–927

[23] Chen X, Huimin M, Wan J, Li B, Xia T. Multi-view 3d object detection network for autonomous driving. In: Proceedings of the IEEE conference on Computer Vision and Pattern Recognition, 2017; p. 1907–1915

[24] Jason K, Mozifian M, Lee J, Harakeh A, Waslander SL. Joint 3d proposal generation and object detection from view aggregation. In: 2018 IEEE/RSJ international conference on intelligent robots and systems (IROS). IEEE, 2018; p. 1–8

[25] James T, Huichen L, Yan X, Ren M, Chen Y, Liang M, Bitar E, Yumer E, Urtasun R. Exploring adversarial robustness of multi-sensor perception systems in self driving. arXiv preprint arXiv:2101.06784. 2021

[26] Goodfellow IJ, Shlens J, Szegedy C. Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572. 2014

[27] Zhang Q, Shengtuo H, Sun J, Chen QA, Mao Z. On adversarial robustness of trajectory prediction for autonomous vehicles. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2022; p. 15159–15168

[28] Zheng H, Zhang Z, Juncheng G, Lee H, Prakash A. Efficient adversarial training with transferable adversarial examples. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2020; p. 1181–1190

[29] Yousseef A, Satam S, Latibari BS, Pacheco J, Salehi S, Hariri S, Satam P. Autonomous vehicle security: A deep dive into threat modeling. arXiv preprint arXiv:2412.15348. 2024

[30] Satam P, Satam S, Hariri S, Alshawi A. Anomaly behavior analysis of IoT protocols. In: Kamhoua CA, Njilla LL, Kott A, Shetty S, editors. Modeling and Design of Secure Internet of Things. Hoboken, NJ: John Wiley & Sons; 2020. p. 295–330

[31] Abrar MM, Hariri S. An anomaly behavior analysis framework for securing autonomous vehicle perception. In: 2023 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA). IEEE, 2023; p. 1–6

[32] Abrar MM, Youssef A, Islam R, Satam S, Latibari BS, Hariri S, Shao S, Salehi S, Satam P. Gps-ids: An anomaly-based gps spoofing attack detection framework for autonomous vehicles. arXiv preprint arXiv:2405.08359. 2024

[33] Uriawan W, Ramadita R, Putra RD, Siregar RI, Addiva R. Authenticate and verification source files using sha256 and hmac algorithms. 2024

[34] Tsai C, Salim H. Intelligent obstacle resilience in autonomous vehicles under security threats. 2025. p. 34–41,11

[35] QCar2 Developers. Qcar2: Autonomous vehicle simulation platform. Available from: https://www.qcar2.com [Accessed: 2025-August-18]

[36] AVP-Dataset: Autonomous Vehicle Perception Dataset. 2023. GitHub repository; Available from: https://github.com/mehrab-abrar/AVP-Dataset/ [Accessed: 2025-August-19]

Chapter 6

Security and Privacy Threats in Connected Vehicle Environment

Ayan Roy

Abstract

Connected vehicle (CV) technologies and vehicle-to-everything (V2X) communications are reshaping transportation by enabling vehicles to exchange data with other vehicles, roadside infrastructure, pedestrians, and cloud services. These systems rely on protocols such as dedicated short-range communications (DSRC) and cellular-V2X (C–V2X) to support safety-critical applications like collision avoidance and traffic flow optimization. However, the reliance on continuous connectivity introduces significant security and privacy concerns, including eavesdropping, spoofing, denial of service, and large-scale traffic manipulation. This chapter provides a comprehensive overview of security and privacy threats in CV environments. We first introduce the fundamental concepts of CVs and their communication protocols. We then analyze threat actors, attack surfaces, and attack models with real-world examples. Existing solutions, including cryptographic authentication, intrusion detection systems, and blockchain-based trust management, are surveyed. Finally, we highlight open-ended research challenges such as scalability, postquantum resilience, and privacy-preserving data sharing.

Keywords: connected vehicles, V2X, DSRC, C–V2x, security, privacy, attack models, threat actors

1. Introduction

Connected vehicle (CV) technologies are revolutionizing modern transportation by transforming isolated vehicles into intelligent, interconnected nodes within a broader mobility ecosystem. Through vehicle-to-everything (V2X) communication, vehicles continuously exchange real-time data with other vehicles, roadside infrastructure, pedestrians, and cloud services. This pervasive connectivity enables the sharing of critical parameters such as speed, location, and road conditions, thereby supporting applications ranging from collision avoidance and cooperative lane-changing to traffic management and emergency response [1]. V2X communication is the cornerstone of emerging intelligent transportation systems (ITS), which aim to enhance roadway safety, improve traffic efficiency, and deliver a more seamless driving experience for both human-operated and autonomous vehicles. A general architecture for the V2X communication model has been proposed by the authors in [2] and is depicted in **Figure 1**.

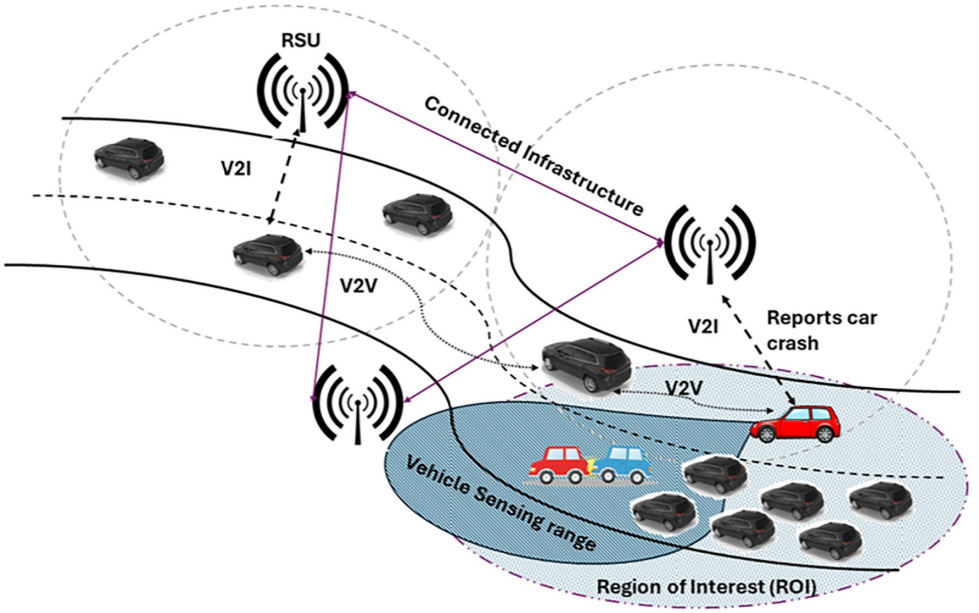


Figure 1.
Illustration of a connected vehicle ecosystem showing V2X communication links.

The communication backbone of CVs relies on standardized wireless protocols that ensure reliability, low latency, and interoperability. Dedicated short-range communication (DSRC), based on the IEEE 802.11p standard, was the earliest technology to support safety-critical vehicular messaging, such as the transmission of Basic Safety Messages (BSMs) between nearby vehicles [3]. More recently, cellular-V2X (C–V2X) – developed by the third generation partnership project (3GPP) – has emerged as a complementary solution that leverages long-term evolution (LTE) and 5 G networks to provide greater coverage, higher data rates, and more resilient connectivity. To promote regional interoperability, additional frameworks such as IEEE 1609.x (for security services and WAVE architecture), SAE J2735 (for message definitions), and ETSI ITS-G5 (for European cooperative ITS deployments) have been standardized [4]. The adoption of these technologies has produced clear societal benefits. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) links enable early hazard detection and cooperative awareness, reducing the likelihood of collisions. Vehicle-to-network (V2N) connectivity extends these capabilities by linking vehicles to mobile networks and cloud platforms, enabling dynamic route planning, real-time traffic analytics, and seamless infotainment experiences [5]. Through V2N, CVs can also participate in crowdsourced data ecosystems – for example, applications such as Waze aggregate vehicular reports on congestion or incidents and relay this information to third-party services for optimized routing and congestion control. In this sense, V2N acts as a large-scale, mobile sensor network that transforms vehicles into participants of an intelligent, data-driven transportation grid. However, the increased connectivity also introduces significant security and privacy vulnerabilities. Unlike traditional automobiles that relied mainly on mechanical components, CVs are cyber-physical systems integrating wireless communication interfaces, embedded software, and cloud infrastructures [6]. Features such as over-the-air (OTA)

software updates, remote diagnostics, and cloud-based data synchronization expand the attack surface, creating opportunities for remote code injection, firmware manipulation, and ransomware attacks. The broadcast nature of V2X communication further exposes data to threats including eavesdropping, spoofing, replay attacks, and denial-of-service (DoS) disruptions [7]. Beyond technical exploits, privacy concerns are equally critical: continuous transmission of unique identifiers and geolocation data enables long-term vehicle tracking, behavioral profiling, and potential misuse by malicious entities [8]. Conceptually, a V2X network can be likened to a social network among vehicles, where participants share information for collective benefit. Unfortunately, this cooperative structure can also be weaponized. An adversarial vehicle may behave as a "malicious influencer," disseminating falsified or misleading information that distorts traffic perception and undermines trust in cooperative systems. Such misinformation can cascade across applications that rely on shared V2X data, degrading the accuracy of traffic flow prediction and route-optimization algorithms. A vivid real-world example is the demonstration of a fake traffic jam created using 99 smartphones carried in a handcart, which deceived Google Maps into reporting congestion on an empty street. This incident highlights how even simple data-level manipulation can disrupt intelligent mobility platforms and underscores the urgency for robust validation, authentication, and privacy-preserving mechanisms within V2X ecosystems.

These challenges underscore the urgent need for comprehensive security and privacy frameworks capable of detecting, preventing, and mitigating the wide spectrum of cyber-physical threats facing CVs. As the boundaries between the physical and digital layers of transportation continue to blur, safeguarding vehicular networks demands not only technical defenses but also resilient architectures that ensure trust, integrity, and accountability across all communication channels. To this end, this chapter is structured to provide a holistic exploration of the CV threat landscape and its countermeasures. Section 2 analyzes the key threat actors and attack models, supported by real-world case studies that illustrate how vulnerabilities manifest in practice. Section 3 surveys a range of security and privacy countermeasures, including cryptographic protocols, intrusion detection systems (IDS), trusted hardware components, blockchain-based frameworks, and artificial intelligence (AI) – driven techniques. Section 4 highlights open research challenges that remain unresolved – particularly those concerning scalability, postquantum resilience, and privacy preservation. Finally, Section 5 concludes the chapter with overarching insights and a forward-looking discussion on the development of secure, trustworthy, and human-centric CV ecosystems.

2. Threat actors and attack models

2.1 Threat actors

CV environments involve a wide array of stakeholders – automotive manufacturers, software vendors, communication providers, and end users – which also creates multiple entry points for adversaries. The diversity of participants means that attackers differ in motivation, resources, sophistication, and persistence. Understanding these threat actors is crucial for designing effective defense mechanisms. They can broadly be categorized as follows:

- Malicious individuals (hackers or pranksters): these are typically independent actors or small groups who exploit vulnerabilities out of curiosity, challenge, or personal recognition. Their motivation often stems from the desire to demonstrate technical skill or expose weaknesses in connected systems rather than direct financial gain. However, such exploits can still have severe consequences in safety-critical environments. A well-known example includes the remote exploitation of a Jeep Cherokee in 2015, where security researchers gained wireless control of the steering and braking systems through a vulnerability in the vehicle's infotainment module [9]. While conducted for research purposes, this incident illustrated the ease with which a motivated individual or small group could manipulate a vehicle's behavior remotely, potentially leading to traffic accidents or widespread panic if replicated by malicious actors.

- Organized crime groups: unlike opportunistic hackers, organized crime groups are driven primarily by financial incentives. They possess greater resources, coordination, and access to underground marketplaces for purchasing exploits, stolen data, or hardware tools. These groups may target CVs to perform ransomware attacks, vehicle theft through relay and key-fob cloning, or data exfiltration from onboard systems. With the increasing digitization of vehicles, criminals can also intercept payment data from in-vehicle apps, disable telematics for extortion, or sell stolen information on dark-web platforms. For example, several ransomware variants, such as TeslaCrypt and CarLocker, have been conceptually demonstrated to lock users out of vehicles or infotainment systems, demanding cryptocurrency payments for restoration. Such organized attacks reflect a growing underground economy surrounding vehicular cybercrime.

- Nation-state adversaries: nation-state or advanced persistent threat (APT) actors represent the most capable and well-funded category of attackers. Their objectives extend beyond individual profit toward espionage, disruption, or strategic advantage. These adversaries may seek to compromise large-scale transportation infrastructure, such as traffic management centers, connected highway systems, or cloud-based fleet controllers, to cause economic damage or social disruption. For example, simulated studies have shown that coordinated DoS or false data injection attacks against traffic-signal networks could paralyze entire urban regions, leading to secondary impacts on emergency response and logistics. In geopolitical contexts, such actors could weaponize vehicular connectivity to disable supply chains, perform targeted surveillance, or trigger cascading failures across smart-city infrastructures.

- Insiders: insider threats stem from individuals with legitimate access to sensitive systems – employees of manufacturers, service providers, or cloud operators – who may intentionally or unintentionally compromise security. Insiders often possess deep system knowledge and privileged credentials, making their actions particularly difficult to detect. Motivations range from financial gain and revenge to negligence or coercion. For instance, an insider could leak proprietary vehicle firmware, disable encryption modules in OTA update servers, or introduce backdoors during software development. Insider threats also encompass third-party contractors and suppliers, whose security practices may not

align with those of the original equipment manufacturer (OEM). A notable example is the discovery of diagnostic backdoors unintentionally left open in several aftermarket telematics units, exposing thousands of vehicles to remote exploitation [10].

Together, these threat actors represent the multifaceted adversarial landscape of CV environments. Their varying goals – from curiosity-driven exploration to state-sponsored sabotage – demand a layered defense strategy that integrates technical safeguards, organizational policies, and continuous threat intelligence sharing across the automotive ecosystem.

2.2 Attack surfaces

The attack surface of a CV spans multiple layers of the ecosystem:

- Wireless interfaces: DSRC, C–V2X, Wi–Fi, Bluetooth, and satellite links.
- In-vehicle networks: controller area network (CAN), FlexRay, and infotainment systems.
- Back-end infrastructure: telematics servers, cloud platforms, and OTA update services.

These diverse entry points make V2X systems vulnerable to both local and remote adversaries.

2.3 Attack models

Several categories of cyberattacks have been extensively studied in the context of CVs, some of which have already been demonstrated in real-world or simulated environments. These attacks exploit different components of the V2X ecosystem, ranging from wireless communication channels to onboard systems and backend infrastructures.

- Eavesdropping and traffic analysis: this attack involves the unauthorized interception of wireless V2X communications, allowing an adversary to monitor message exchanges between vehicles or between a vehicle and roadside units (RSUs). Even when data payloads are encrypted, attackers can analyze communication patterns – such as message timing, frequency, or signal strength – to infer sensitive information like driving routes, behavioral patterns, or vehicle identities [8]. Over time, traffic analysis enables long-term tracking and profiling of drivers, leading to serious privacy violations. In dense urban areas, eavesdroppers can use inexpensive radio receivers to capture unencrypted beacon messages and reconstruct entire traffic flows.
- Message injection and replay attacks: in this scenario, an attacker injects fabricated or previously captured BSMs into the network. These falsified messages can mislead other vehicles into making incorrect decisions – such as unnecessary

braking or lane changes – by simulating nonexistent hazards [11]. Replay attacks amplify this risk by retransmitting old but valid messages, creating temporal confusion in vehicle control logic. Since BSMs are often broadcast without strong temporal validation, attackers can easily exploit timing mismatches. A single malicious node can, therefore, disrupt cooperative awareness systems over a wide area.

- Sybil attacks: a Sybil attack occurs when a single adversary generates multiple pseudonymous identities to impersonate numerous vehicles within the network [12]. Thus, the attacker can distort traffic density information, fabricate congestion events, or manipulate local consensus algorithms used in platooning and routing. Such attacks can cause artificial traffic rerouting, reduce network efficiency, or even endanger safety-critical maneuvers. Detecting Sybil nodes is difficult because pseudonymity is an inherent feature of privacy-preserving V2X systems.

- DoS: A DoS attack aims to disrupt the availability of communication channels or computational resources essential for vehicular operations. This can be achieved through radio-frequency jamming, excessive message flooding, or resource exhaustion on vehicular processors [13]. When directed against DSRC or C-V2X frequencies, DoS attacks can completely disable safety-critical functions like cooperative collision warnings. Furthermore, distributed variants (DDoS) targeting backend servers or cloud services can cripple fleet management and navigation systems. The ephemeral and mobile nature of vehicular nodes makes detecting and mitigating DoS attacks particularly challenging.

- Man-in-the-middle (MITM) attacks: MITM attacks exploit weaknesses in authentication protocols, allowing adversaries to intercept, alter, or relay communications between two legitimate entities – such as a vehicle and a RSU [14]. Through packet manipulation, the attacker can inject false commands, downgrade encryption, or harvest credentials. For instance, an attacker could modify firmware updates in transit or redirect safety messages to different routes. Because V2X messages are frequently relayed through intermediate nodes, the potential for MITM attacks increases in multihop or mesh-based topologies without robust mutual authentication.

- Malware and ransomware: these attacks target the software integrity of in-vehicle systems, particularly infotainment modules, telematics units, and electronic control units (ECUs). Once compromised, malware can be used to monitor driver activity, manipulate control signals, or disable essential functions. Ransomware variants lock the vehicle's systems or display units and demand payment to restore functionality, effectively immobilizing the car. A landmark example is the Jeep Cherokee hack of 2015, where security researchers remotely accessed the vehicle's network via its infotainment system, demonstrating how wireless interfaces could serve as gateways into safety-critical subsystems [6]. With OTA updates now standard in modern vehicles, securing the update delivery chain is critical to preventing large-scale malware propagation.

Together, these attack models illustrate the multifaceted vulnerabilities within CV ecosystems. Their diversity – ranging from low-cost eavesdropping to complex coordinated assaults – necessitates multilayered defenses combining cryptographic authentication, network anomaly detection, and resilient system design. The following section examines how these attacks are mitigated through evolving security and privacy countermeasures. A summarized version of the threat model, attack surfaces, and the attack model can be obtained from **Table 1.**

3. Complexity of attacks by threat actors

The feasibility and complexity of attacks executed against vehicular systems depend primarily on the threat actor's **skill level, resources, and motivation,** as summarized in **Table 2**.

Attack surface	Attack model	Description
Wireless interfaces	Eavesdropping/traffic analysis	Intercepting V2X messages to track vehicles or infer user behavior.
Wireless interfaces	Message injection/ replay	Injecting false or outdated basic safety messages (BSMs) to mislead vehicles.
Wireless interfaces	Denial of service (DoS)/ jamming	Overloading or blocking DSRC or C-V2X channels disables safety applications.
In-vehicle networks	Malware/ransomware	Compromising ECUs or infotainment systems to lock functions or demand ransom.
In-vehicle networks	Man-in-the-middle (MITM)	Intercepting internal or external communications and altering transmitted data.
Cloud/back-end systems	Sybil attack	Generating multiple fake identities to disrupt decision-making or traffic flow.
Cloud/back-end systems	Data exfiltration (Insider)	Unauthorized access or leakage of sensitive driving data from backend servers.

Table 1.
Summary of threat models and attack surfaces in connected vehicle environments.

Category	Skill/ resources	Primary target	Example attack
Low-complexity	Low/basic	Physical access/key fobs	Keyless entry; relay attacks; GPS Jamming
Medium-complexity	Moderate	Software/basic protocols	CAN bus injection/replay attacks; basic sensor spoofing
High-complexity	High/well-funded	Critical systems/vulnerability chains	Zero-day remote exploits (e.g., telematics); adversarial AI attacks

Table 2.
Attack complexity versus threat actor capability.

3.1 Detailed attack profiles

3.1.1 Low-complexity attacks

These often exploit known, inherent weaknesses or require minimal specialized equipment. Examples include:

- **CAN bus injection and DoS:** leveraging the lack of intrinsic authentication in the CAN bus protocol, an attack often requires brief physical access (e.g., via the OBD-II port) to inject malicious control messages. Furthermore, due to the dominant low priority assigned to legitimate traffic in the CAN bus arbitration scheme, it is easy for an attacker to perform a DoS attack, thereby starving legitimate ECUs of sending essential messages [15].

- **Relay attacks:** simple electronic amplification of signals to steal vehicles with keyless entry systems. The feasibility of capturing signals for keyless entry and replaying them at a later time to gain access to a vehicle has been explored by researchers in [16].

3.1.2 High-complexity/sophisticated attacks

These require extensive resource investment, deep domain expertise, and often target previously undiscovered (zero-day) vulnerabilities.

- **Zero-day remote exploits:** discovering and chaining vulnerabilities in internet-connected components (e.g., telematics control units) to gain persistent remote control over safety-critical functions (steering, braking).

- **Adversarial AI attacks:** specifically targeting the machine learning (ML) models used by autonomous driving systems (e.g., manipulating camera or LiDAR data) to induce dangerous misclassifications.

- **Infrastructure compromise:** attacking backend servers or cloud services used for fleet management, cryptographic key distribution, or OTA updates, potentially compromising a large number of vehicles simultaneously.

4. Mitigation strategies and technological approaches

A wide variety of technical and architectural countermeasures have been proposed to enhance the security and privacy of CVs. These range from traditional cryptographic frameworks and authentication mechanisms to emerging paradigms such as blockchain, trusted hardware, and intelligent IDS. The following subsections summarize key approaches, their advantages, and limitations.

4.1 Cryptographic protocols for secure communication

Cryptography forms the foundation of secure V2X communication. The IEEE 1609.2 standard specifies message authentication, integrity, and confidentiality

mechanisms for vehicular environments [17]. Each vehicle is equipped with digital certificates issued by a trusted certificate authority (CA), allowing secure exchange of BSMs. To balance authentication with privacy, pseudonym-based schemes have been introduced [18]. Vehicles periodically change short-term certificates, making it difficult for external observers to link successive transmissions. The US Security Credential Management System (SCMS) and Europe's Cooperative ITS Credential Management System (CCMS) are two leading implementations of this model. However, certificate revocation, scalability, and computational overhead remain pressing issues. Hybrid encryption schemes that combine elliptic-curve cryptography (ECC) for key exchange and symmetric encryption (AES) for payload protection are increasingly adopted to reduce latency without compromising security [19].

4.2 Intrusion detection systems (IDS)

Even with encryption, insider attacks and zero-day vulnerabilities may compromise vehicular systems. Consequently, IDS have become an essential second line of defense. The effectiveness of existing IDS in real-time, high-mobility vehicular environments faces significant hurdles due to the highly dynamic nature of these systems.

The key challenges of the existing IDS mechanisms include:

- **High mobility and dynamic topology:** vehicular ad-hoc networks (VANETs) feature vehicles constantly moving, leading to rapid network topology changes. This necessitates that IDS mechanisms (especially for V2X communication) adapt quickly without sacrificing monitoring consistency or accuracy.

- **Real-time latency requirements:** vehicular threats (e.g., spoofing of BSMs) demand detection and response within milliseconds (≈ 100 ms) to prevent safety incidents. Computational complexity, particularly in advanced models, often conflicts with these low-latency constraints.

- **Resource constraints:** on-board units (OBUs) and ECUs possess limited computational resources (CPU, memory). Executing complex **anomaly-based IDS (A-IDS)** algorithms, which rely heavily on ML, risks system overload.

- **High false positives in anomaly-based systems:** the natural variability in legitimate vehicular behavior (e.g., traffic conditions, driving patterns) can generate numerous false alarms in A-IDS, potentially hindering the identification of genuine threats.

IDS approaches are generally categorized into:

4.2.1 Signature-based IDS

Signature-based IDS rely on predefined patterns of known attacks that are stored in an internal signature or rule database [20–23]. Each incoming event or network flow is compared against this repository of known malicious behaviors. When a match is found, the system flags the traffic as an attack instance. These signatures may correspond to specific characteristics within BSMs, particular communication ports, or other

identifiable features within the in-vehicle or V2X communication interfaces. Such systems are highly effective at detecting known attack patterns in network traffic or ECU command sequences, offering high accuracy and low false-positive rates for previously observed threats. However, their effectiveness is limited against novel or evolving attacks that do not yet have corresponding signatures in the database [24].

4.2.2 Anomaly-based IDS

A-IDS operate by identifying deviations from established patterns of normal vehicular behavior [25–28]. Unlike signature-based approaches that rely on known attack patterns, anomaly-based systems learn the typical operational profiles of ECUs, BSMs, or in-vehicle communication flows and flag instances that diverge significantly from these norms. Such anomalies may manifest through unusual signal strength variations, irregular message content or frequency, or timing discrepancies in messages exchanged between in-vehicle entities or V2X nodes. For example, if a vehicle suddenly transmits BSMs at an abnormal rate or from an unexpected location, the system classifies the behavior as suspicious.

These systems typically employ statistical models or ML algorithms to model normal traffic patterns and detect outliers dynamically. Their primary advantage lies in the ability to identify previously unseen or zero-day attacks, making them essential complements to signature-based mechanisms. However, anomaly-based approaches are prone to false positives, especially in highly dynamic vehicular environments where legitimate behavior can vary widely with context.

Recent research emphasizes hybrid intrusion detection frameworks that integrate both paradigms to enhance detection accuracy and resilience. For instance, CAN-bus anomaly detection models have used autoencoders and random forests to maximize detection accuracy with minimal computational overhead. Additionally, emerging edge-based IDS, deployed directly on OBUs, enable localized analysis to reduce bandwidth consumption and safeguard data privacy, aligning with the low-latency requirements of CV ecosystems.

4.3 Secure hardware and trusted execution environments

Hardware-based security adds a physical trust anchor to the CV ecosystem. Trusted platform modules (TPMs) and hardware security modules (HSMs) are increasingly integrated into ECUs to store cryptographic keys securely and enforce policy-based access. Mechanisms such as secure boot and firmware integrity verification ensure that only authenticated software can execute within vehicular subsystems. For instance, automotive manufacturers use TPM 2.0-based attestation to verify firmware signatures during startup. Emerging research also investigates trusted execution environments (TEEs) – such as ARM TrustZone – to isolate sensitive operations (e.g., encryption, key management) from untrusted software. These hardware-enforced partitions greatly reduce the success probability of privilege-escalation and code-injection attacks.

4.4 Blockchain-based trust management

Blockchain and distributed ledger technologies (DLT) provide a decentralized alternative to centralized certificate authorities. Vehicles can register transactions

(e.g., message validation, software update logs) on a tamper-evident ledger, creating a transparent and auditable trust framework. Decentralized identity management: blockchain can manage pseudonym certificates without relying on a single CA. Secure data sharing: smart contracts regulate when and how vehicular data are exchanged between stakeholders (OEMs, insurance providers, infrastructure) [29–32]. Reputation systems: nodes accumulate trust scores based on historical behavior, mitigating Sybil attacks. However, scalability and latency remain obstacles. Classical blockchains, such as Ethereum, have high transaction delays, which are unsuitable for real-time safety messaging. Lightweight or consortium blockchains (e.g., Hyperledger Fabric) and directed acyclic graph (DAG)-based ledgers are being explored to improve throughput.

4.5 AI for threat detection

ML has emerged as a key tool for identifying complex, dynamic cyber-attacks in CVs. Supervised and unsupervised models are applied to classify anomalies within CAN-bus data, telematics streams, or V2X packets. Supervised learning: uses labeled attack datasets to train classifiers such as SVM, random forest, or gradient boosting for detecting DoS or spoofing attempts. Unsupervised/deep learning: employs autoencoders, LSTM, and graph neural networks to detect deviations in temporal and spatial communication patterns. Federated learning (FL) and transfer learning approaches enable vehicles to collaboratively improve models without sharing raw data, preserving privacy. Nevertheless, ML-based systems remain vulnerable to adversarial manipulation, making explainability and robustness important future research directions.

Table 3 provides a comprehensive summary of the above-mentioned key solutions that are currently proposed to mitigate the impact of security and privacy threats in the CV environment.

5. Implementation barriers and deployment challenges

Despite the recognized necessity of IDS, their real-world deployment in CV ecosystems faces significant practical and operational obstacles.

Solution Ccategory	Threat protection	Key advantages	Major limitations
Cryptographic protocols	Ensure confidentiality and authentication	Standardized (IEEE 1609.2), mature, and interoperable.	Latency; complex revocation
Intrusion detection systems	Detect abnormal or malicious behavior	Effective on zero-day; complements PKI.	False positives; model drift
Secure hardware	Protect keys and boot integrity	HW-enforced trust; tamper resistance.	Cost; limited upgradability
Blockchain-based trust	Decentralized identity and logging	Transparency; nonrepudiation; auditability.	Scalability; added delay
AI-driven detection	Adaptive threat identification	Learns evolving patterns; improves resilience.	Adversarial ML risk; data quality needs

Table 3.
Security and privacy countermeasures against threats in connected vehicle environments.

5.1 Challenges specific to signature-based IDS (S-IDS)

- **Signature database maintenance:** S-IDS relies on static repositories of known attack patterns. In the automotive sector, the diversity of vehicle models, ECUs, and proprietary communication protocols necessitates constant, vendor-specific updates. Maintaining this global and rapidly changing signature database is computationally and logistically expensive.

- **Lag time for novel threats:** the core limitation remains the inability to detect zero-day or polymorphic attacks until a corresponding signature has been analyzed, developed, and deployed across the fleet – a process that can take critical time.

- **Integration across heterogeneous networks:** S-IDS must operate across disparate networks, including the high-speed Ethernet backbone, the security-lacking CAN bus, and V2X wireless links, requiring multiple, often incompatible detection engines.

5.2 Challenges specific to A-IDS

- **Profiling the "normal" state:** training A-IDS requires gathering massive datasets of "normal" vehicular behavior across all possible operating conditions (high speed, traffic, idle, different climate zones, etc.). Defining this normal baseline is complex, and any misprofiling leads directly to high false positive rates (FPR).

- **Resource overhead on ECUs:** sophisticated A-IDS, particularly those using deep learning (Autoencoders, LSTMs), demand substantial computational resources (CPU and memory). Deploying these heavy models directly on resource-constrained ECUs or OBUs can introduce unacceptable latency or even impair the primary function of the control unit.

- **Concept drift:** legitimate vehicular behavior is not static; it evolves with software updates, new hardware installations, and changes in driving patterns (e.g., the introduction of new ADAS features). The normal profile (**concept**) of the system **drifts** over time, forcing A-IDS to be continuously retrained and updated to maintain accuracy.

5.3 Architectural and operational hurdles

- **Legacy vehicle adaptation and protocol ossification:** incorporating security protocols or newer IDS mechanisms is extremely difficult for previous-generation vehicles. Furthermore, the inherent design of the existing CAN bus protocol is deeply entrenched; any fundamental security-focused change would necessitate significant, costly modification and recertification across the global automotive fleet, making it **practically infeasible** to update the protocol at this stage.

- **Standardization and interoperability:** the lack of universal security standards across OEMs and suppliers complicates the creation of interoperable IDS solutions that can be easily integrated into diverse vehicle architectures.

- **Mixed-mode transportation complexity:** the operation of connected and autonomous vehicles alongside nonconnected legacy vehicles and other transportation methods (e.g., pedestrians, bicyclists) creates a complex, unpredictable environment. IDS systems must accurately distinguish between malicious activity and the expected communication chaos resulting from this mixed-mode traffic.

- **Data privacy and bandwidth:** edge-based IDS deployed on OBUs generate vast amounts of data. Transmitting this raw data to a centralized analysis platform for global model updates consumes significant bandwidth and raises critical data privacy concerns regarding driver behavior.

6. Open research questions

Despite significant progress in securing CV environments, several research challenges remain unresolved. These open questions highlight critical areas for future exploration and development:

6.1 Scalability of security architectures

The scalability of public key infrastructure (PKI) and certificate management systems in large-scale vehicular networks remains a major bottleneck [17]. The dynamic nature of vehicular mobility demands real-time certificate issuance, revocation, and validation, which can overwhelm current centralized architectures. Research is needed on distributed or hybrid trust management systems that balance scalability, latency, and security.

6.2 Real-time constraints and security trade-offs

Security mechanisms often introduce computational overhead, which can conflict with the strict latency requirements of safety-critical applications such as collision avoidance [18]. Designing lightweight cryptographic algorithms that minimize on-board computational overhead – thus eliminating the need for cloud delegation – and developing context-aware authentication mechanisms capable of dynamically adapting to vehicular mobility and network conditions remain ongoing challenges.

6.3 Privacy preservation beyond location data

Most privacy research in V2X focuses on location confidentiality. However, behavioral privacy – protecting patterns derived from acceleration, braking, or route history – remains underexplored. Future systems must incorporate contextual privacy-preserving analytics, ensuring user trust while enabling necessary data sharing for safety and optimization.

6.4 Resilience against adversarial and AI-driven attacks

With the increasing integration of ML in vehicular systems, new attack surfaces have emerged through the adversarial manipulation of AI models [24]. Future

intrusion detection and perception systems must not only detect such adversarial perturbations but also continuously adapt to an evolving threat landscape without degrading real-time performance. Moreover, deploying ML algorithms in resource-constrained vehicular environments introduces additional challenges, as these models must operate with limited processing power and memory. Equally important is the need to handle previously unseen or novel attack patterns, which remain undetectable by conventional supervised learning models trained solely on historical data. Developing adaptive and resilient ML frameworks that can learn autonomously and maintain robustness under such dynamic conditions is, therefore, a critical area of ongoing research.

6.5 Postquantum and long-term security

As quantum computing advances, existing elliptic-curve and RSA-based cryptographic schemes may become vulnerable. Research into postquantum cryptographic (PQC) protocols tailored for low-latency vehicular environments is essential to ensure the long-term confidentiality and authenticity of V2X communications.

7. Conclusion

CVs represent the convergence of cyber-physical systems, wireless communication, and intelligent automation. While these technologies promise unprecedented benefits in safety, efficiency, and user convenience, they also introduce complex challenges in maintaining security, privacy, and trustworthiness across distributed vehicular ecosystems.

This chapter presents a structured overview of security and privacy threats in CV environments. It begins with an introduction to CV technologies and protocols, followed by a taxonomy of threat actors, attack surfaces, and representative attack models. We review existing countermeasures, including cryptographic frameworks, IDS, and blockchain-based approaches.

Despite these efforts, CV security remains a moving target. Future research must prioritize scalable security frameworks, lightweight yet robust cryptographic solutions, and privacy-preserving architectures that can adapt to dynamic vehicular networks. Moreover, as AI-driven autonomy and postquantum technologies emerge, interdisciplinary collaboration between cybersecurity, automotive engineering, and data science will be essential to ensure safe and trustworthy vehicular ecosystems.

Ultimately, the goal is to achieve a secure-by-design vehicular environment – where connectivity enhances, rather than undermines, the safety and privacy of all road users.

Acknowledgment

During the preparation of this chapter, AI-assisted tools, including **ChatGPT** and **Semantic Scholar AI**, were used to support language polishing and rephrasing of the content. The authors take full responsibility for the final text and its scholarly integrity.

Security and Privacy Threats in Connected Vehicle Environment
DOI: http://dx.doi.org/10.5772/intechopen.1014482

Author details

Ayan Roy
Christopher Newport University, Newport News, Virginia, USA

*Address all correspondence to: ayan.roy@cnu.edu

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

[1] Kenney JB. Dedicated short-range communications (DSRC) standards in the United States. Proceedings of the IEEE. 2011;**99**(7):1162–1182

[2] Roy A, Chakraborti R. Smart: Secure incentive-based mechanism for addressing reliability in trustworthy vanets. In: NOMS 2025-2025 IEEE Network Operations and Management Symposium; IEEE; 2025. 1–9

[3] EEE Computer Society LAN/MAN Standards Committee. "IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications." IEEE Std 802.11^ (2007). 2007

[4] EN ETSI. 302 665 V1. 1.1 (2010–09) Intelligent Transport Systems (Its); Communications Architecture. Sophia Antipolis*:* European Telecommunication Standards Institute*;* 2010

[5] Ning L, Cheng N, Zhang N, Shen X, Mark JW. Connected vehicles: Solutions and challenges. IEEE Internet of Things Journal. 2014;**1**(4):289–299

[6] Koscher K, Czeskis A, Roesner F, Patel S, Kohno T, Checkoway S, McCoy D, Kantor B, Anderson D, Shacham H, et al. Experimental security analysis of a modern automobile. In: 2010 IEEE symposium on security and privacy; IEEE; 2010. 447–462

[7] Petit J, Shladover SE.Potential cyberattacks on automated vehicles. IEEE Transactions on Intelligent Transportation Systems. 2014;**16** (2):546–556

[8] Papadimitratos P, Buttyan L, Holczer T, Schoch E, Freudiger J, Raya M, Zhendong M, Kargl F, Kung A, Hubaux J-P. Secure vehicular communication systems: Design and architecture. IEEE Communications Magazine. 2008;**46**(11):100–109

[9] Miller C, Valasek C. Remote exploitation of an unaltered passenger vehicle. Black Hat USA. 2015;**2015** (S 91):1–91

[10] Woo S, Hyo Jin J, Lee DH. A practical wireless attack on the connected car and security protocol for in-vehicle can. IEEE Transactions on Intelligent Transportation Systems. 2014;**16**(2):993–1006

[11] Leinmüller T, Schoch E, Kargl F, Maihöfer C. Decentralized position verification in geographic ad hoc routing. Security and Communication Networks. 2010;**3**(4):289–302

[12] Raya M, Hubaux J-P. Securing vehicular ad hoc networks. Journal of Computer Security. 2007;**15**(1):39–68

[13] Yan GY, Choudhary G, Weigle MC, Olariu S. Providing vanet security through active position detection. In: Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks; 2007. 73–74

[14] Haas JJ, Yih-Chun H, Laberteaux KP. Design and analysis of a lightweight certificate revocation mechanism for vanet. In: Proceedings of the sixth ACM international workshop on VehiculAr InterNETworking; 2009. 89–98

[15] Roy A, Madria SK. Cansafe: An mtd based approach for providing resiliency against dos attack within in-vehicle networks. In: 2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC);. IEEE; 2022. 3243–3250

[16] Csikor L, Lim HW, Wong JW, Ramesh S, Parameswarath RP, Chan MC. Rollback: A new time-agnostic replay attack against the automotive remote keyless entry systems. ACM Transactions on Cyber-Physical Systems. 2024;**8**(1):1–25

[17] Whyte W, Weimerskirch A, Kumar V, Hehn T. A security credential management system for v2v communications. In: 2013 IEEE Vehicular Networking Conference; IEEE; 2013. 1–8

[18] Zhang C, Rongxing L, Xiaodong Lin P-HH, Shen X. An efficient identity-based batch verification scheme for vehicular sensor networks. In: IEEE INFOCOM 2008-The 27th Conference on Computer Communications; IEEE, 2008. 246–250

[19] Gerlach M, Guttler F. Privacy in vanets using changing pseudonyms-ideal and real. In: 2007 IEEE 65th Vehicular Technology Conference-VTC2007-Spring; IEEE, 2007. 2521–2525

[20] Anjum F, Subhadrabandhu D, Sarkar S. Signature based intrusion detection for wireless ad-hoc networks: A comparative study of various routing protocols. In: 2003 IEEE 58th Vehicular Technology Conference. VTC 2003-Fall (IEEE Cat. No. 03CH37484), volume **3**, IEEE; 2003. 2152–2156

[21] Deng Z, Liu J, Xun Y, Qin J. Identifierids: A practical voltage-based intrusion detection system for real in-vehicle networks. IEEE Transactions on Information Forensics and Security. 2023;**19**:661–676

[22] Jenefa J, Anita EAM. Identity-based message authentication scheme using proxy vehicles for vehicular ad hoc networks. Wireless Networks. 2021;**27**(5):3093–3108

[23] Jin S, Chung J-G, Yinan X. Signature-based intrusion detection system (ids) for in-vehicle can bus network. In: 2021 IEEE International Symposium on Circuits and Systems (ISCAS), 2021. 1–5

[24] Eykholt K, Evtimov I, Fernandes E, Li B, Rahmati A, Xiao C, Prakash A, Kohno T, Song D. Robust physical-world attacks on deep learning visual classification. In: Proceedings of the IEEE conference on computer vision and pattern recognition; 2018. 1625–1634

[25] Abrar MM, Islam R, Satam S, Shao S, Hariri S, Satam P. Gps-ids: An anomaly-based gps spoofing attack detection framework for autonomous vehicles. ArXiv. 2024; abs/2405.08359

[26] Aksu D, Aydin MA. Mga-ids: Optimal feature subset selection for anomaly detection framework on in-vehicle networks-can bus based on genetic algorithm and intrusion detection approach. Computers & Security. 2022;**118**(102717):102717

[27] Kishore CR, Rao DC, Nayak J, Behera HS. Intelligent intrusion detection framework for anomaly-based can bus network using bidirectional long short-term memory. Journal of the Institution of Engineers (India): Series B. 2024;**105**:1–24

[28] Liu J, Fan W, Dai Y, Lim E, Pan Z, Lisitsa A. Leveraging semi-supervised learning for enhancing anomaly-based ids in automotive ethernet. In: 2024 IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom); 2024. 1563–1571

[29] Roy A, Madria SK. Blame: A blockchain-assisted misbehavior detection and event validation in vanets. In: 2021 22nd IEEE International Conference on Mobile Data Management (MDM); 2021. 69–78

[30] Memary E, Shen C-C, Guo H, Nejad MM. Trcoin: A blockchain-based robust trust management system for vanet. Journal on Autonomous Transportation Systems. 2025;**2**(1):–20

[31] Kudva S, Badsha S, Sengupta S, Hung L, Khalil I, Atiquzzaman M. A scalable blockchain based trust management in vanet routing protocol. Journal of Parallel and Distributed Computing. 2021;**152**:144–156

[32] Bohan L, Liang R, Zhu D, Chen W, Lin Q-X. Blockchain-based trust management model for location privacy preserving in vanet. IEEE Transactions on Intelligent Transportation Systems. 2021;**22**:3765–3775

Chapter 7

Security and Privacy of ITS Standards and Their Research Challenges

Takahito Yoshizawa

Abstract

Intelligent Transport System (ITS) enables communication among entities on the road, including vehicles, roadside units (RSUs), pedestrians, and cyclists. This communication plays a key role in cooperative, connected, and automated mobility (CCAM). As a result of standardization work by standard developing organizations (SDOs) such as IEEE, SAE, and ETSI, ITS standards consist of a number of specifications in both the United States and Europe. However, close examinations of the security and privacy aspects of these standards reveal a number of significant unresolved issues. These security and privacy issues arise from some of the fundamental operational circumstances under which vehicles operate. We discuss various types of adversarial attacks and other system-level issues that have a high impact on road safety. This point raises significant concerns about the integrity of the ITS system. At the same time, new trends in cybersecurity have emerged over the past years, such as the evolution of quantum computers and their threats to break certain mathematical problems, such as those used in public-key cryptography. National Institute of Standards and Technology (NIST) in the United States and cybersecurity organizations in Europe have announced timelines to migrate to post-quantum cryptography (PQC) algorithms. Being a real-time cyber–physical system (RT CPS), ITS systems also need to adapt to this changing paradigm shift in cybersecurity to ensure that vehicular communication remains secure, resilient, and trustworthy. However, the nature of RT CPS raises its unique problems. This chapter discusses these challenging issues in the security and privacy aspects of ITS standards.

Keywords: ITS, security and privacy, vehicular communication, V2X, V-PKI, PQC migration

1. Introduction

Vehicular communication, or so-called Vehicle-to-everything (V2X), is the enabling technology of the Intelligent Transport System (ITS). This communication capability in vehicles plays a key role in realizing cooperative, connected, and automated mobility (CCAM). The objective of this V2X communication is to improve road safety by sharing information about vehicle movements and other

relevant data, which enables proactive detection of dangerous situations before accidents occur. Unlike other vehicle sensors, such as radar, LiDAR, and cameras, radio communication is not restricted by line-of-sight (LoS). This characteristic supplements these sensors and enhances road safety. Safety-related messages in V2X are called basic service messages (BSMs), standardized by SAE in the United States [1], and cooperative awareness messages (CAMs) and de-centralized environmental notification messages (DENMs), standardized by ETSI ITS in Europe [2].

As vehicles become computerized, the security of the ITS system becomes an important aspect, as V2X communication represents a cyber–physical system (CPS) – its unintentional consequences can result in injury or property damage. The security and privacy aspects are specified in IEEE 1609.2 and 1609.2.1 for the United States, and in the ETSI ITS standard for Europe [2].[1]

The key element of the security solution for the ITS system is the public key infrastructure (PKI) system, which issues digital certificates to vehicles and other entities within the ITS system. Communication privacy is addressed through the use of pseudonym certificates and by periodically changing them to avoid the tracking of vehicles. However, upon close examination of these specifications, a number of issues emerge. The causes of these issues vary; some are fundamental limitations of the solution, while others arise from detailed designs of the specifications. Yet another cause is the consequence of recent technological advancements and their impacts on cybersecurity. One notable case is the threat posed by the advancement of quantum computers (QCs).

In this chapter, we discuss the following security and privacy-related issues in these ITS standards: (1) possible cyberattacks on the V2X communication, (2) issues in PKI-based certificate usage, (3) issues associated with the pseudonym-based privacy protection scheme, (4) integration of non-vehicle entities into the ITS system, and (5) impacts of PQC migration. Our discussion of these points concisely presents the current open issues of security and privacy in ITS standards.

These are urgent issues; not resolving them likely results in a situation where V2X communication becomes not only unusable but also actively undermines the safety of the road. Through our research work, we have observed that attention to the security and privacy aspects of V2X communication is low within the research community. In this sense, our contribution is to raise awareness among a wider audience of these open issues in the security and privacy aspects of the ITS standards.

2. Security and privacy issues of vehicular communication (V2X)

V2X communication involves several security and privacy issues. These issues originate from multiple aspects: (1) open communication as the fundamental nature of the vehicular network, (2) certificate-based message verification, (3) dependence on pseudonymity as the privacy protection, (4) integration of non-vehicle entities, and (5) migration to new signature algorithms. They represent significant challenges, given that the objective of V2X communication is to improve traffic safety due to its usage, not the opposite. The overview of these security- and privacy-related issues is captured in **Figure 1,** and the key issues are summarized in **Table 1**, indicating the respective sections for detailed discussions.

[152]As ETSI ITS standard specifications are organized based on specific topical areas, many specification documents exist, each of them focusing on specific areas and sub-areas of the ITS system. A representative specification is the security architecture in TS 102 940 [11].

Figure 1.
Overview of ITS security and privacy issues.

Security and privacy issues	Discussion
No protection against various types of attacks	Section 2.1.2
Certificate management issues	Section 2.2.2
Pseudonym-related issues	Section 2.3.2
Vulnerable road user (VRU)-related issues	Section 2.4.2
No PQC migration solution	Section 2.5.2

Table 1.
List of security issues.

2.1 Open nature of communication and its vulnerabilities

2.1.1 Discussion

The fundamental aspect of vehicular communication that serves as the underlying constraint from a security perspective is its dynamic nature, that is, vehicles move, by definition. Thus, it makes its network topology highly dynamic. From a given moving vehicle's perspective, random unknown vehicles enter and exit its communication range at any time. Maintaining the exact set of vehicles within its communication range under all circumstances is neither practical nor realistic. Due to this nature, V2X communication necessarily uses a broadcast mode. In broadcast mode, messages transmitted by a vehicle are received by all vehicles within its range. This is the fundamental mode of operation in communication with an unknown number of vehicles in one's vicinity. This implies that safety messages discussed in Section 1 are transmitted in plain text, that is, no confidentiality protection (encryption) is applied in all standardized message services.[2]

Due to the nature of this "open" plain-text-based communication, any entity capable of receiving messages can receive, store, analyze, and even replay them. All of the attack types discussed in this section represent significant security vulnerabilities. These attacks are easy to execute and can potentially cause significant impacts on road safety. Furthermore, there is no effective mechanism to differentiate malicious senders from honest ones.[3]

2.1.2 Open issues in standards

Eavesdropping: Eavesdropping is a passive attack that involves listening to the communication channel and inferring various information that can be obtained from the messages on this channel, including the message contents as well as metadata associated with them. Because all BSMs are transmitted in clear (i.e., without encryption) broadcast mode, any passive adversaries capable of accessing the ITS spectrum can listen to and process all communication that takes place. Furthermore,

[154]t is generally possible to employ encryption in group communication. However, maintaining encryption keys in a highly dynamic operating environment, such as V2X, will significantly complicate its operation; thus is not practical.

[3] Much of the reasons for these characteristics are due to the use of privacy-protection mechanisms.

determined adversaries may install eavesdropping devices at multiple locations simultaneously over an extended period to collect a large amount of data. In this way, they can collect, store, correlate, and integrate information from a wide area over time to analyze vehicle movement on a larger scale. In fact, receiving and storing messages are necessary parts of constructing and maintaining a "dynamic map" for honest vehicles to understand their surroundings and determine safe conditions. In this sense, being "open" is a necessary element to achieve road safety. At the same time, this fundamental nature implies that there is no defense against this type of passive attack.

Replay attack: Replay attack is possible in CAM and vulnerable road user (VRU) awareness messages (VAMs) in ETSI ITS [3, 4] and BSMs in SAE J2,735 [1]. Although these messages contain a timestamp, they fall short of serving the intended purpose to detect "old" messages. The timestamps in both CAM and VAM messages are defined as "`generationDeltaTime = TimestampIts mod 65,536`" where TimestampIts is an integer (msec) since `2004-01-01T00:00:00:000Z` [3] in the ETSI ITS standard. In SAE J2735, the timestamp in BSM messages is defined as "`DSecond::= INTEGER(0..6,5535)`" with the valid range of 60,000 to 60,999 to represent milliseconds within a minute [1]. Due to this definition, the timestamp in these messages wraps around every 65.536 and 60 seconds, respectively. This means that a message sent at time $t = n$ (seconds) is also valid at $t = n + c * i$, where c is the cadence of either 65.535 (ETSI CAM/VAM) or 60 seconds (SAE J2735 BSM) and i is any integer. This replayed message is still perfectly valid as all information elements within the message are valid, that is, the message content, the certificate, and the signature, given that the original message was sent by a legitimate vehicle holding a legitimate certificate with a valid signature. In other words, the replayed messages are valid as long as the certificate in the message is valid (i.e., not expired or revoked). Furthermore, no modification of the message is required; simply store and replay it at a later time of this timestamp with the stated cadence.

Combined with the absence of confidentiality protection, any adversary capable of receiving and storing CAM, BSM, and VAM messages can replay the stored messages as valid when they are sent at the right timing. Because the replayed message is still valid, receiving vehicles of those messages have no way to tell that the messages are "fake" and sent by an adversary. This situation means that adversaries can effectively create any number of "fake vehicles" that do not exist in reality and cause other vehicles on the road to react to these fake vehicles accordingly.

For example, if a vehicle perceives that a fake vehicle "appears" to be immediately in front of it, this vehicle may trigger actions that can negatively impact road safety. If it is a conventional human-driven vehicle, it likely triggers a warning indication on the dashboard to alert the driver, who becomes confused by the contradictory alert indication when the driver perceives no danger. If it is an autonomous vehicle (AV), it may decide to take an action to prevent an accident, for example, hard braking. Such a reaction by AVs can cause an even more dangerous situation, as other vehicles may consider that this AV has applied brakes for no reason.[4]

[155]This point implies that relying solely on V2X messages to determine vehicle maneuver can be dangerous. Instead, vehicles need to combine other sensor inputs to determine the validity of received messages. However, mandating such implementation is outside the scope of ITS standards.

Identity attack: As stated in the "replay attack" scenario above, adversarial vehicles can receive and store messages transmitted by other vehicles they encounter on the road.[5] A possible attack by adversaries is to intentionally use the same pseudonym identity that another vehicle uses. It is a type of "spoofing attack". The consequence is that multiple vehicles transmit messages using the same identity, confusing other vehicles that receive these messages.[6] Because each vehicle independently selects its pseudonym identities, other vehicles cannot identify or determine which vehicle is honest or adversarial. As a consequence, other vehicles cannot map one-to-one between a pseudonym identity and a pseudonym certificate. This condition results in a confused state when maintaining a dynamic map of their surroundings. In other words, if the two vehicles using the same pseudonym identity are distinctively different in their position and movement, as indicated in their CAM message content, other vehicles are not able to tell which identity is mapped to which vehicle's movement. This condition can result in a potentially dangerous situation in which other vehicles cannot make safe maneuvering decisions.

Sybil attack: Another identity-related attack is a Sybil attack. It is a type of attack in which an adversary uses multiple identities in its communication in such a way that transmissions by a single entity appear as multiple entities. The vehicular PKI (V-PKI) system architecture defined in both the IEEE 1609.2 [5] and ETSI ITS [3] standards specifies that the V-PKI system provisions a pool of pseudonym certificates to vehicles with overlapping validity periods. These standards suggest periodically changing pseudonym identities and certificates for privacy protection purposes without specifying the exact change scheme.[7]

An extreme scheme is to change pseudonyms in every message a vehicle transmits from the pool of available pseudonyms, randomly or otherwise. This effectively results in a Sybil attack. It should be noted that this usage pattern of pseudonym ID and certificate is one extreme type of certificate reuse scheme and does not necessarily imply adversarial intent. To put it another way, strictly speaking, IEEE 1609.2 and ETSI ITS standards do not "prohibit" this type of pseudonym change scheme, although it results in adversarial attack behavior.

Gray-hole attack: Gray-hole attack refers to a malicious node that selectively drops or mishandles message forwarding so that receivers do not receive all expected packets [6]. In V2X communication, the same result can effectively occur due to the vehicle's own internal mechanism to avoid channel congestion. In the ETSI ITS standard and 802.11p-based DSRC, the decentralized congestion control (DCC) mechanism checks the communication channel usage and withholds outbound packets if the usage level exceeds the pre-determined threshold [7–10]. It should be noted that this is a necessary mechanism as a MAC layer function to prevent channel saturation from occurring. However, from a security perspective, this mechanism inadvertently creates a self-inflicted gray-hole attack situation. This poses

[5] Strictly speaking, honest vehicles also need to receive and store information in its internal memory to perform the normal V2X communication functionality. In this sense, the difference between honest vehicles and adversarial vehicles is the presence or absence of adversarial intent only. However, it is beyond the scope of our discussion.

[6] Because pseudonym identities are randomly determined by individual vehicles, strictly speaking, multiple vehicles within the same transmission range selecting the same pseudonym identity is significantly low, but not impossible.

[156] These standards require that all identities, that is, pseudonym ID, MAC address, IPv6 address (in case of IPv6 packets), and pseudonym certificate to be changed at the same time. This is to prevent observers from linking different layers' identities.

a challenging situation to resolve, given the nature of this functionality proactively preventing performance degradation on the communication channel. In other words, the absence of this functionality also implies that channel congestion may occur as a result of no mitigation mechanism being in place, and similar message loss may occur as a result. However, from a security perspective, it appears as a type of attack.

DoS attack: Physical layer attacks, for example, transmitting a jamming signal, result in a degradation of signal quality. Eventually, the channel quality degrades to such an extent that it is no longer usable for communication. In addition, a MAC layer attack, for example, transmitting "bogus messages" to occupy the channel, results in channel congestion. In both cases, a DoS attack situation arises, that is, honest vehicles cannot transmit or receive legitimate messages.

2.1.3 Possible solutions, research needs and challenges

Attack types discussed in this section are rooted in the open nature of the safety messages. Furthermore, it is a necessary part of achieving awareness of "honest" vehicles. In this sense, the problem is rooted in the fundamental conflict between openness and the need to defend against adversarial behaviors in this operating environment. This openness poses a fundamental challenge to the effectiveness of V2X communication. (→ **Difficulty level:** Very high)

Research challenges to address the open issues raised in the preceding discussion are as follows.

(1) Investigate a novel approach to applying confidential protection or an equivalent scheme in broadcast-based communication to prevent passive attacks, such as eavesdropping, specifically paying attention to the constraints in real-time CPS (RT CPS).

(2) Investigate how to mitigate or prevent various active attacks, for example, replay attack, identity attack, Sybil attack, gray-hole attack, and DoS attack.

2.2 PKI-based certificate usage

2.2.1 Discussion

Much of the security solution in the ITS standards is concerned with the use of PKI. The V-PKI system is responsible for generating, issuing, and managing digital certificates for vehicles [5, 11]. Specifically, transmitting vehicles generate a message signature and attach it to the message upon sending it; receiving vehicles verify the message's integrity by checking the signature and the sender's authenticity by checking the certificate chain to the root certificate authority (RCA). These operations are performed using public-key cryptography called the Elliptic Curve Digital Signature Algorithm (ECDSA). The transmitting vehicles generate a signature using their private key, and the receiving vehicles verify it by using the corresponding public key carried in the digital certificate, which is appended to the upper-layer message upon transmission. Due to this mechanism, V-PKI is an essential functionality of the ITS management system. In other words,

the specifics and details of the V-PKI system and its vehicle operations are the largest part of the security solution for V2X communication in the standards. Due to the absence of confidentiality protection, this is the only security solution in the ITS standards.

2.2.2 Open issues in standards

Absence of inter-V-PKI coordination: Both IEEE 1609.2 and ETSI ITS standards specify the V-PKI's system architecture and its operations. These architectures are described from a single V-PKI perspective only; considerations on necessary interactions among multiple V-PKI systems are absent. The need for this is evident when we consider environments such as Europe, where countries share borders and vehicles freely cross them as normal daily events. The V-PKI systems are deployed at an individual country level at the maximum or at a smaller level, such as a province or other jurisdiction [12]. Thus, interactions among V-PKI systems are a necessity. One such example is the sharing of revocation-related information. The absence of such information sharing across V-PKI systems implies that the dissemination of revocation status (e.g., CRL distribution) or misbehavior reporting of "roaming" vehicles cannot be communicated to/from their "home" V-PKI system. This means that the standardized V-PKI-related functionalities collapse as soon as vehicles belonging to different V-PKI systems are involved. This is a significant architectural issue. Given that the ITS system involves multiple nations, this issue cannot be left as an implementation-dependent matter to ensure a uniform and standardized solution [13].

Absence of effective revocation: Besides issuing certificates, another important function of the V-PKI system is to revoke certificates if and when necessary. For example, positive detection of a misbehaving vehicle requires prompt revocation of all its outstanding certificates.[8]. The dissemination of revocation information is defined in IETF standards, such as Certificate Revocation List (CRL), Online Certificate Status Protocol (OCSP), and its variants. However, implementing a reliable revocation mechanism is far from trivial, as we witness from the fragmented revocation solutions in the context of internet web browsers [14]. In the browser context, browser vendors implement their proprietary solutions, which are gaining more traction in how revocation is done in practice.

Within the context of V-PKI, both IEEE 1609.2 and ETSI ITS rely on CRL or no revocation at all. The CRL approach is known to have limitations in ensuring the reliable dissemination of revocation information. The "no revocation" approach is built upon the "short-term certificate" concept [15]. However, the ITS standards neither specify nor recommend the exact duration of the validity period of pseudonym certificates. In this sense, how revocation is done in practice is unspecified and likely results in an implementation-dependent matter. Leaving the actual solution to an implementation decision implies that the actual effectiveness in practice will vary from one system to another. This approach goes against the goal of creating a uniform and effective solution.

[158] A similar operation will be required when a vehicle is unenrolled (i.e., reverse operation of enrollment of a vehicle) from the V-PKI system, for example, when a vehicle is de-registered from the vehicle registration office.

2.2.3 Possible solutions, research needs and challenges

An obvious gap is the absence of standardization to define inter-V-PKI system interactions. This involves defining inter-system architecture and messages among multiple V-PKI systems. This definition includes distribution of CRL and misbehavior reporting across the V-PKI system boundary. As this is already a well-defined problem scope, a solution may be designed and standardized within IEEE 1609.2 and ETSI ITS without requiring academic research. However, the dissemination of revocation information requires further research. (→ **Difficulty level:** High)

Research challenges to address the open issues raised in the preceding discussion are as follows.

(1) Investigate how the V-PKI system architecture can be extended to ensure that inter-V-PKI system communication is facilitated, including aspects such as defining reference points, messages, and information that can be exchanged among multiple V-PKI systems.

(2) Investigate potential schemes and solutions to effectively revoke certificates, specifically considering the operating environment of moving traffic and vehicles.

2.3 Pseudonymization as privacy protection

2.3.1 Discussion

The definition of privacy includes five properties: "anonymity," "pseudonymity," "unlinkability," "undetectability," and "unobservability." The precise definition of these properties is given in literature [16, 17]. Specifically, it is important to note that the concepts of anonymity and pseudonymity are similar but different. To be precise, anonymity disassociates information from specific individuals. Thus, it is not possible to identify a specific individual from anonymized data. On the contrary, pseudonymity can be traced to an individual with the use of additional information; thus, pseudonymized data are still personal data [18]. From this, we note that the sole use of pseudonyms is not sufficient to guarantee users' anonymity.

As a solution for privacy protection, both IEEE 1609.2 and ETSI ITS standards require ITS stations to: (1) periodically change pseudonyms, and (2) change other identities (pseudonym certificate, MAC address, and IPv6 address (if applicable)) simultaneously. From a practical perspective, the expected behavior in vehicles is to change the pseudonym identity within a certain period on the order of minutes or after transmitting a specific number of messages. ETSI ITS documents multiple approaches to pseudonym change schemes based on academic literature [19]. However, it is not a normative specification; thus, no scheme is specified as a normative solution. The likely outcome is that the exact pseudonym change scheme is left to individual implementations.

2.3.2 Open issues in standards

Incomplete coverage of privacy properties: Based on the privacy properties described in this section and in literature [16, 17], it is clear that users' anonymity is

not guaranteed by simply applying pseudonyms unless additional and supplemental mechanisms are in place to ensure that any other additional data from other sources, such as related metadata, does not lead to positive user identification.

There are solutions such as mix zones [20] and silent periods [21], but they have unique issues.[9] Furthermore, we note that the existing standards do not address the remaining three privacy properties, namely unlinkability, undetectability, and unobservability.

Absence of standardized pseudonym change scheme – impacts of proprietary implementations: The situation described in this section implies that the effectiveness of privacy protection varies from one implementation to another, resulting in a situation where certain vehicle makes or types are more prone to compromising privacy than others, based on metadata such as a vehicle's usage pattern and frequency, and the locations they travel to and from.

This is far from ideal from the vehicle owners' perspectives – all vehicle owners should be entitled to an equal level of guarantee in privacy protection, irrespective of the make and model of their vehicle. From this perspective, both standards should specify a standardized pseudonym-change scheme to avoid these variations in effectiveness.

2.3.3 Possible solutions, research needs and challenges

ETSI ITS has already conducted a study on this subject in literature [19]. Based on this, both IEEE 1609.2 and ETSI ITS should take a step further to specify a normative pseudonym change scheme. Furthermore, additional academic research to identify new innovative solutions on the unaddressed privacy properties will be beneficial to fully cover the privacy aspect. (→ **Difficulty level:** Medium to high)

Research challenges to address the open issues raised in the preceding discussion are as follows in order to improve privacy protection.

(1) Investigate and standardize an effective pseudonym change scheme.

(2) Investigate approaches and solutions to address the other privacy properties that are not addressed in the existing standards, namely unlinkability, undetectability, and unobservability.

2.4 VRU integration into the V-PKI system

2.4.1 Discussion

ITS communication is extended to include VRUs with the intent to extend road safety to non-vehicle road users, such as pedestrians and cyclists. The devices used by these entities transmit VAMs so that vehicles in the vicinity become aware of the presence and movement of these VRUs [4]. Some VRU entities, such as bicycles and electric kickboards, may be equipped with an embedded device dedicated to this

[9] For example, the use of mix zone can only take place in specific places, such as intersections with multiple vehicles traversing. Silent period negatively impacts road safety as vehicles voluntarily withhold communication for a certain period of time.

purpose. However, for other VRU types, such as pedestrians, various literature assumes that "smartphones" will be the device of choice.[10]

2.4.2 Open issues in standards

Modification of V-PKI architecture and its functionalities: The integration of VRUs into the ITS system implies including generic consumer devices as legitimate members of V2X communication. From the security perspective, the functionalities of the V-PKI system also need to be extended to accommodate these non-vehicle device types. This includes not only enrolling smartphones and provisioning certificates to them, but also verifying and ensuring that they are legitimate devices owned and used by legitimate users rather than adversaries with malicious intent [22]. In this sense, both IEEE 1609.2 and ETSI ITS standards need to be updated to include these additional functionalities in the V-PKI system.

Privacy challenge of VRUs: For the purpose of protecting the privacy of vehicle owners, ITS standards specify the use of pseudonyms and periodically changing them [11, 19]. Similarly, privacy protection also needs to cover VRUs as they are integrated into the ITS system. Furthermore, the relationship between a *smartphone* and an individual is much tighter than that between vehicles and their user(s).[11] In this sense, the relationship between a vehicle and its driver/passengers is not one-to-one. On the contrary, a smartphone is used by a single person only – it is not shared with anybody else. It is a strict one-to-one relationship. In this sense, the need for privacy protection for smartphones requires being more stringent than that of vehicles.

VRU dynamics and the reliability of VAM: The kinetic dynamics of vehicles and those of VRUs are fundamentally different. This difference may have a significant influence on the reliability of VAM messages. For example, a pedestrian's inertia is significantly lower than that of vehicles – a pedestrian can start/stop and make a U-turn within a second, while vehicles have much higher momentum and are not able to make such agile movements as pedestrians do. In addition, VRUs can change their state over time. For example, a pedestrian is no longer a pedestrian when she steps on a bus; similarly, a bus passenger becomes a pedestrian when she hops off the bus. This agility or change of state in VRUs makes it significantly challenging to predict VRU's movements and accurately reflect and update them in the VAM messages these devices transmit.[12] Annex G in the VAM specification [4] contains an informative annex that describes this point. In order for VAM messages to accurately reflect the VRU's movements and positively contribute to improving road safety, this point needs to be resolved.

[10] Due to the proliferation of smartphones that consumers use for various aspects of daily life, from browsing the Internet to chatting with friends and family to making phone calls, it is highly unlikely that pedestrians will purchase and use purpose-specific devices such as ones that only serve V2X communication [28].

[11] For example, a privately owned passenger vehicle may be shared by the family members, a city bus is typically occupied by passengers who don't know one another, and a taxi has different customers at different times and locations.

[161] Another interesting question is the change of state of pedestrians – once a pedestrian steps on a bus, she becomes a passenger and is no longer a pedestrian. When she steps off a bus and starts walking, she becomes a pedestrian again. The question is how the user's device accurately reflects this change of state in the VAM messages.

2.4.3 Possible solutions, research needs and challenges

The points raised in this section likely require significant research and standardization work. Including consumer devices in the V-PKI system requires architectural change to include additional functionalities, such as verifying the legitimacy of the device and/or the user, which may involve vetting by mobile operators to verify an active subscription. The need for a higher level of privacy protection for smartphones likely requires a different pseudonym usage scheme from vehicles. Furthermore, VRU dynamic is a difficult problem to address. (→ **Difficulty level:** Very high)

Research challenges to address the open issues raised in the preceding discussion are as follows.

(1) Define architectural changes necessary to accommodate non-vehicle consumer-type devices (i.e., smartphones) within the V-PKI system.

(2) Investigate schemes and solutions on how to verify that consumer-type devices are legitimate, with legitimate users behind them, upon enrolling them in the ITS V-PKI system.

(3) Investigate schemes and solutions for detecting "misbehavior" of non-vehicle consumer-type devices in the ITS V-PKI system and revoking outstanding certificates. This includes the effective dissemination of revocation information to all relevant entities in the ITS system (e.g., vehicles on the road and other VRUs in the vicinity).

(4) Investigate schemes and solutions on how to enhance privacy protection for consumer-type devices in the ITS system, such as smartphones.

(5) Investigate schemes and solutions on how to make the VRU's movement in the VAM message more reliable, considering the different dynamics of some VRU types.

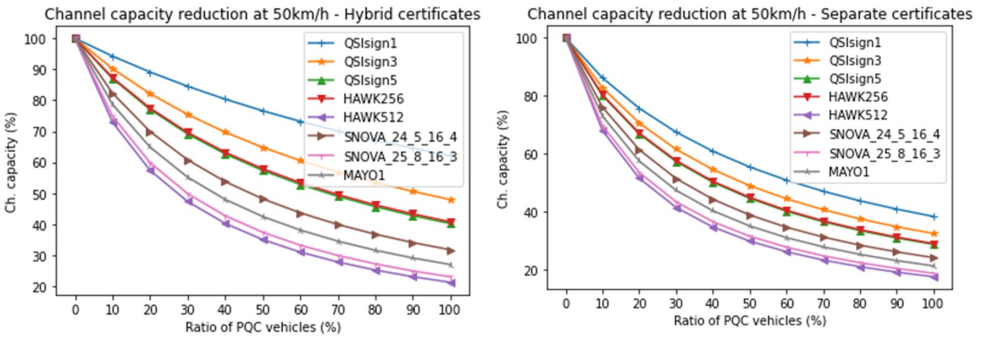
2.5 PQC migration

2.5.1 Discussion

National Institute of Standards and Technology (NIST) is the *de facto* SDO for standardizing cryptography-related technologies, such as encryption and hash function algorithms. To address the threats posed by the evolution of QCs [23], they initiated the PQC standardization process in 2016. After three rounds of evaluation cycles, they published the results of their evaluation in 2022 [24]. This report announces the selected algorithms: one public-key encapsulation mechanism (KEM) and three signature algorithms.[13]

Later in the same year, NIST announced a call for additional signature schemes, specifically stating that they were interested in schemes that "*are not based on*

[162] The standardized signature algorithms are CRYSTALS-Dilithium, Falcon, and SPHINCS+. The first two are lattice-based, and the last one is a hash-based scheme [24].



(a) Hybrid Certificate (b) Separate Certificates

Figure 2.
Impact on the channel capacity reduction at 50 km/h for PQC algorithms in the ongoing NIST competition.

structured lattices" and that they "*may also be interested in signature schemes that have short signatures and fast verification*" [25].

At the time of writing (Fall 2025), 14 candidate algorithms for additional signature schemes have been selected for the second-round evaluation process, and the finalists for the third-round evaluation are expected to be announced in 2026 [26].

The problems associated with the migration toward PQC algorithms, specifically in the RT CPS, are twofold: (1) the hardware platform's capability to handle the processing required to generate a PQC algorithm signature at the transmitting end and verify it at the receiving end within a specific time bound, and (2) the additional communication channel usage due to the increased size of the public key in the certificate and the signature carried in the message. Both these aspects are unfortunate but a natural consequence of PQC migration in RT CPS systems. The first concerns the extra computation overhead and memory/storage usage; the latter concerns the efficiency of the communication channel usage. We focus our discussion on the latter point.[14]

We have analyzed the impact on the latter aspect of the standardized signature algorithms [24] and concluded that the channel capacity will significantly reduce as a result of PQC migration [22]. Even the best-case scenario (*Falcon 512*) will result in approximately a 50% reduction of channel capacity when approximately 30% of vehicles migrate to this PQC algorithm.[15]

We have further analyzed the public key and the signature sizes of the 14 candidate schemes in the ongoing NIST competition and investigated their impacts on the communication channel [26]. The results are shown in **Figure 2**.[16] These two figures show channel capacity reduction based on the "hybrid" certificate (left) and "separate"

[14] The former aspect is directly dependent on specific signature algorithm and hardware implementations, for example, processor and memory/storage usage. However, the latter directly results from the increase in public key and signature size unique to specific PQC algorithms being used.

[15] In this discussion, the "channel capacity" means the number of messages transmitted in a unit time, for example, messages/second, not the total number of bits/second as this value remain constant irrespective of the message size increase.

[163] The 14 candidates in the ongoing NIST competition are: CROSS, LESS, HAWK, Mirath, MQOM, PERK, RYDE, SDitH, UoV, MAYO, QR-UOV, SNOVA, FAEST, SQIsign. All of them have three different security

certificates (right), respectively. A hybrid certificate refers to a certificate format in which a public key (K_P) and an issuing CA's signature (Sig_{CA}) of both legacy ECDSA ($K_{P\ -\ ECDSA}$, $Sig_{CA\ -\ ECDSA}$) and PQC ($K_{P\ -\ PQC}$, $Sig_{CA\ -\ PQC}$) are present. A separate certificate refers to the conventional approach, where two different certificates, containing either the ECDSA-based public key and CA's signature ($K_{P\ -\ ECDSA}$, $Sig_{CA\ -\ ECDSA}$) or the PQC-based ones ($K_{P\ -\ PQC}$, $Sig_{CA\ -\ PQC}$) are separately transmitted.

Our finding regarding the signature algorithms of the ongoing competition was not significantly different from our previous analysis [22]; the impact on the channel capacity is less than that of the three algorithms standardized in 2022. However, even the impact of the smallest public key size still significantly reduces channel usage. For example, as shown in **Figure 2a**, the smallest public key size (QSIsign1) will result in approximately 20% capacity reduction when 50% of the vehicles use hybrid certificates.

The conventional way to convey the public key is to attach a certificate (which contains a public key) to the upper-layer message and send them together. In periodic messages, such as CAM and BSM, messages are transmitted at the maximum rate of 10 messages/second. In this case, attaching the certificate to every message is redundant. For this reason, the existing standards allow vehicles to omit the certificate in CAM/BSM messages to optimize the channel usage in such a way that the certificate is attached only at a frequency of one per /second or less. When a certificate is omitted, a certificate "digest" (eight octets long) is attached. This scheme requires receiving vehicles to dynamically resolve unknown digests by querying other vehicles within the communication range, and a vehicle that has the full certificate corresponding to the digest responds to this request. This mechanism is called peer-to-peer certificate distribution (P2PCD), as specified in IEEE 1609.2 [5] and ETSI ITS [3].

2.5.2 Open issues in standards

PQC Migration roadmap: The P2PCD mechanism described in the preceding text depends on the presence of other vehicles in the vicinity. If, on the contrary, there is no vehicle within the communication range or none of the vehicles has the corresponding full certificate, then this scheme fails. In this case, the vehicle needs to wait for the next CAM/BSM message that contains a full certificate, which occurs within the next one second at most.

Although this P2PCD scheme saves channel usage to some extent, it does not sufficiently scale with large public key or signature sizes in the PQC algorithm being used. In this sense, a new solution needs to be designed so that conveying the public key and the signature remains scalable irrespective of their sizes.

2.5.3 Possible solutions, research needs and challenges

Migration to PQC algorithm is a challenge in real-time communication systems, such as V2X due to both the limited radio spectrum allocation, and hard-time-bound processing requirement.[17] In this sense, a novel approach to convey public keys and signatures in V2X communication needs to be designed to ensure

levels that translates to different public key and signature sizes. **Figure 2** compares the impacts of the eight smallest (public key + signature) sizes. Further details are in literature [26].

[164] The constraints on processing capacity/capability are generally applicable to resource-constrained operational environments, such as IoT devices.

that the large increase in public key and signature size has minimal impact on the reduction of the communication capacity. This is possibly a departure from the conventional certificate-based solution; thus, significant research effort is likely required. (→ **Difficulty level:** Very high)

Research challenges to address the open issues raised in the preceding discussion are as follows.

(1) Investigate schemes and solutions for disseminating public keys in periodic messages, such as CAM/VAM/BSM messages, in a scalable manner, independent of the relative size differences between the public key and signature from one signature algorithm to another, while minimizing the impact on communication channel usage. Specific attention should be paid to the RT CPS nature of V2X communication.

(2) Investigate schemes and solutions for certificate formats for both the conventional ECDSA-based and new PQC-based certificates in a manner that is both backward and forward compatible as well as scalable.

One possible approach to the solution is described in literature [27]. To address the transition period, this solution uses a "partially hybrid certificate" scheme, along with the P2PCD mechanism to optimize the frequency of attaching the certificate to CAM/BSM messages. However, this solution has problems in multiple aspects.[18] In this sense, further research effort is required to invent innovative solutions.

2.6 Summary of research needs and challenges

Based on the discussion in the previous sections, we succinctly summarize the key research challenges that require further research: **(1) Open broadcast communication and absence of message confidentiality** – (1.a) How to mitigate various types of attacks, (1.b) Potential use of confidentiality protection; **(2) Certificate management** – (2.a) Inter-V-PKI coordination, (2.b) Effective provisioning and revocation mechanisms; **(3) Pseudonymization policy** – (3.a) Reliable pseudonym change scheme, (3.b) Full coverage of all privacy properties; **(4) VRU integration into the V-PKI system** – (4.a) Integration of non-vehicle devices into the V-PKI system, including verification of non-vehicle devices' legitimacy, (4.b) Misbehavior detection and revocation of non-vehicle devices; **(5) PQC migration strategy** – (5.a) New approach to disseminate public key and signature in a scalable manner independent from the key and signature size.

3. Conclusions

In this section, we described multiple security and privacy-related issues in existing ITS standards. We discussed that the hurdles to launching cyberattacks

[18] Most notably, the P2PCD mechanism assumes the presence of other cooperating "honest" vehicles within one's communication range, which is not always the case (e.g., late night or rural areas where there is no vehicles are present, or the proportion of V2X-capable vehicles is small compared to the total number of vehicles within the range). Furthermore, it opens opportunities for "dishonest" vehicles to send a "bogus" responses to mislead the querying vehicle.

and compromising privacy in V2X communication are low; many of them are even trivial or require only a small effort. At the same time, these attacks have the potential to cause immediate damage to road safety and compromise privacy. Furthermore, we described open issues that originate from architectural oversight in the standards, such as the absence of inter-V-PKI system interaction and the integration of consumer devices into the ITS system. For this reason, closing the gaps in these attacks requires a fundamental reconsideration of how V2X communication is defined. This is far from trivial. Once any of these attacks occur in reality, the ITS system may lose its credibility in the eyes of the general public, and attempts to correct them may become difficult. Furthermore, not establishing a migration roadmap to PQC algorithms will leave V2X vulnerable to future attacks aimed at breaching private keys, thus compromising its integrity. In light of this situation, we believe ITS standards need to address these issues.

Some of these topics have been discussed in the literature in past years, such as various pseudonym change schemes, but the absence of normative standardized solutions means that they are likely left open for implementation, resulting in non-uniform systems. Thus, they require further research and standardization. Due to the nature of an RT CPS system, the ITS system must be secure, resilient, and robust against present and future threats, vulnerabilities, and attacks. Hence, these challenging issues need resolution to make the ITS system effective in real-world implementations and deployments toward the realization of CCAM.

Acknowledgments

This work was supported by the Flemish Government through the Cybersecurity Research Program with grant number VOEWICS02.

Conflict of interest

The author declares no conflict of interest.

Abbreviations

BSM	Basic safety message
CAM	Cooperative awareness message
CCAM	Connected, cooperative, and autonomous mobility
CPS	Cyber–physical system
DENM	De-centralized environmental notification message
DSRC	Dedicated short range communications
ETSI	European Telecommunications Standards Institute
ITS	Intelligent Transport System
PQC	Post-quantum cryptography
TR	Technical report
TS	Technical specification

V2V	Vehicle-to-vehicle
V2X	Vehicle-to-everything
VAM	VRU awareness message
VRU	Vulnerable road user

Author details

Takahito Yoshizawa
COSIC, KU Leuven, Leuven, Belgium

*Address all correspondence to: takahito.yoshizawa@esat.kuleuven.be

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] SAE. V2X Communications Message Set Dictionary 2022-11, [Online] https://www.sae.org/standards/content/j2735_202211/

[2] ETSI TSG ITS Home page. [Online] https://portal.etsi.org/tb.aspx?tbid=702&SubTB=702,707,708,709,710,711#/

[3] ETSI, EN 302 637-2. Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, V1.4.1, 2019–04

[4] ETSI TS 103 300-3. Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) Awareness; Part 3: Specification of VRU Awareness Basic Service; Release 2, V2.2.1, 2023–02

[5] IEEE Intelligent Transportation Systems Committee, Std 1609–2. Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages, 2016

[6] Gurung S, Chauhan S. A novel approach for mitigating gray hole attack in MANET. Wireless Networks. Springer 2018;**24**(2):565–579

[7] ETSI. Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems Operating in The 5 GHz Range; Access Layer Part, TS 102 687, Ver. 1.2.1, Apr. 2018

[8] ETSI. Intelligent Transport Systems (ITS); Facilities layer; Communication Congestion Control; Release 2, TS 103 141, Ver. 2.1.1, Nov. 2021

[9] ETSI. Intelligent Transport Systems (ITS); Congestion Control Mechanisms for The C-V2X PC5 Interface; Access Layer Part, TS 103 574, Ver. 1.1.1, Jan. 2018

[10] ETSI. Intelligent Transport Systems (ITS); Radiocommunications Equipment Operating in The 5855 MHz to 5925 MHz Frequency Band; Harmonised Standard Covering The Essential Requirements of Article 3.2 of Directive 2014/53/EU, EN 302 571, Ver. 2.1.1, Feb. 2017

[11] ETSI. TS 102 940: Intelligent Transport Systems (ITS); Security, ITS Communications Security Architecture and Security Management, v1.3.1, 2018–04

[12] European Commission. "JRC Technical Reports, C-ITS Point of Contact (CPOC) Protocol," Release 1, Jan. 2019

[13] Yoshizawa T, Preneel B. Misbehaviour Reporting in ETSI ITS Standard Considered Broken. In: 2022 IEEE Conference on Standards for Communications and Networking (CSCN). New York, NY: IEEE. 2022. p. 144–150.

[14] Samoshkin A. "SSL Certificate Revocation and How It Is Broken in Practice," [Online] https://medium.com/alexeysamoshkin/how-ssl-certificate-revocation-is-broken-in-practice-af3b63b9cb3, Jan. 2018

[15] Sheffer Y, Lopez D, Gonzalez de Dios O, Pastor Perales A, Fossati T. RFC 8739 Support for Short-Term, Automatically Renewed (STAR) Certificates in the Automated Certificate Management Environment (ACME). IETF; 2020

[16] Pfitzmann A, Hansen M. A Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, 2010. https://www.maroki.de/pub/dphistory/2010_Anon_Terminology_v0.34.pdf

[17] The European Parliament and The Council of The European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council. Official Journal of the European Union. **OJ L119**. 2016;679

[18] Agencia Española Protección Datos (AEPD). 10 Misunderstandings Related to Anonymisation, [Online] https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf, Mar. 2021

[19] ETSI. TR 103 415: Intelligent Transport Systems (ITS); Security; Pre-Standardization Study on Pseudonym Change Management, V1.1.1, 2018–04

[20] Arain QA, Memon I, Deng Z, Memon MH, Mangi FA, Zubedi A. Location monitoring approach: multiple mix-zones with location privacy protection based on traffic flow over road networks. Multimedia Tools and Applications. Springer 2018; 77 (5):5563–5607

[21] Lefevre S, Petit J, Bajcsy R, Laugier C, Kargl F. Impact of V2X Privacy Strategies on Intersection Collision Avoidance Systems. In: 2013 IEEE Vehicular Networking Conference. New York, NY: IEEE; 2013, p. 71–78

[22] Yoshizawa T, Preneel B. Post-Quantum Impacts on V2X Certificates – Already at The End of The Road. In: 2023 IEEE 97th Vehicular Technology Conference (VTC2023-spring). New York, NY: IEEE. 2023. p. 1–6

[23] ETSI. ETSI White Paper No. 8, Quantum Safe Cryptography and Security An introduction, Benefits, Enablers and Challenges, [Online] https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf, 2015

[24] Alagic G, Apon D, Cooper D, Dang Q, Dang T, Kelsey J, Lichtinger J, Liu Y, Miller C, Moody D, Peralta R, Perlner R, Robinson A, Smith-Tone D. Status Report on The Third Round of The NIST Post-Quantum Cryptography Standardization Process, IR 8413-upd1, US Department of Commerce, National Institute of Standards and Technology, 2022

[25] NIST. Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process, [Online] https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf, 2022

[26] Alagic G, Bros M, Ciadoux P, Cooper D, Dang Q, Dang T, Kelsey J, Lichtinger J, Liu Y, Miller C, Moody D, Peralta R, Perlner R, Robinson A, Silberg H, Smith-Tone D, Waller N. Status Report on The First Round of The Additional Digital Signature Schemes for The NIST Post-Quantum Cryptography Standardization Process, IR 8528, US Department of Commerce, National Institute of Standards and Technology, 2024

[27] Twardokus G, Bindel N, Rahbari H, McCarthy S. When Cryptography Needs a Hand: Practical Post-Quantum Authentication for V2V Communications. In: Network and

Distributed System Security Symposium (NDSS 2024), Network and Distributed System Security Symposium (NDSS). 2024

[28] Yoshizawa T, Preneel B. Open Questions in VRU Standards from Security and Privacy Perspectives. In: IEEE Conference on Standards for Communications and Networking (CSCN). New York, NY: IEEE;2023. p. 284–289

Chapter 8

Cybersecurity Risk Management in Cooperative Intelligent Transport Systems

Ramin Ranjbar Motlagh

Abstract

Vehicles have been connected for decades through over-the-air updates, infotainment systems, Wi–Fi, and Bluetooth interfaces. The emergence of cooperative intelligent transport systems (C-ITS) as the next generation of intelligent transport systems (ITS) has greatly expanded this connectivity. C-ITS is a key enabler for autonomous driving, providing real-time coordination between vehicles and infrastructure. By linking vehicles, infrastructure, road users, and cloud platforms through vehicle-to-everything (V2X) communication, C-ITS supports safer, more efficient, and intelligent transport. At the same time, expanded connectivity enlarges the cyberattack surface, exposing safety functions such as braking, steering, and traffic signal control to potential manipulation. This chapter contributes a literature-based conceptual mapping that uses a tri-level perspective to relate vulnerabilities to detection techniques. It pinpoints technical challenges, including false positives, latency, scalability, heterogeneity, and adversarial machine learning, and discusses strategies such as hybrid intrusion detection systems (IDS). To further enhance applicability, it presents methodologies including simulations, hardware-in-the-loop testbeds, and case studies based on C-Roads implementations. It further incorporates cybersecurity asset management and cybersecurity risk assessment as part of the C-ITS ecosystem, consistent with the NIST Cybersecurity Framework (CSF) and ISO/SAE 21434 standard, to enforce regulation and lifecycle-dependent security administration. The chapter also highlights the research challenges, which include asset-agnostic detection, insider and supply-chain threats, adversarial resilience, regulation alignment, and few real-world verifications, and provides a roadmap to further develop IDS research and practice toward C-ITS.

Keywords: cooperative intelligent transport systems (C-ITS), connected and automated vehicles (CAVs), cybersecurity risk management, vehicle-to-everything (V2X), data privacyintrusion detection systems (IDS), C-ITS regulation

1. Introduction

ITS uses electronics, information, and communication technologies to improve the safety, efficiency, and reliability of transportation. These technologies have been

used for many years, evolving through advancements in computing, sensors, and communications. ITS applications rely on systems that collect, process, and share traffic and mobility data, mainly from infrastructure and road sensors, to support drivers in various ways, such as through dynamic signs, and to manage vehicles using physical barriers and traffic lights. They are generally categorized into two main types: vehicle-based ITS, installed within vehicles and encompassing features like advanced driver-assistance systems (ADAS) and safety functions, and infrastructure-based ITS – often simply referred to as ITS – integrated into the road network and including tolling, traffic monitoring, control, and information systems. Together, these two systems, vehicular and infrastructure-based ITS systems, form the foundation of smarter, more-responsive transport networks [1].

ITS and modern vehicles have increasingly depended on an integrated network of sensors, software, electronic control units (ECUs), and communication technologies, including Wi–Fi and Bluetooth. These technologies are integrated into both, vehicles and roadside, infrastructure, facilitating enhanced connectivity and more intelligent decision-making throughout the transportation network. For example, modern vehicles contain more lines of software code than an F-35 fighter jet [2] and can contain up to 150 ECUs [3]. While this technological integration improves mobility performance and user experience, it also introduces new cyber–physical vulnerabilities. The extensive network of interconnected sensors and software modules creates potential entry points for cyberattacks. A notable example is the study by researchers from Keen Security Lab of Tencent [4], who demonstrated a remote cyberattack on a Tesla Model S, successfully taking control of critical functions in both Parking and Driving modes. Such attacks highlight the systemic risks of cybersecurity breaches in connected vehicles (CVs) and, more broadly, across the connected ecosystem, where disruptions can cascade throughout the entire transportation network.

Over the past decade, emerging technologies such as 5G, automated vehicles, and advancements in wireless communication and the Internet of Things (IoT) have significantly propelled the development of more interconnected ITS devices and vehicles. However, this enhanced connectivity has also increased their vulnerability to risks from hackers and cybercriminals. The shift toward enhanced wireless connectivity and the introduction of related services and applications to enable cooperation among road users have laid the foundation for C-ITS, widely recognized as the next evolution of ITS [5]. C-ITS emerged not only as a result of technological progress but also as a foundational enabler for the deployment of automated vehicles [6, 7]. Without vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communication – key elements of C-ITS – autonomous vehicles face considerable challenges in preventing collisions in complex traffic scenarios, such as lane merging, making left turns, or detecting hidden pedestrians, due to their limited sensing range and inability to predict the actions of nearby road users [8].

The term C-ITS, which is predominantly used in this chapter, is most common in European contexts. In contrast, terms like CV and CAVs are more widely used in US-based literature, while intelligent CVs is a term often found in Asian studies. Although C-ITS remains in the early stages of technological maturity and widespread adoption, its global development is steadily gaining momentum. In Europe, the C-Roads platform represents a major multinational initiative, involving multiple pilot deployments of C-ITS services across EU member states [9]. In Australia, several pilot programs have showcased the potential of C-ITS to improve transport

efficiency and road safety. One notable example is the Cooperative and Automated Vehicle Initiative (CAVI), Australia's largest on-road CV trial, which was conducted between 2018 and 2021 [10]. These are just two examples highlighting the growing global interest in C-ITS. As this momentum continues, it becomes increasingly important to prepare for the challenges associated with its development and deployment – particularly cybersecurity and data privacy concerns, which will be explored in detail in the next section of this chapter.

2. C-ITS architecture and the foundations of cybersecurity

Cybersecurity, as defined by the NIST in Special Publication 800–12, is the practice of "preventing damage to, protecting, and restoring computers, electronic communication systems, and the information they contain, to ensure their availability, integrity, authentication, confidentiality, and non-repudiation." In the context of transportation systems, and particularly C-ITS, cybersecurity means protecting the physical and digital assets and communication links that support connected mobility, including roadside infrastructure, in-vehicle electronics, wireless interfaces, and backend control systems. According to the NIST CSF, data privacy – considered within the broader scope of cybersecurity – focuses on an individual's control over when, how, and to what extent their personal information is collected, used, and shared. Together, cybersecurity and data privacy serve as the foundational pillars of trust in C-ITS, where vehicles, infrastructure, and users continuously exchange sensitive information such as location and vehicle ID. Understanding these fundamental concepts is essential for addressing the complex risks posed by V2X communications and enabling secure and resilient C-ITS deployment.

A cyber threat, as defined by NIST SP 800–53, is "any circumstance or event with the potential to adversely impact organizational operations, assets, individuals, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service." A vulnerability, another common term in the cybersecurity context, is a weakness in an information system, security procedures, internal controls, or implementation that could be exploited by a threat source. In practical terms, vulnerabilities represent the points of exposure, while threats are the entities or events that aim to exploit them. This distinction is important in C-ITS environments, where the interconnected nature of vehicles, infrastructure, backend, and cloud-based services expands both the number and type of vulnerabilities. According to recent research [11], the most common vulnerabilities in C-ITS include exposed communication channels, improperly configured access controls, and weak authentication methods – factors which could result in spoofing, message falsification, or Denial-of-Service (DoS) attacks if not addressed. The layered, multi-stakeholder nature and dynamic architecture of C-ITS systems demand a holistic approach to cybersecurity that accounts for these evolving risks.

The cyberattack surface represents all potential entry points in a system where an unauthorized user or attacker could infiltrate, exploiting these vulnerabilities to access data or seize control of system functions. According to NIST, it encompasses all accessible hardware, software, network interfaces, and processes that an adversary might attempt to exploit. In the automotive and C-ITS context, the attack surface has grown substantially over the past decade due to the increasing

digitalization of vehicles, with number of ECUs, connectivity, and software codes. Even before the integration of C-ITS and the interconnection of road users, modern cars already included various entry points such as Bluetooth and Wi-Fi interfaces, infotainment systems, telematics control units, GPS receivers, and remote keyless entry, all of which have proven susceptible to cyberattacks [12]. For instance, researchers have demonstrated successful exploits through infotainment systems to access vehicle Controller Area Network (CAN) buses or through compromised key fobs to unlock and start vehicles remotely [13]. With the emergence of C-ITS, the attack surface expands even further as vehicles are no longer standalone entities; they are now part of a larger ecosystem involving roadside units (RSUs), traffic control centers, cloud platforms, and other CVs. Each added node or communication channel introduces new opportunities for intrusion or disruption, significantly increasing the system's overall complexity and risk.

C-ITS offers a groundbreaking opportunity to develop safer, more efficient, and environmentally sustainable transportation networks [14]. At its core concept, C-ITS enables cooperation between road users, infrastructure, and backend systems through message exchange standardized by the European Telecommunications Standards Institute (ETSI). Two fundamental message types in C-ITS are the Cooperative Awareness Message (CAM) and the Decentralized Environmental Notification Message (DENM). CAMs are periodically broadcast by vehicles to share basic status information, such as location, speed, and heading, and improve situational awareness. DENMs, in contrast, are event-triggered alerts designed to warn nearby road users about specific hazards or unusual conditions, such as roadworks, accidents, or slippery surfaces [15]. ETSI has standardized the CAM and DENM messaging protocols in the European Union (EU), while the Society of Automotive Engineers has defined comparable message structures under the SAE J2735 standard for use in the United States [16].

The communication mechanisms and wireless message exchanges enable a wide range of cooperative applications in the C-ITS ecosystem. For example, Green Light Optimal Speed Advisory (GLOSA) systems help drivers adapt their speed to upcoming traffic signals, minimizing unnecessary stops, enhancing fuel efficiency, and lowering emissions [17]. Blind Spot and Lane Change Warnings alert drivers and vehicles in adjacent lanes, minimizing collision risks as part of vehicular ITS, and can be improved in C-ITS. Basic safety messages (BSMs), particularly used in US C-ITS deployments and similar to CAM, support forward collision warnings and intersection movement assistance. In another critical use case, infrastructure can broadcast approaching emergency vehicle alerts, prompting nearby vehicles to yield appropriately and improving emergency response times.

The cooperation enabled by C-ITS depends entirely on the continuous wireless exchange of data between vehicles, infrastructure, and other road users. This real-time communication, using standardized messages such as CAM and DENM, allows road users to share their status, perceptions, and collaboratively address hazards. As demonstrated by pilot projects in Europe, North America, and Australia, the growing adoption of C-ITS shows its strong potential to improve safety, reduce congestion, and support cleaner mobility. C-ITS aims to address the challenges of urbanization, particularly by supporting UN Sustainable Development Goals (SDG 7 and SDG 9) to enhance energy efficiency and develop reliable, sustainable infrastructure.

C-ITS communications have evolved based on two distinct wireless technologies: Dedicated short-range communications (DSRC) and cellular vehicle-to-everything

DOI: http://dx.doi.org/10.5772/intechopen.1014246

(C–V2X). DSRC, standardized by IEEE 802.11p and supported by SAE J2735, operates in the 5.9 GHz band and enables direct, low-latency communication between vehicles and infrastructure without relying on cellular networks. Meanwhile, C–V2X, developed by the Third Generation Partnership Project (3GPP) and standardized under 3GPP Release 14 and beyond, leverages cellular networks – especially 4G LTE and 5G NR – to provide broader coverage, higher reliability, and greater scalability. While some regions, like the United States, have begun transitioning toward C–V2X to align with the broader industry shift to 5G, DSRC has not been phased out entirely and is still active in several deployments, especially in Europe and parts of Asia [18, 19].

Both DSRC and C–V2X wireless communication technologies support various modes of interaction: V2V enables real-time exchange of data between cars for safety applications like collision avoidance; V2I connects bidirectional vehicles to RSUs for services like traffic signal priority and speed advisory; vehicle-to-pedestrian (V2P) warns about vulnerable road users, such as pedestrians and cyclists; and V2X represents the unified ecosystem of all these interactions. Together, these technologies create a connected ecosystem where road users and infrastructure cooperate to enhance mobility, safety, and environmental performance [18].

However, this interconnectivity in the core concept of C-ITS also introduces cyberattacks as a risk. Unlike traditional ITS, where digital systems were more isolated, C-ITS relies on persistent, real-time communication between a wide array of dynamic and distributed actors. Each communication interface adds new network entry points that can be exploited by malicious actors or simply expand the cyberattack surface. These interconnected entities may propagate threats across vehicles, infrastructure, cloud services, or pedestrian devices. As the number of connected nodes increases and the cyberattack surface expands, it makes robust, multi-layered cybersecurity not just a requirement but a core design principle for secure and resilient C-ITS deployments.

Cybersecurity risk, as defined by ISO/SAE 21434, is "the potential that a threat exploits one or more vulnerabilities, leading to negative impacts on the road user or other stakeholders." This definition places emphasis on understanding how threats, vulnerabilities, and impacts interact within the context of a vehicle's entire lifecycle. Developed jointly by the ISO and SAE, the ISO/SAE 21434:2021 standard provides a comprehensive framework for cybersecurity engineering in road vehicles. It covers everything from the concept phase, risk assessment, cybersecurity goals, technical implementation, and validation, through to maintenance and end-of-life decommissioning [20, 21].

ISO/SAE 21434 utilizes a risk-based approach, integrating processes such as item definition, threat analysis, and risk assessment (TARA), goal setting, requirements traceability, and cybersecurity validation. As highlighted in the study by Zhou et al. [21], this standard focuses primarily on the vehicle domain, covering internal systems, ECUs, software, and communication interfaces – including those that support V2X capabilities in C-ITS. While the broader C-ITS ecosystem also involves infrastructure and cloud services, the standard ensures that vehicles themselves are cyber-resilient and prepared to interact securely within that larger environment.

Effective cybersecurity starts with a clear understanding of what needs to be protected. The next section will examine C-ITS asset management, identifying critical physical, digital, and human assets, and assessing their exposure to cyber threats within this evolving landscape.

3. Cybersecurity asset management in C-ITS

The NIST CSF 2.0 offers a structured approach to addressing cyber risks through six core functions: Identify, Protect, Detect, Respond, Recover, and Govern. Among these, the Identify function is foundational. It focuses on developing an accurate understanding of organizational assets, business context, and resources, which is essential for prioritizing cybersecurity efforts.

Within the Identify function, the Asset Management category plays a key role. It ensures that all components – systems, devices, data, software, communication channels, and people – are properly taken into consideration and managed. In the C-ITS ecosystem, where vehicles, infrastructure, cloud platforms, and road users interact in real time, asset management becomes both critical and complex. Assets span physical elements such as sensors and RSUs; digital assets like V2X messages and traffic logs; software and firmware used in control systems; communication interfaces and links; external service providers; and human actors, including drivers, technicians, and traffic operators. Proper classification and mapping of these assets are essential not only for understanding exposure to cyber threats but also for designing effective, layered protection strategies. The following paragraphs will explore each asset category in detail, beginning with physical assets, and discuss their roles, vulnerabilities, and examples relevant to C-ITS.

Physical assets form the most tangible layer of cybersecurity asset management in C-ITS and are typically divided into two main categories: vehicular assets and infrastructure-based assets. Vehicular assets include on-board perception sensors such as LiDAR, radar, ultrasonic sensors, cameras, Global Navigation Satellite System (GNSS) receivers, Infrared (IR) sensors, and Inertial Measurement Units (IMUs). These sensors act as the "eyes and ears" of vehicles, providing real-time environmental and situational awareness and supporting vital functions like obstacle detection, path planning, connectivity, and navigation. Additional in-vehicle components include the On-Board Unit (OBU) dedicated to C-ITS signaling, ECUs, infotainment systems, and the On-Board Diagnostic (OBD) port – play critical roles in vehicle control, data processing, and diagnostics. **Figure 1** illustrates the cyber–physical layout and example components. As CAVs, and in a broader aspect, vehicles become more

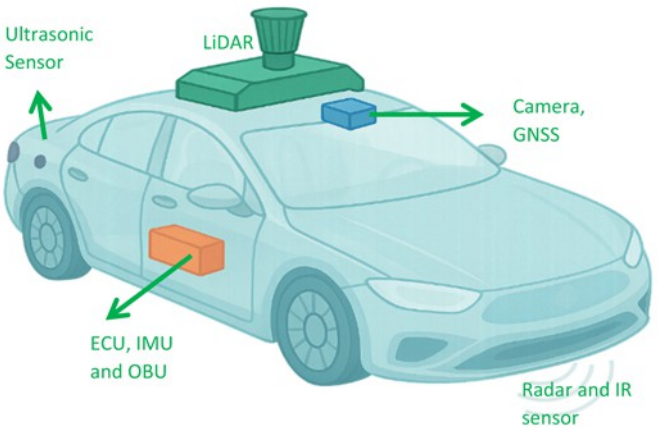


Figure 1.
Cyber–physical layout of a CAV.

connected, these devices are increasingly attractive targets for physical tampering and cyber intrusion, particularly through access points like the OBD port or unsecured wireless interfaces [11, 22].

On the infrastructure side, physical assets include RSUs, traffic controllers, backend servers, roadside Bluetooth detectors, and increasingly, fog nodes, edge servers, and racks. These components extend the C-ITS functionality beyond the vehicle, enabling V2I and V2X communication, cooperative awareness messaging, and system-wide coordination. However, they are also exposed to environmental vulnerabilities, unauthorized physical access, and legacy system weaknesses [23, 24] Given the distributed and interconnected nature of these assets, effective cybersecurity asset management demands a detailed inventory and risk mapping of all physical elements in both the vehicle and infrastructure domains. Their interdependence underscores the importance of implementing tamper detection, access control, and secure hardware protocols across the entire ecosystem.

Digital assets and data represent another vital layer of cybersecurity asset management in C-ITS. These assets include structured information and configurations that support the operation, coordination, and decision-making of connected mobility systems. Key examples of digital assets are logs, system configurations, map databases, V2X messages (e.g., BSM, CAM, DENM), Signal Phase and Timing (SPaT) data, and cryptographic credentials. In vehicular systems, these digital elements are processed and stored inside the OBUs, ECUs, and infotainment platforms, forming the basis for route planning, event recognition, and system diagnostics. For instance, compromised audit logs or tampered navigation databases can mislead automated decision-making, causing safety risks [25]. On the infrastructure side, backend servers, edge processors, and RSUs depend on trustworthy data from vehicles to optimize traffic signals and broadcast SPaT or MAP messages. However, falsified V2X messages – such as spoofed CAMs or DENMs – can disrupt intersection mobility operations and cooperation between road users or trigger false hazard alerts, as shown in studies of data spoofing attacks on traffic signal control systems [25].

The authenticity and integrity of these digital assets are critical in the C-ITS ecosystem. Cryptographic keys and digital certificates ensure secure and authenticated data exchange across the network, particularly in C–V2X and DSRC links. Similarly, over-the-air (OTA) updates, which transmit software and firmware packages to vehicles, must be tightly secured to prevent unauthorized modifications that could compromise vehicle functions and broader system stability [26].

Software and firmware play a key role in the functionality, safety, and user interaction within C-ITS-enabled and CVs and infrastructure systems. These assets include human–machine interface (HMI) software for driver alerts and displays, mobile applications interacting with the vehicle, and core modules such as autonomous driving decision software, path-planning algorithms, and vehicle control systems. On the firmware side, sensor-level firmware (e.g., for LiDAR and GNSS sensors), ECU firmware, and boot-level systems such as BIOS and bootloaders create the backbone of operational logic and system integrity [27].

Firmware and application software used in Traffic Management Centers (TMCs) and ITS operations management platforms play a vital role in handling V2X communications and synchronizing traffic signal operations. The complexity of these firmware modules – particularly in infotainment and control systems – demands robust validation and continuous update mechanisms. Similarly, certain

researchers highlight the need to incorporate software redundancy and multi-layered security in CAV systems to counter growing and evolving threats [28]. Proper inventory and management of these assets, including version control, secure update protocols, and traceability, are essential for reducing system-level cybersecurity risks across the C-ITS ecosystem.

Third-party assets are external services and content providers that play an increasingly critical role in the operation of C-ITS environments. These include SatNav data providers offering real-time traffic and routing information, cloud and telecom platforms such as Amazon Web Services (AWS) and Microsoft Azure that host vehicle data and analytics platforms, and infotainment and media content providers integrated into vehicle systems. For example, navigation apps like TomTom supply dynamic maps and routing, while cloud services enable OTA updates and data processing at scale. Infotainment platforms may deliver music streaming, voice assistants, or in-vehicle app ecosystems. Reliance on third-party providers introduces new dependencies and trust boundaries, making it essential to consider their security, data handling policies, and service availability in overall cybersecurity planning [29].

Human assets are another component of cybersecurity asset management in C-ITS, though often underestimated, including a wide range of individuals such as drivers and passengers who may interact with in-vehicle systems, maintenance personnel, and system operators [30]. These include mechanics and calibration experts who service vehicles, traffic operators managing roadside infrastructure, and cybersecurity or IT staff working in TMCs and Original Equipment Manufacturer backends. Each role introduces potential cybersecurity risks, whether through accidental misconfigurations, social engineering, or lack of adequate training. For instance, improperly calibrated sensors by maintenance teams may impair perception systems, while traffic control personnel may unknowingly grant access to attackers through phishing schemes. As recent research shows, human factors continue to be a significant vulnerability in connected transport systems, underscoring the need for structured training programs, strict access controls, and continuous awareness across all personnel.

In addition to cataloging asset types, this chapter offers a systematic approach to enhancing IDS for the C-ITS environment. While most current work groups IDS based on technique – for example, signature, anomaly, or hybrid – they do not explicitly associate methods with specific assets to be guarded. Based on the current mapping of assets in this chapter, a conceptual multi-layer perspective can be outlined. Physical assets such as sensors and RSUs, for instance, may be covered under anomaly detection, digital and programmatic assets may employ cryptographic integrity checks, and third-party and human assets may fall under trust and access control monitoring. This mapping indicates areas of research to be done; for instance, there has been a lack of focus on insider misuse or supply-chain tampering. It is proposed that IDS methods should be adaptive and specific to the asset, rather than purely conceptual. By correlating IDS design to asset types, researchers and practitioners may bring themselves that much closer to tried-and-tested administration that enhances intellectual understanding as well as real-world applicability.

In summary, effective cybersecurity asset management in C-ITS requires a comprehensive understanding of the diverse components that make up the ecosystem – ranging from physical sensors and software systems to digital data,

third-party services, and human actors. Each asset category introduces unique operational roles and potential exposure points, underscoring the importance of accurate classification, secure lifecycle management, and cross-domain coordination. As this foundational mapping is now complete, the next section will explore the specific vulnerabilities associated with each asset type, highlighting the cybersecurity threats and risks they face in real-world C-ITS environments.

4. Risk assessment and vulnerability management in C-ITS

Risk assessment, a category within the Identify function of NIST CSF 2.0, focuses on evaluating the likelihood and impact of cybersecurity events. In C-ITS, this involves identifying weak points across vehicles, infrastructure, and networks. Key activities include vulnerability identification, threat intelligence, and risk analysis. Supporting elements such as inherent risk estimation, response planning, change management, authenticity checks, disclosure processes, and supplier assessment help ensure a proactive, context-driven approach to managing evolving cyber risks. The ISO/SAE 21434 standard supports this effort by defining a structured process to embed cybersecurity across the full vehicle lifecycle – from design and engineering to testing, operation, and maintenance – making it one of the most comprehensive frameworks for CV security [31].

In the context of C-ITS, vulnerabilities exist across all asset categories and types, as discussed in Section 3. For example, physical assets such as cameras and LiDAR sensors can be misled through spoofing or jamming, while unsecured OBUs and infotainment systems may be exploited via privilege escalation or open communication ports. Digital assets, including logs and map updates, are susceptible to false data injection and insider misconfiguration, potentially compromising automated decision-making. Software and firmware within ECUs and TMCs may be targeted by malicious code injection or supply chain attacks, while communication interfaces like Bluetooth and DSRC face threats such as eavesdropping, Sybil attacks, and location tracking exploits. Even third-party services can introduce risks, for example, through tampered map updates or compromised cloud infrastructure, and human assets remain vulnerable to social engineering, phishing, and malicious insider activity [11].

These vulnerabilities create opportunities for real-world threats that could compromise safety, disrupt traffic operations, or erode public trust in connected mobility systems if left unmitigated. The following sections will examine each asset category in detail, outlining the most critical cybersecurity threats and related risk management strategies within the C-ITS ecosystem.

In order to step beyond general descriptions of vulnerability, this chapter suggests correlating vulnerabilities directly to IDS design in C-ITS. Rather than addressing risks narrowly by category, vulnerabilities can be conceptually organized into three layers of detection. The perception layer addresses sensors, OBUs, and ECUs, upon which spoofing, jamming, or replay attacks can be detected based on anomaly-oriented IDS. The communication layer comprises V2X channels, logs, and digital data, which can contain falsification of messages or manipulation from inside, based on cryptographic verification and behavior-oriented IDS. Lastly, the application level encompasses third-party services and human assets, upon which trust administration and monitoring of access control are necessary. This tri-level

perspective highlights areas in which IDS methods are underexplored – for example, insider misuse or supply-chain compromise – and clarifies a direction toward adaptive, asset-specific detection. By stepping vulnerability research in sync with vulnerability category, research can shift from conceptual surveys to realistic frameworks, which build resilience throughout the complete C-ITS ecosystem.

Figure 2 illustrates the cyber–physical vulnerabilities associated with each attack surface shown in **Figure 1**, highlighting example weaknesses in CAV sensors and internal components.

Physical assets in C-ITS – such as perception sensors, OBUs, ECUs, and RSUs – are highly exposed to a range of cyber–physical threats due to their accessibility and crucial role in system operation. Sensors are susceptible to blinding attacks, jamming, spoofing, and adversarial inputs, which can misrepresent environmental perception and mislead path planning algorithms [22]. For instance, a blinding attack on a front-facing camera or targeted LiDAR spoofing can create false objects or hide real ones, potentially leading to unsafe maneuvers [23]. GNSS receivers and IMUs are also vulnerable to replay attacks, where previously captured valid data is maliciously retransmitted to confuse vehicle localization [11]. Additionally, OBUs and ECUs may be targeted through privilege escalation, malware injection, or supply chain compromise, enabling remote takeover of critical functions [22].

In-vehicle systems often lack encryption in internal communication buses, and open diagnostic ports (OBD-II) can serve as physical entry points for potential attackers. Many ECUs and controllers still operate with weak or default credentials, increasing susceptibility to unauthorized physical tampering [11]. On the infrastructure side, RSUs and traffic controllers are often deployed in exposed roadside environments and may lack adequate physical protection or tamper detection, leaving them open to port access attacks or manipulation via legacy interface vulnerabilities [24]. These threat vectors highlight the need for robust access control, sensor fusion with redundancy checks, and secure firmware validation across both vehicle and infrastructure components.

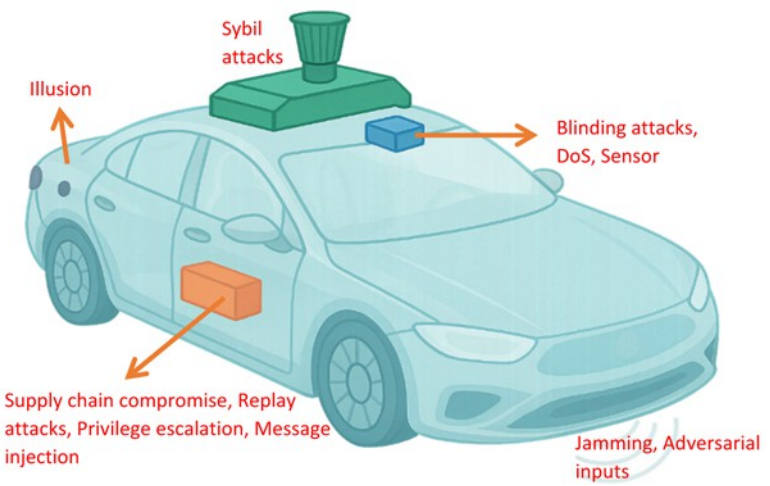


Figure 2.
Cyber-physical vulnerabilities in CAV sensors and components.

Digital assets and data in C-ITS are increasingly targeted through a range of attack methods. One common vulnerability is the exposure of unencrypted or plaintext log files, which can be exploited for unauthorized system monitoring or manipulation [26, 32]. Additionally, unverified map updates present a threat pathway, as attackers may introduce tampered navigation data that misdirects vehicles or disrupts routing decisions [11]. Abnormal message injection attacks, such as falsified CAMs or DENMs, can trigger false alarms or alter intersection behavior, as demonstrated in recent simulations of traffic signal control systems [33]. Insider threats, including misconfiguration or false data injection, pose a particularly insidious risk by compromising the integrity of V2X data from within legitimate systems. Poor key management practices, such as insider key leakage or improper storage of cryptographic credentials, can undermine secure communication and authentication across the network. These threats highlight the critical need for robust validation, secure logging, and strict access controls to safeguard the digital foundation of C-ITS.

Software vulnerabilities in C-ITS introduce serious risks to both vehicles and infrastructure domains. Insecure communication channels can enable remote control of ECUs, especially when authentication mechanisms are weak or absent. Firmware tampering during OTA updates or through compromised supply chains can inject persistent malicious code into infotainment or control systems. Additionally, poor isolation between critical software modules increases the likelihood of cascading failures or privilege escalation. These threats are amplified in autonomous systems, where flawed decision-making logic or insufficient software validation may lead to unsafe driving behavior under adversarial conditions [34]. Backend systems, such as traffic management platforms, are also exposed to unauthorized remote access, which may lead to platform-wide compromise through code injection or control override [27].

Third-party providers and supply chains introduce unique cybersecurity risks into the C-ITS ecosystem. For instance, tampered map updates from navigation service providers may mislead routing systems, resulting in traffic inefficiencies or safety hazards. Similarly, if a cloud platform such as AWS or Azure is compromised, attackers could gain access to sensitive vehicle telemetry, location history, or OTA update mechanisms. Infotainment systems sourced from external vendors may carry vulnerabilities or embedded malware, creating an attack surface that extends into the vehicle's core network. Additionally, the integration of external APIs and SDKs – often with limited vetting – can expose systems to unauthorized data access or manipulation. As noted by researchers, compromised third-party components or updates may bypass in-vehicle security layers and serve as vectors for data exfiltration, remote code execution, or service disruption across the fleet [26].

Human actors can inadvertently or deliberately introduce cybersecurity risks into the C-ITS ecosystem. While social engineering remains one of the most common vectors – such as phishing emails that compromise operator credentials – more sophisticated threats have historically exploited trusted insiders or human error. A prominent example is the Stuxnet attack, where malicious code was introduced into isolated critical systems through infected USB devices handled by unwitting personnel, bypassing network-based security entirely. Similar risks exist in C-ITS environments, where maintenance technicians, OEM staff, or contractors with physical or administrative access might unknowingly facilitate the injection of malware or backdoors into vehicle systems or infrastructure platforms.

Human-centric threats – such as lack of security awareness, poor access control enforcement, or malicious insiders – remain persistent vulnerabilities. These risks underline the importance of integrating cyber hygiene training, role-based access control, and insider threat detection programs into broader C-ITS security strategies [30].

While IDS solutions for C-ITS are maturing, it is still highly difficult to have a fully autonomous IDS due to various technical challenges. One of the main challenges is the high level of false positives that occur in dynamic traffic scenarios, in which natural fluctuations of driver or sensor activity are inaccurately classified as attacks. Latency and scalability form another challenge: the IDS needs to handle massive amounts of V2X data in real time, oftentimes under tight milliseconds, which is challenging for resource-limited ECUs and RSUs. Asset heterogeneity makes detection even more difficult, as vehicles, RSUs, and cloud services deploy various communication protocols and software stacks. Adversarial attacks against machine learning can also tamper with detection models, further diminishing confidence in AI-driven IDS. To overcome these challenges, researchers investigate hybrid IDS architectures that blend anomaly detection and rule checks, distributed learning to train models across distributed systems and avoid centralizing sensitive information, and edge–cloud cooperation to balance real-time detection against deeper offline analysis. These approaches, although not yet proven conclusive, provide insight toward deployable, scalable IDS architectures capable of enabling the secure deployment of C-ITS.

To bring these challenges and tactics to real-world outcomes, adopting concrete methods to evaluate IDS in C-ITS has merit. One approach to this end is to utilize simulation environments like Veins, Simulation of Urban Mobility (SUMO), or OMNeT++, which enable researchers to scale V2X environments to large sizes and evaluate IDS effectiveness under controlled attack modes like spoofing or jamming. Another approach involves hardware-in-the-loop or testbed experiments, in which OBUs, RSUs, and ECUs are interfaced with real communication links, allowing researchers to validate latency, false positive rates, and resilience to hostile conditions. Furthermore, case studies based on pilot projects – for example, the C-Roads deployments throughout Europe or the CAVI trial in Australia – yield important lessons about how to deploy IDS inside current traffic authority systems. Lastly, hybrid methods that bring simulations and minimal real-world deployment together are able to strike a balance between scale and realism and deliver both quantification of the performance data and real-world insights. Together, these methods move IDS research from concept to practice in real-world C-ITS deployments.

Despite the advances described, there are some outstanding research areas for building efficient IDS for C-ITS. First, prior approaches are predominantly asset-agnostic and adopt generic detection schemes that are not specialized to the individual characteristics of physical sensors, digital information, or human users. Second, there has been little work on handling insider threats and supply-chain compromise, which are both high-footprint and recurrent threats but are lower priorities when designing IDS. Third, although machine learning–oriented IDS approaches are encouraging, they are still susceptible to adversarial inputs and are not extensively validated in real-world V2X scenarios. Fourth, scaling and latency issues when deploying on a large scale are not well studied, especially in resource-limited roadside and in-vehicle systems. Lastly, few have moved from simulation to pilots or cross-domain testbeds, so real-world application remains uncertain. This

chapter highlights key gaps and offers a roadmap for research on adaptive detection, resilience, and real-world validation.

In summary, the diverse asset categories within C-ITS – ranging from physical sensors and software systems to third-party services and human operators – introduce a wide array of vulnerabilities that adversaries can exploit. Each asset type requires tailored threat modeling and mitigation strategies to reduce systemic risk. By adopting structured risk assessment frameworks such as NIST CSF and ISO/SAE 21434, and implementing proactive measures like encryption, secure updates, access control, and cyber awareness training, stakeholders can build a more resilient C-ITS ecosystem prepared for evolving cyber threats.

5. Conclusion

As C-ITS evolve toward greater connectivity, automation, and reliance on digital infrastructure, cybersecurity has become a foundational pillar of system safety, reliability, and public trust. This chapter explores the landscape of cybersecurity asset management within C-ITS, structured around the NIST CSF and enriched by insights from ISO/SAE 21434 and related literature. By categorizing assets into six groups, including physical assets, digital assets and data, software and firmware, communication interfaces, third-party assets, and human assets, the chapter provides a clear understanding of where and how cybersecurity risks arise in C-ITS environments.

One of the key insights is that each asset group presents unique vulnerabilities and threats. Physical components like LiDAR, cameras, and OBUs are exposed to sensor spoofing, jamming, and tampering, often through physical access points or wireless interfaces. Digital assets, including map databases, system logs, and V2X messages, are at risk of manipulation through false data injection, misconfiguration, and insider threats. Software and firmware vulnerabilities extend this risk by introducing pathways for remote control, DoS attacks, and supply chain compromises, especially in the context of OTA updates and third-party integrations.

Moreover, the inclusion of third-party providers – such as cloud platforms and infotainment services – expands the attack surface beyond the direct control of C-ITS stakeholders. These dependencies demand stronger verification, encryption, and access control to ensure that external services do not become entry points for malicious actors. On the contrary, human assets such as drivers, maintenance personnel, and backend operators continue to represent persistent risk vectors, whether through social engineering, inadequate training, or insider sabotage. High-profile examples like Stuxnet highlight how human actions – intentional or not – can bridge otherwise air-gapped systems, introducing severe cybersecurity consequences.

This chapter also underscores the importance of proactive risk assessment and vulnerability management practices tailored to the complex, dynamic nature of C-ITS. The application of the NIST CSF's Identify function, particularly its Risk Assessment category, provides a structured foundation for evaluating cybersecurity threats based on impact and likelihood. Complementing this, the ISO/SAE 21434 standard emphasizes the importance of lifecycle-based security management, ensuring that cybersecurity is integrated from the earliest design stages through operation and decommissioning.

Looking ahead, several strategic priorities emerge for improving cybersecurity in C-ITS deployments. First, a shift toward real-time, adaptive risk management

systems is essential to respond to the evolving nature of cyber threats in connected environments. Second, cross-sector collaboration – including between transport authorities, OEMs, cybersecurity experts, and cloud service providers – is critical to ensure end-to-end protection across the C-ITS ecosystem. Third, human factors must be more deeply integrated into cybersecurity planning, not only through awareness training but also through access control, role separation, and accountability frameworks.

This chapter offers a literature-based conceptual mapping relating assets to IDS approaches and uses a tri-level perspective to conceptually link vulnerabilities to detection techniques. It further frames vulnerabilities using a tri-level perspective – perception, communication, and application – to guide the discussion of detection techniques. By framing IDS in terms of asset management, the chapter moves beyond description toward a synthesized perspective intended to guide researchers and practitioners.

Finally, the chapter outlines important technical challenges like false positives, latency, scalability, heterogeneity, and adversarial machine learning, and describes tactics like hybrid IDS, federated learning, and edge–cloud cooperation. To further enhance applicability, it suggests specific methodologies like simulations using SUMO and Veins, hardware-in-the-loop testbeds, and case studies from C-Roads implementations. Lastly, it outlines important research gaps – asset-agnostic detection, insider and supply-chain threats, adversarial resilience, and limited real-world validation – as areas of focus for follow-up work. Collectively, these additions highlight the chapter's novelty, extend its analysis, and chart a course for furthering IDS research and practice in C-ITS.

Acknowledgments

This research was supported by an Australian Government Research Training Program (RTP) Scholarship [DOI: https://doi.org/10.82133/C42F-K220]

The author acknowledges the responsible use of Artificial Intelligence (AI) tools, such as Grammarly, to support the editing process, assist in summarizing relevant articles, and refine the clarity and coherence of the text. All source materials were reviewed manually to ensure the accuracy, reliability, and scholarly integrity of the chapter.

Author details

Ramin Ranjbar Motlagh
Victoria University, Melbourne, Australia

*Address all correspondence to: ramin.ranjbarmotlagh@live.vu.edu.au

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] Lu M. Cooperative Intelligent Transport Systems: Towards High-Level Automated Driving. London, UK: The Institution of Engineering and Technology (IET); 2019

[2] King WA. A Quantitative Analysis of Autonomous Vehicle Cybersecurity as A Component of Trust. Maryland, USA: D.Sc., Capitol Technology University; 2022

[3] Grimm D, Stang M, Sax E. Context-Aware security for vehicles and fleets: A survey. IEEE Access. 2021;**9**: 101809–101846

[4] Nie S, Liu L, Du Y. Free-Fall: Hacking tesla from wireless to can bus. Briefing. 2017;**25**(1):16

[5] Emami A, Sarvi M, Bagloee SA. Network-wide traffic state estimation and rolling horizon-based signal control optimization in a connected vehicle environment. IEEE Transactions on Intelligent Transportation Systems. 2022;**23** (6):5840–5858

[6] Djahel S, Doolan R, Muntean GM, Murphy J. A communications-oriented perspective on traffic management systems for smart cities: Challenges and innovative approaches. IEEE Communications Surveys and Tutorials. 2015;**17**(1):125–151

[7] Hepner E, Zhao C, Seipel K, Hoyer R; IEEE. Optimization of the Traffic Flow in Public Transport through C-Its. In: 7th International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS); IEEE; 2021

[8] Shetty A, Yu MQ, Kurzhanskiy A, Grembek O, Tavafoghi H, Varaiya P. Safety challenges for autonomous vehicles in the absence of connectivity. Transportation Research Part C-Emerging Technologies. 2021;**128**:20

[9] Kotsi A, Mitsakis E. Large scale deployment of C-Its: Impact assessment results of the C-Roads Greece pilots. arXiv Preprint. 2023;arXiv:2311.10734

[10] Rodwell D, Ho B, Pascale MT, Elrose F, Neary A, Lewis I. In their own words: A qualitative study of users' acceptance of connected vehicle technology after nine months of experience with the technology. Transportation Research Part F: Traffic Psychology and Behaviour. 2023;**97**:73–93

[11] Abdo A, Chen H, Zhao X, Wu G, Feng Y. Cybersecurity on connected and automated transportation systems: A survey. IEEE Transactions on Intelligent Vehicles. 2024;**9**(1):1382–1401

[12] Eiza MH, Ni Q. Driving with sharks rethinking connected vehicles with vehicle cybersecurity. IEEE Vehicular Technology Magazine. 2017;**12**(2):45–51

[13] Petit J, Shladover SE. Potential cyberattacks on automated vehicles. IEEE Transactions on Intelligent Transportation Systems. 2015;**16** (2):546–556

[14] Soto I, Calderon M, Amador O, Urueña M. A survey on road safety and traffic efficiency vehicular applications based on C-V2x technologies. Vehicular Communications. 2022;**33**:100428

[15] Botte M, Pariota L, D'Acierno L, Bifulco GN. An overview of cooperative driving in the European Union: Policies and practices. Electronics. 2019;**8**(6):25

[16] Weinbauer K, Renzler T, Stolz M, Watzenig D; IEEE . Taking standardized C-Its communication to the next level - Lightweight and extensible vehicle-to-everything library. In: IEEE Wireless Communications and Networking Conference (WCNC); IEEE; 2023

[17] Bhattacharyya K, Laharotte PA, Burianne A, El Faouzi NE. Assessing connected vehicle's response to green light optimal speed advisory from field operational test and scaling up. IEEE Transactions on Intelligent Transportation Systems. 2023;**24**(6):6725–6736

[18] Raza N, Jabbar S, Han J, Han K, Assoc Comp M. Social Vehicle-to-Everything (V2x) communication model for intelligent transportation systems based on 5g scenario; In: 2nd International Conference on Future Networks and Distributed Systems (ICFNDS); Assoc Computing Machinery; 2018

[19] Pham M, Xiong KQ. A survey on security attacks and defense techniques for connected and autonomous vehicles. Computers & Security. 2021;**109**:29

[20] Jayaratne DND, Kamtam SH, Shaikh SA, Ramli MA, Lu Q, Mepparambath RM, Nguyen HN, Rakib A. A simulation framework for automotive cybersecurity risk assessment. Simulation Modelling Practice and Theory. 2024;**136**:16

[21] Zhou Z, Zhi Q, Tao L, Ping P, Long Q. Odfa2: Overall defense framework against cyber-attacks on intelligent connected vehicles. IEEE Transactions on Vehicular Technology. 2024;**73**(5):6318–6331

[22] Ahmad J, Zia MU, Naqvi IH, Chattha JN, Butt FA, Huang T, Xiang W. Machine Learning and Blockchain Technologies for cybersecurity in connected vehicles. WIREs Data Mining and Knowledge Discovery. 2024;**14**(1):39

[23] Chowdhury A, Karmakar G, Kamruzzaman J, Jolfaei A, Das R. Attacks on self-driving cars and their countermeasures: A survey. IEEE Access. 2020;**8**:207308–207342

[24] Yang TS, Sun RK, Rathore RS, Baig I. Enhancing cybersecurity and privacy protection for cloud computing-assisted vehicular network of autonomous electric vehicles: Applications of machine learning. World Electric Vehicle Journal. 2025;**16**(1):32

[25] Feng YH, Huang SHE, Wong W, Chen QA, Mao ZM, Liu HX. On the cybersecurity of traffic signal control system with connected vehicles. IEEE Transactions on Intelligent Transportation Systems. 2022;**23**(9):16267–16279

[26] Kidmose B. A review of smart vehicles in smart cities: Dangers, impacts, and the threat landscape. Vehicular Communications. 2025;**51**:66

[27] Costantino G, De Vincenzi M, Matteucci I. A vehicle firmware security vulnerability: An Ivi exploitation. Journal of Computer Virology and Hacking Techniques. 2024;**20**(4):681–696

[28] Suo DJ, Moore J, Boesch M, Post K, Sarma SE. Location-Based schemes for mitigating cyber threats on connected and automated vehicles: A survey and

design framework. IEEE Transactions on Intelligent Transportation Systems. 2022;**23**(4):2919–2937

[29] Salek MS, Khan SM, Rahman M, Deng HW, Islam M, Khan Z, Chowdhury M, Shue M. A review on cybersecurity of cloud computing for supporting connected vehicle applications. IEEE Internet of Things Journal. 2022;**9**(11):8250–8268

[30] Ahn H, Choi J, Kim YH. A mathematical modeling of stuxnet-style autonomous vehicle malware. IEEE Transactions on Intelligent Transportation Systems. 2023;**24**(1):673–683

[31] Sharma P, Gillanders J. Cybersecurity and Forensics in Connected Autonomous Vehicles: A Review of the State-of-the-Art. **10**. Piscataway, NJ, USA: IEEE Access; 2022. p. 108979–108996

[32] Khan SK, Shiwakoti N, Stasinopoulos P, Warren M. Modelling cybersecurity regulations for automated vehicles. Accident Analysis and Prevention. 2023;**186**:15

[33] Vargas P, Tien I. Methodology to quantitatively assess impacts of 5g telecommunications cybersecurity risk scenarios on dependent connected urban transportation systems. Asce-Asme Journal of Risk and Uncertainty in Engineering Systems Part a-Civil Engineering. 2022;**8**(2):15

[34] Panda S, Rass S, Moschoyiannis S, Liang K, Loukas G, Panaousis E. Honeycar: A Framework to Configure Honeypot Vulnerabilities on the Internet of Vehicles. **10**. Piscataway, NJ, USA: IEEE Access; 2022. p. 104671–104685

Chapter 9

The Road to Autonomous Vehicular Security: From Manual Updates to Lifetime Defenses Driven by Intelligent Agents

Yunfan Huang

Abstract

The rise of Cooperative, Connected, and Autonomous Mobility (CCAM) holds promise to redesign current transport architectures, and Vehicular Ad-hoc Networks (VANETs) are a fundamental component of this underlying communication architecture. Nevertheless, this induced increased interconnectivity breeds a dynamic and expansive attack surface that renders traditional IDS insufficient to counter new emerging threats owing to inherent drawbacks such as catastrophic forgetting. The current chapter provides an all-encompassing account of the development of lifetime learning-based intrusion detection systems (LL-IDS), highlighting their important role in securing this new transport epoch. The review traces the evolution from simple human-in-the-loop prototypes, which require manual intervention by domain experts to acquire knowledge, to semi-autonomous architectures that utilize semi-supervised training approaches to reduce dependence on data labels, and finally to systems that cooperate using privacy-preserving methods within Federated Learning frameworks to build robust, generalized patterns that are resilient to adverse events like data poisoning attacks. The paper further identifies potential directions for future work by speculating on using large language models (LLMs) as reasoning engines to thereby realize a truly autonomous, zero-intervention, and self-adapting security construct, while at the same time overcoming important research hurdles. The central hypothesis holds that such ongoing progression to progressively smarter, flexible, and eventually autonomous security devices represents an important step toward achieving the CCAM ecosystem's maximum safety and efficiency potential.

Keywords: vehicular security, vehicular ad-hoc network (VANET), lifetime learning, incremental learning, semi-supervised learning, connected and autonomous vehicles (CAVs), large language models (LLMs), intelligent transportation systems (ITS)

1. Introduction

1.1 The vision of cooperative, connected, and autonomous mobility (CCAM)

The introduction of CCAM has the potential to completely change the concept of mobility by transforming it into Mobility as a Service (MaaS), which would enable safer, more efficient, comfortable, and sustainable transport systems. This outlook has far-reaching societal implications, as it merges technologies, regulatory policies, and standardization. The application of artificial intelligence (AI) is a crucial factor that has the potential to drastically change the mobility sector and accelerate this transformation at a much faster pace [1].

The vision of CCAM is based on three pillars. First, connected mobility is already here, with the most recent car models connected to external services for infotainment, security, and maintenance. Second, cooperative mobility anticipates direct communication among vehicles, pedestrians, and infrastructure through various radio technologies in the near future. Many people believe that inter-vehicle cooperation will significantly improve overall traffic performance and safety. Third, automated mobility focuses on the huge, ongoing effort from stakeholders to push automated driving, traditionally centered around the vehicle's onboard sensors. Combined, these three pillars are increasingly viewed not just as complementary technologies but as the enablers for all future revolutionary CCAM applications [2].

1.2 Vanets: The critical communication fabric of the CCAM ecosystem

CCAM's ambitious vision is vitally reliant on a strong and dynamic communication architecture that supports information exchange among all the stakeholders in the mobility ecosystem [3]. At the center of this architecture is the Vehicular Ad-hoc NETwork (VANET), which is a specialized wireless network created by the vehicles themselves. The key elements of a VANET are the on-board units (OBUs) mounted in every vehicle and the road-side units (RSUs) installed on the road infrastructure. These elements together support a range of communication modes that are collectively referred to as Vehicle-to-Everything (V2X).

Communication fabric plays a central role, analogous to that of the nervous system, at the CCAM ecosystem level, with two main operational modes. Vehicle-to-Vehicle (V2V) communication promotes a decentralized vehicle network able to share real-time data on location, velocity, and prospective hazards directly between peers without intermediaries, and such data play a vital role in helping to avoid collisions and reduce road congestion [4]. On the other hand, vehicle-to-infrastructure (V2I) communication empowers vehicles to cooperate with management systems like traffic lights and advisory signage to promote efficient flow as well as safe movement within roads. Such communications are underpinned by two main classes of wireless technologies that function within a specific spectrum range: one class adheres to the IEEE 802.11p standard (known as DSRC within America and ITS-G5 within the EU), while cellular-based C–V2X forms the other class. The incorporation of supplementary ubiquitous cellular networks like 4 G and 5 G complements vehicle-to-network (V2N) connections to empower this heterogeneous communication network to make all components within the CCAM ecosystem act together collaboratively, thereby making individual vehicles part of an ensemble intelligent agent [5]. **Figure 1** shows the structure of VANET communication in CCAM.

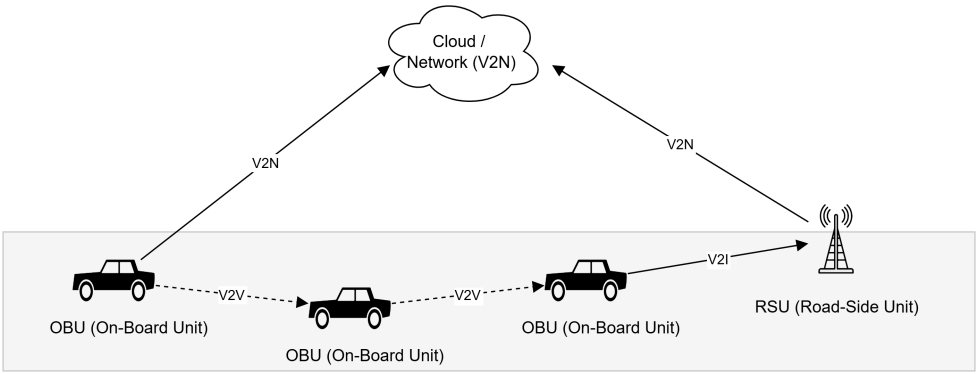


Figure 1.
The structure of VANET communication in CCAM.

1.3 The double-edged sword: New security challenges in a hyper-connected environment

The widespread interconnectivity typical of the CCAM ecosystem can potentially enhance transport safety and improve the efficiency of transport systems; however, it also creates a broad and complex new attack surface that poses significant challenges. Increased reliance upon V2X communications exposes vehicle and infrastructure assets to myriad cyber menaces that can threaten passenger safety as well as the overall transport network integrity [6]. Evaluating the most impactful attack vectors, as seen in **Table 1**, could provide a positive overall picture of this rich threat landscape [7].

The addition of such mobility, dynamic topology, and tremendous scale in VANETs intensifies these threats, rendering them much more difficult to defend against than in conventional IT systems. This wide and powerful range of potential attacks, each aimed at core principles of secure communications, highlights the limitations of static, predefined security policies [8]. The need for a dynamic defense system, which can learn from and react to these diverse and new threats in real time, directly brings us to the main subject of this chapter.

1.4 The need for lifetime, adaptive security: Chapter scope and structure

One vulnerability inherent to the CCAM ecosystem is highlighted by the complex and dynamic nature of the security threats outlined above: conventional security solutions, particularly those based on predefined signature sets or consensus-derived protocols, are inadequate for this task. Such approaches are inherently retrospective and struggle to counter emerging zero-day issues that are ever more common within sophisticated cyber-physical systems. This dilemma necessitates a shift in strategy, transitioning from static defenses to a new class of security products that are intelligent, adaptive, and capable of continuous learning throughout their operational lifespan. Toward this end, this chapter focuses on implementing lifetime learning (LL) within intrusion detection systems (IDS), calling for its implementation as a first-principles approach to strengthening vehicle security within Vehicle Ad-Hoc Networks (VANETs). To make an ethical analysis of this topic, the latter half of this

Attack type	Description	Violated Security Objective(s)
Eavesdropping	An attacker passively intercepts and listens to private communications over the wireless channel to gather sensitive information without authorization.	Confidentiality
Bogus/False information injection	A malicious node actively fabricates and disseminates false information, such as fake hazard warnings or nonexistent traffic jams, to disrupt traffic flow or trick other vehicles into making dangerous decisions.	Integrity
Replay attack	An attacker records legitimate messages (e.g., a safety alert) and retransmits them at a later time or in a different location to cause confusion or trigger inappropriate actions.	Integrity, Authenticity
Denial of service (DoS/DDoS)	An attacker overwhelms a target vehicle (OBU) or an RSU with a flood of illegitimate traffic, exhausting its resources and making it unavailable to legitimate users.	Availability
Jamming attack	An attacker deliberately transmits interfering radio signals to disrupt the wireless communication channel, preventing the successful exchange of any messages, including critical safety warnings.	Availability
Sybil attack	An attacker creates and operates a large number of pseudonymous fake identities simultaneously, using them to gain disproportionate influence, fake a traffic jam, or undermine reputation-based trust systems.	Authenticity
Masquerading/ Spoofing	An attacker impersonates a legitimate entity (e.g., another vehicle, an RSU, or a trusted authority) to send malicious commands or gain unauthorized access to information.	Authenticity

Table 1.
Taxonomy of major security attacks in the CCAM ecosystem.

volume is structured as follows: Section 2 delves into the basic tenets of the lifetime learning paradigm and elucidates its application to strengthen security within certain CCAM application scenarios. Section 3 includes a detailed account of the development of LL-IDS, describing the evolution of these systems from the earliest human-in-the-loop deployments to increasingly autonomous and collaborative systems. Section 4 explores possible directions of development within this domain, noting trends linked to LLM agents that enable completely autonomous security systems. Lastly, Section 5 concludes this volume by highlighting key insights and offering a thorough examination of this development in the context of end-to-end vehicle security.

2. The lifetime learning paradigm for securing CCAM operational domains

2.1 Limitations of traditional intrusion detection systems in VANETs

Traditional approaches to intrusion detection systems (IDSs) have been found to have significant weaknesses when faced with the specific challenges presented by VANETs, despite the general agreement on their central role in network security.

Typically, traditional IDSs may be divided into two main approaches: signature-based systems and anomaly-based systems; both face challenges within the dynamic and hostile environments of vehicular communications. Particularly, signature-based detection works by comparing network communications to a library of predefined attack signatures; this approach, however, is inherently at a disadvantage owing to a severe limitation: its inherent inability to identify new, zero-day threats [9]. This reactive approach is not properly matched to the CCAM environment, which experiences a rapid introduction of new threats. Traditional anomaly detection systems face a unique set of challenges as they create a model to define "normal" network activity and then identify anomalies. The inherent dynamism of VANETs, with their ever-changing topologies, high node mobility, and nonuniform traffic density, makes it extremely difficult to maintain a stable and uniform level of "normalcy" [10]. A context-dependent circumstance faced on a busy street may appear quite unusual on an empty highway, thus creating a higher rate of false positives. Furthermore, using machine learning techniques for pattern discovery shows that traditional offline or batch training approaches are susceptible to an effect known as "catastrophic forgetting" [11]. Retraining these static models with new data to adapt to new attack sources usually ends up overwriting and subsequently losing prior knowledge of past menaces, thus leading to obsolescence with the passage of time. Such an inability to concurrently maintain prior knowledge while still absorbing new knowledge makes traditional IDS architectures insufficient for securing VANETs, thereby establishing a need for a new conceptual approach.

2.2 Lifetime learning (LL): A conceptual framework for continual adaptation

To overcome the inherent shortcomings of traditional systems, a new paradigm needs to be developed to support a learning structure with the ability to accommodate an unending flow of data, including new classes of attacks that evolve with time. This paradigm, called lifetime learning (LL), alternatively referred to as continual learning or incremental learning [12], has a primary goal: to allow a learning system to continuously learn new knowledge about fresh categories and concepts while simultaneously maintaining information about material already learned, so as to establish an overall classifier that generalizes well to all data encountered [13]. One critical problem that LL hopes to overcome, among other important challenges, is that of catastrophic forgetting, a major problem where a model's effectiveness decreases substantially on previously learned tasks after acquiring new ones. As a result, the ideal LL model needs to strike a subtle balance between two competing goals: plasticity, or the ability to undergo rapid adaptation and learning of new patterns, and stability, or the capability to lock down and retain previously learned knowledge without its loss [14]. In dealing with this so-called "stability-plasticity dilemma," the LL paradigm provides a theoretical ground upon which to design an intrusion detection system (IDS) capable of truly adapting to the changing threat landscape typical of the Connected and Automated Mobility environment. **Figure 2** shows the lifetime learning framework for VANET IDS.

2.3 Contextualizing LL-IDS within CCAM operational domains

The intrinsic worth and core objective of the lifetime learning (LL) paradigm, applied to intrusion detection, become better understood when considered within

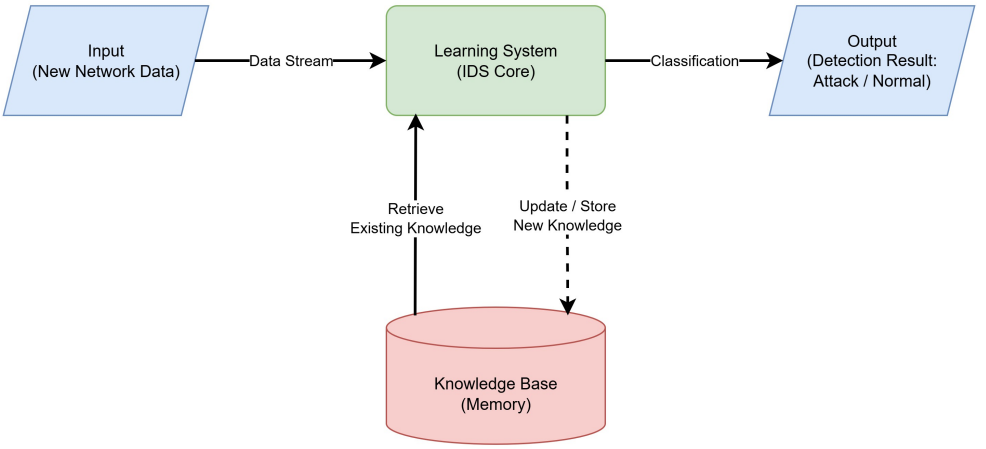


Figure 2.
Lifetime learning framework for IDS.

the particular operational scenarios of Cooperative, Connected, and Autonomous Mobility (CCAM) [15]. In such a paradigm, an LL-IDS's main goal extends beyond achieving a high detection rate by virtue of ideal measures; it becomes a key facilitator for safety-critical applications where data exchanges are essential to their operation. Such applications require effective data communications to either avoid or mitigate potential dangers to occupants, pedestrians, and other vulnerable road users [16]. This strategy is based on the dependable and uniform dissemination of messages, such as Cooperative Awareness Messages (CAMs) and Basic Safety Messages (BSMs), which contain critical information about a vehicle's position, speed, acceleration, and direction heading.

The functional space of cooperative maneuvering supports a wide range of application scenarios, such as vehicle platooning, lane-change maneuvers, and forward collision warning. These features require that vehicles participate in coordinated decision-making processes based on the Basic Safety Messages (BSMs) exchanged with other vehicles. Due to the common tendency to opt for low-latency levels by transmitting such messages in unencrypted form, they are vulnerable to a variety of attacks, such as spoofing and falsification. An attacker might fake false mobility information, possibly triggering a vehicle to perform dangerous and unexpected maneuvers, such as sudden braking or acceleration, which may lead to traffic accidents [17]. It is, therefore, essential to implement an efficient lifetime learning intrusion detection system (LL-IDS) to ensure perpetual verification of the integrity of received messages and thus enable the trust essential for vehicles to participate safely in high-speed, close-proximity collaboration. Concurrently, for applications dedicated to safeguarding vulnerable road users, an LL-IDS capable of efficiently identifying jamming or denial of service (DoS) attacks might be critical for providing uninterrupted alert notifications about pedestrians and cyclists. Finally, the implementation of an LL-IDS infrastructure is not just a technical improvement but a fundamental necessity to ensure the safety, reliability, and social acceptability of the advanced, life-saving services promised by the Connected, Cooperative, and Automated Mobility (CCAM) vision [18].

3. The evolution of lifetime learning IDS: A systematic review

3.1 Foundational models: Human-in-the-loop incremental learning

The evolution of adaptive security measures applied to vehicles draws from initial techniques that, albeit rooted within classical machine learning approaches, recognized the inherently changing threat landscape. Early approaches used strong but rigid models, such as Long Short-Term Memory (LSTM) networks, to detect attacks by inspecting traffic parameters over a long timescale. While these models showed very high accuracy in detecting previously known threats, they were inherently static and could not accommodate new patterns of attacks without going through very long retraining processes aided by an external trusted party [19]. The inability to accommodate new patterns occasioned a keen necessity to recognize a system capable of being updated continuously so that the intrusion detection system (IDS) could constantly gain knowledge during its deployed lifespan.

One significant development within this area was the development of the lifetime learning intrusion detection system (LL-IDS) [20]. The major improvement provided by the LL-IDS was its ability to recognize previously unencountered assaults, a significant step forward compared to existing architectures. The overall architectural structure of the system included a blockchain-based architecture specifically designed to maintain suspect or unclear data that could not be labeled by the incorporated intrusion detection mechanism. The data, with its high predictive capability to recognize novel patterns within emerging threats, was then distributed to established security institutions, including data research centers and security corporations, as a distributed network of "mining nodes" within the blockchain [20]. The institutions then utilized their unique expertise to analyze and label the unclear data. The newly labeled ground-truth data was then redistributed through the blockchain to all involved vehicles, allowing them to integrate it during their onboard models' retraining processes within their intrusion detection mechanisms.

The first LL-IDS system, while innovative in its ability to update its models, essentially functioned as a human-in-the-loop system. The discovery and incorporation of new threats did not take place on autopilot; instead, they were largely dependent on external human experts' manual processing, analysis, and annotation. However, while reliance on manual processing improved upon static models and ineffective unsupervised strategies [21], it still required significant latency and the continuous availability and attentiveness of security staff. Therefore, the first phase drove home the importance of a system that could learn continuously over the course of its run time while at the same time exposing the limitations of update-oriented methods based on human contributions, thus setting the correct background for more automated successive solutions. **Figure 3** shows the human-in-the-loop LL-IDS framework.

3.2 Advancing automation: Semi-supervised and unsupervised approaches

The original human-in-the-loop models, while innovative, revealed a major operational limitation: their fundamental reliance on a large quantity of high-quality, manually annotated data for model revision [22]. The strategy of relying on third-party security experts to assess and annotate suspicious data, although effective, is inherently costly and manpower-intensive. Such a dependency hinders the IDS

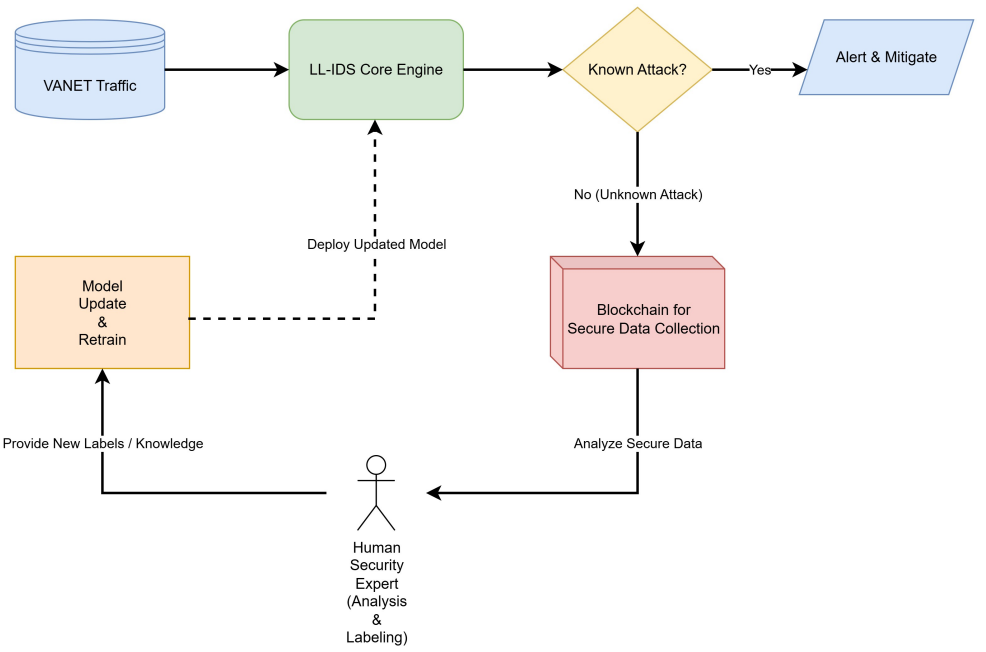


Figure 3.
Human-in-the-loop LL-IDS framework.

from quickly adjusting to the rapidly evolving VANET threat environment. Thus, the next logical step in the evolution of lifetime learning IDS was to shift from reliance on manual human action, with the goal of considerably reducing or even eliminating dependence on manual human intervention.

The Automatic Incremental Lifetime Learning Intrusion Detection System (AILL-IDS) exemplifies the advancements in this field. The key innovation of AILL-IDS lies in its use of incremental semi-supervised learning, allowing the system to learn knowledge from a data stream that contains a vast majority of unlabeled data, with a small number of labeled examples augmenting it. The system effectively deals with data-labeling challenges. Instead of, or perhaps in addition to, employing human expertise, AILL-IDS employs a sophisticated two-stage unsupervised clustering technique. In the first stage, an incremental K-Means algorithm carries out initial classifications, clustering the traffic data into clusters of "normal" and "abnormal," based on the assumption that a large volume of traffic contains a high density of data points. Upon carrying out initial classifications, the anomalous data undergoes a density-based stream clustering algorithm, called DBSTREAM, which, with complete autonomy, clusters data into significant clusters. Any newfound cluster within this process becomes a candidate for a new category of attack data and is then assigned to a new category labeled as an "Unknown Attack."

Additionally, the AILL-IDS system has embraced a more advanced system update methodology. Unlike traditional real-time updating methodologies, it integrates a concept drift detector, specifically utilizing the Kolmogorov-Smirnov Windowing (KSWIN) technique to evaluate the statistical distribution of input data flow. System updates are performed through incremental learning only when a drastic concept drift is detected, indicating a significant change within the network environment

or the appearance of a new threat pattern. This methodology ensures that updates to models remain relevant and useful. To further augment real-time protection provision within these update periods, AILL-IDS also integrates a double ensemble learning scheme, where a classifier model continually provides predictions within a certain timespan, and its offline-updated counterpart provides smooth, stable, and persistent protection functionalities.

With these innovations, the AILL-IDS framework took a significant step toward automation. By harnessing the strength of semi-supervised and unsupervised learning, it showed the way for an IDS that could learn and adapt to identify new attacks with very little dependence on costly, high-quality labeled data. Experiments demonstrated that AILL-IDS achieved a competitive detection rate, requiring only 5.5% of the data for labeling. This semi-automated phase significantly lowered the latency and expense of the human-in-the-loop models, charting a new path for the creation of more intelligent, efficient, and scalable security solutions for vehicular networks. **Figure 4** shows the workflow of AILL-IDS.

3.3 Broadening the scope: Integration with federated learning for privacy and collaboration

The complete power of machine learning unfolds when models learn from the diverse experiences of a large and varied vehicle fleet, whereas AILL-IDS's semi-supervised approach was a significant step toward automation for a single learning agent. However, this poses a fundamental challenge: conventionally, training a powerful, centralized IDS model typically requires collecting and storing vast amounts of raw data from all participating vehicles on a single server. In the CCAM environment, this centralized approach is consistently infeasible due to significant privacy risks, the commercial sensitivity of data from multiple manufacturers (OEMs), and the prohibitive communication overhead. A new paradigm was needed that would enable collaborative learning without data privacy infringements.

Federated learning (FL) is a structure that has been carefully crafted to achieve the aim of decentralized machine learning and address this problem effectively. The basic idea behind FL involves model training at the data location instead of sending it to a central model. In VANET, this process typically involves a central server sending a complete intrusion detection system (IDS) model to all participating vehicles. These vehicles then perform local model training with their drive data and the security incidents they have experienced. The key aspect here is that, instead of sending raw sensitive data to the central server, each vehicle sends only updated model parameters, maintaining the confidentiality of the learned weights or gradients. The central server then proceeds with a secure aggregation of these updates from many vehicles – possibly tens or hundreds – to update the global model. This iterative process repeats itself, allowing for collaborative improvement of the global model over time, while raw data stays in the vehicles, protecting commercial interests and maintaining end-user anonymity.

Recent research has shed light on the practical application and development of this paradigm in the context of security for Vehicular Ad Hoc Networks (VANETs), with many research studies tackling specific aspects of the problem. Pathbreaking research, as represented by Hbaieb et al.'s research, introduced a conceptual model for an SDN application of a federated learning (FL)-based intrusion detection system (IDS) specifically for the Internet of Vehicles (IoV). Hbaieb et al.'s research

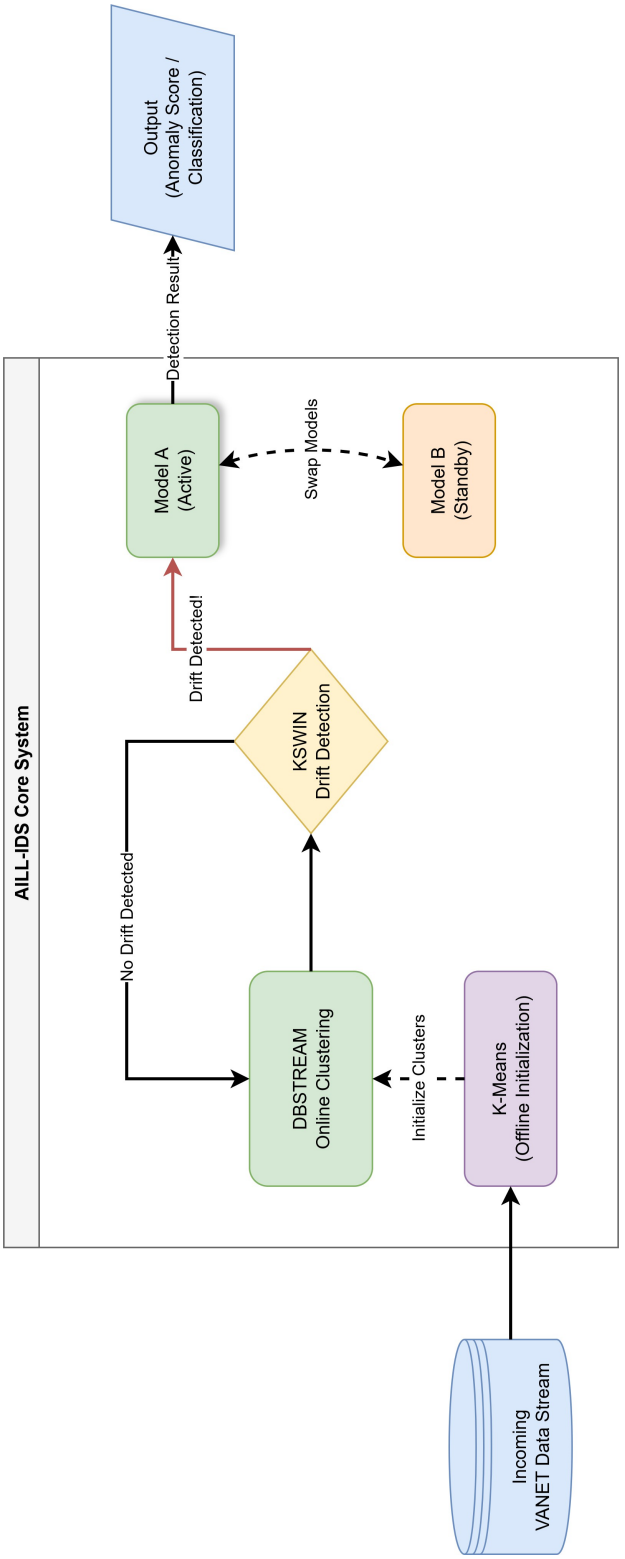


Figure 4.
AILL-IDS workflow.

proposed a novel approach by integrating the FL process into an SDN architecture, incorporating trust metrics to enhance security decision-making, and ultimately creating a comprehensive model [23]. Subsequently, other researchers have adapted the idea to fit more specific and dynamic contexts. Paying heed to the real-time nature of vehicular data, Arya et al. developed an FL architecture specifically designed for intruder detection within VANET data streams. Their contribution stands out by utilizing a distributed federation of diverse neural networks, which provides the system with a much better ability to handle the dynamic and uninterrupted data streams characteristic of smart city scenarios [24].

In an endeavor to enhance usability in real-world applications, Chen et al. aimed to create a more efficient and quicker system. They proposed a "fast and practical" federated learning intrusion detection system (FL-IDS), which accelerated the learning process, thus significantly reducing the usual communication overhead and latency that characterize federated learning. This innovation makes the system feasible even under limited-resource environments. More specifically, the study continued to leverage federated learning to achieve goals beyond conventional intrusion detection. Gurjar et al., for instance, developed a system for misbehavior classification. Their study involved an extensive evaluation of diverse aggregation methods, such as `FedAvg`, `FedProx`, and `FedYogi`, using the VeReMi dataset to prove the effectiveness of federated learning in properly classifying various malicious node behaviors [25]. Further to enhance the reliability of the distributed system, various promising proposals combine federated learning and blockchain technology. A prime example of such unification appears in Mansouri et al.'s methodology. In their novel approach, they use a blockchain framework to store a decentralized, tamper-proof ledger for model update records and the reputations of participating nodes. This combination adds an essential, transparent, and secure aspect of collaboration to the system, effectively safeguarding against nefarious parties that would use malicious updates to compromise the global model.

In all, the addition of federated learning represents a significant leap, moving away from isolated, independent learning approaches toward a collective and privacy-oriented security platform. This evolution is necessary to enable trust and achieve a genuinely intelligent and secure transportation infrastructure, especially within the elaborate CCAM environment, where many automobile manufacturers, fleet operators, and public infrastructure managers need to work together without exchanging confidential information. **Figure 5** shows the federated learning-based collaborative IDS framework.

4. The future frontier: Fully autonomous security driven by intelligent agents

4.1 The ultimate goal: A zero-intervention, self-evolving security framework

The evolution from human-in-the-loop notification systems to semi-automatic and cooperative architectures represents a major step toward improving the flexibility of intrusion detection systems (IDS). The future potential of automotive network security, however, reaches far beyond the basic goal of flexibility; it represents a vision of a truly independent and self-adaptive security setup capable of carrying out tasks without any need for human intervention. This hypothetical

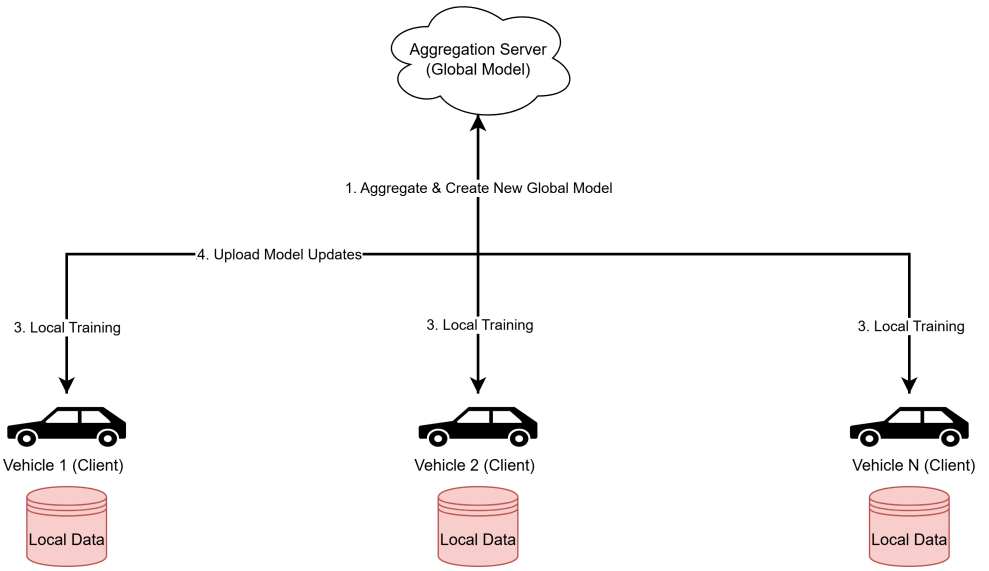


Figure 5.
Federated learning-based collaborative IDS framework.

situation identifies an IDS not merely as a stagnant tool that requires constant maintenance but as a dynamic, responsive setup that adapts and transforms simultaneously while protecting the network.

Long-term objectives are to have an efficient, automated, and adaptive VANET IDS with strong internal protection mechanisms. It should be capable of automatically detecting known and unknown cyberattacks with no necessity to pull people into data annotation, thus evading latency and cost entailed by manual expert processing. It should be capable of accounting dynamically for concept drift, adapting by itself to rapidly changing conditions within the environment of a vehicular network and shifting tactics from those who perpetrate attacks. In functional terms, such an idealized IDS should be capable of operating with high efficiency, with minimal latency related to detecting an event and, more to the point, should not be susceptible to internal update cycle-induced degradation of its own work. Finally, such a system should be inherently secure, capable of safeguarding its data and learning processes from severe perils such as data poisoning, collusion attacks, and future threats from quantum computers. In a way, the idea is to change the VANET IDS from a reactive tool to a proactive, self-sustaining, and robust cyber-defensive organism.

4.2 The role of large language models (LLMs) as reasoning engines for security

The shift to a zero-intervention security model requires a paradigm shift in the approach taken by an intrusion detection system (IDS) in identifying and understanding threats. Existing machine learning and deep learning architectures largely rely on statistical correlation, even though they are adept at identifying complex patterns within data sets. These systems can identify anomalous occurrences based on historic data that has been studied before; however, they lack the ability, unlike human beings, to understand the reason for their malevolent nature. Therefore,

the future challenge of autonomous security is to go beyond pattern recognition and create true reasoning abilities. In this regard, large language models (LLMs) might prove to be instrumental, as they can potentially find application not just as sophisticated classifiers but as advanced reasoning devices for cybersecurity in Vehicular Ad Hoc Networks (VANETs).

The incorporation of a large language model (LLM)-driven reasoning engine in a vehicular ad hoc network (VANET) intrusion detection system (IDS) offers numerous and multifaceted possibilities. One of the key features is the ability to conduct automatic analysis of zero-day attacks, thereby negating the expense and redundancy associated with manual data-labeling operations. An LLM agent may have a constantly updated knowledge database gathered from global cybersecurity intelligence sources, including academic research, threat scanning, and security experts' online forum discussions, allowing it to engage in logical reasoning based on up–to-date emerging attack patterns. The agent can analyze malicious payloads, compare their operating procedures with attack models, and deduce their likely intention and classification – this analysis takes place without needing pre-labeled training data for each threat. This level of automation significantly reduces operational expenses and minimizes the time gap between the discovery of a new threat and the deployment of countermeasures to neutralize it.

Additionally, LLMs present a breakthrough to the "black-box" problem inherent in a number of deep-learning architectures by providing explanations and human-understandable classifications. Instead of merely raising an alarm, an LLM agent can articulate its reasoning in natural language, referencing network traffic and the specific external data it uses to determine the malicious nature of an activity. The explanation is priceless as a means to seed trust within the system and to enable a human analyst to act sooner, with a better outcome. At its ambitious end, this vision extends toward active defense generation, where the LLM doesn't just come to reason about a threat but actually suggests or even generates new defensive strategies, such as building specific sets of firewall policies or suggesting patches to mitigate a newly comprehended threat. This breakthrough possibility sets a new standard to be achieved by future research, shedding light on how next-generation AI can deliver a stronger, smarter security posture across an entire CCAM ecosystem. **Figure 6** shows the LLM-enhanced reasoning engine in IDS.

4.3 The C-VIDS framework: A cognitive vehicular intrusion defense architecture

To translate the vision of an LLM-based reasoning engine into a concrete architectural design, we propose C-VIDS: a Cognitive Vehicular Intrusion Defense framework for Lifetime Learning. C-VIDS is designed as a modular, three-layer system that moves beyond simple pattern matching to enable genuine threat comprehension and adaptive responses. The architecture, as illustrated in **Figure 7**, comprises a Perception Layer, a Cognition Layer, and an Action Layer.

4.3.1 Perception layer: From raw data to structured knowledge

The primary function of the Perception Layer is to process the vast, multi-modal data streams generated by the vehicle and translate them into a structured, human-readable format that an LLM can reason with. This layer includes two key components:

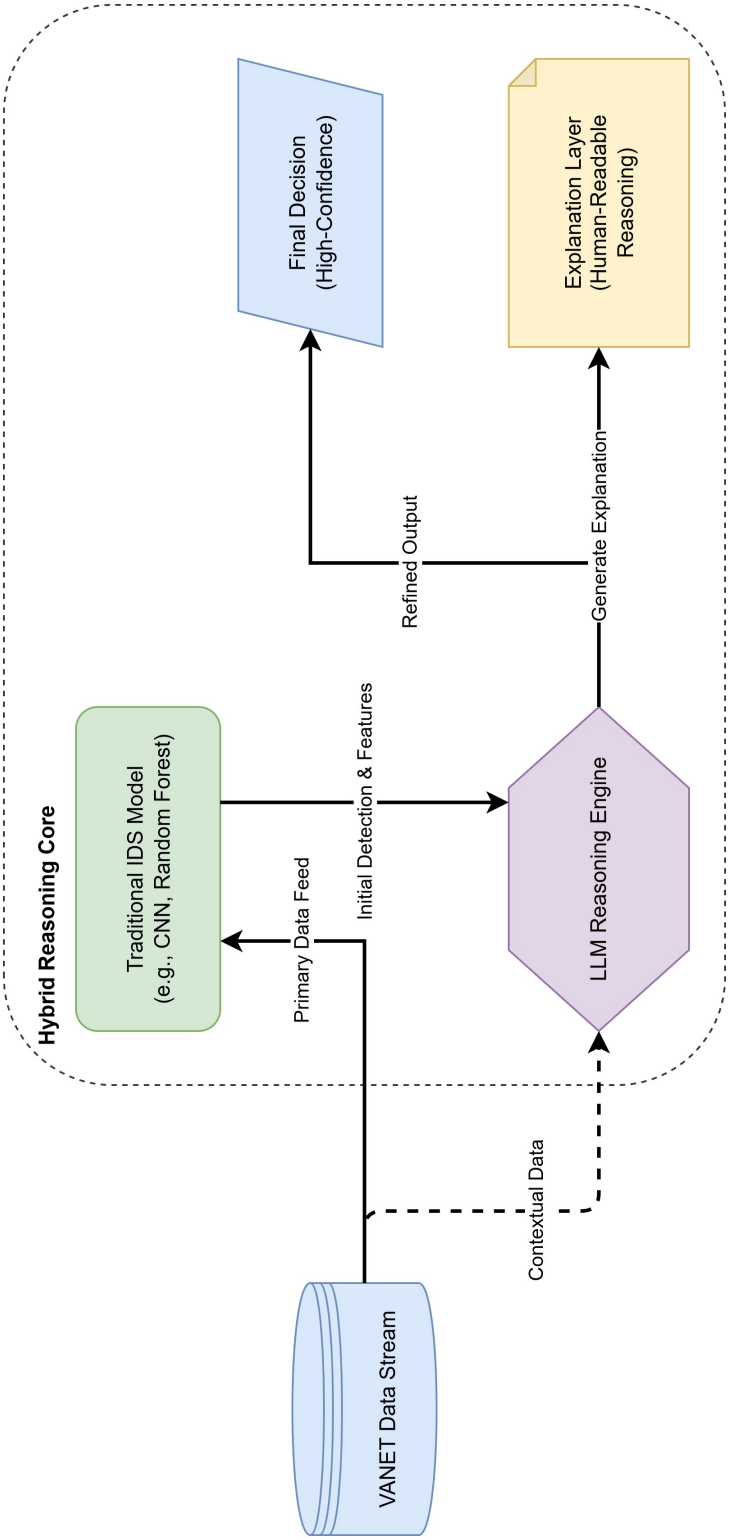


Figure 6.
LLM-enhanced reasoning engine in IDS.

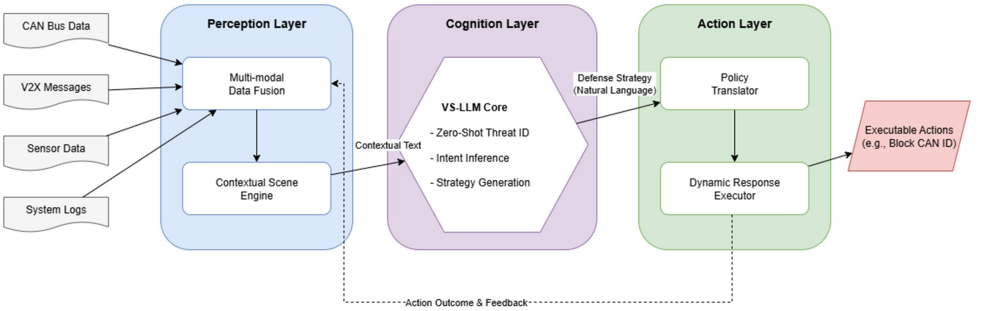


Figure 7.
Architecture of the C-VIDS framework with its lifetime learning feedback loop.

- **Multi-modal data fusion:** This component ingests and synchronizes data from diverse sources, including in-vehicle networks (CAN, Ethernet), V2X communications, physical sensors (GPS, LiDAR), and ECU system logs, creating a unified data stream.

- **Contextual scene engine:** This is a critical innovation that contextualizes the fused data stream into a descriptive text sequence. For instance, raw data like `[Timestamp: 123.45, CAN_ID: 0x1A, GPS: (34.05, -118.24), Speed: 65mph]` is translated into a narrative: "Vehicle is traveling at 65mph on a highway. Engine RPM is stable. A V2X message was received indicating slow traffic 1 mile ahead." This narrative provides the necessary context for high-level reasoning.

4.3.2 Cognition layer: The LLM-driven reasoning core

This layer is the brain of the C-VIDS framework, where a specialized Vehicular Security LLM (VS-LLM) – potentially a fine-tuned, lightweight model like `Llama-3-8B` – analyzes the contextualized text from the Perception Layer. Its core functionalities include:

- **Zero-shot threat identification:** Leveraging its broad knowledge base, the VS-LLM can identify novel zero-day attacks by reasoning about logical contradictions within the scene description (e.g., braking commands being issued while the vehicle accelerates).

- **Attack attribution and intent inference:** Beyond detection, the VS-LLM generates hypotheses about the attack's nature and objective. For example: "Hypothesis: The inconsistent sensor readings suggest a coordinated spoofing attack targeting the ABS control unit, likely aiming to trigger an unnecessary emergency brake."

- **Adaptive defense strategy generation:** Based on its inference, the VS-LLM formulates dynamic, context-aware defense strategies in natural language, such as: "Recommended action: Isolate the suspected compromised ECU from the main CAN bus. Initiate a redundant sensor cross-validation protocol. Alert the driver with a high-priority warning."

4.3.3 Action layer: From cognitive decisions to concrete defense

This layer acts as the framework's effector, translating the LLM's natural language strategies into machine-executable actions.

- **Policy translator:** This module converts textual commands into specific system configurations, such as firewall rules or process termination commands.

- **Dynamic response executor:** This component implements the commands on the vehicle's OS or gateway, for instance, by re-routing data streams or isolating a compromised ECU.

- **Feedback and learning loop:** Crucially, the outcome of any action is fed back into the Perception Layer, creating a closed loop. The VS-LLM analyzes the effectiveness of its responses, reinforcing successful strategies and learning from failures, thus enabling true lifetime learning and system evolution.

4.4 Case study: Defending against a coordinated sensor spoofing attack with C-VIDS

To illustrate the practical utility of the C-VIDS framework, we present a proof-of-concept case study. This "thought experiment" demonstrates how C-VIDS would handle a sophisticated, zero-day attack that traditional IDS would likely miss.

- **Attack scenario:** An autonomous vehicle equipped with C-VIDS is traveling on a highway. An attacker wirelessly injects falsified data into both the camera and LiDAR sensors, creating a "ghost" obstacle while simultaneously broadcasting a fake accident warning via V2X.

- **C-VIDS response:**

1. **Perception layer:** The Contextual Scene Engine receives conflicting data streams and generates the following text: "High-speed highway travel. Critical Alert: Obstacle detected by both camera and LiDAR at 50 meters. V2X message confirms accident ahead. CONTRADICTION: Vehicle speed is constant, no driver braking input, and internal gyroscope data show no deceleration."

2. **Cognition layer:** The VS-LLM analyzes this text and performs a logical inference: "The simultaneous external sensor and V2X alerts are directly contradicted by internal vehicle dynamics. This is a strong indicator of a coordinated sensor spoofing attack, not a genuine obstacle. The attacker's intent is likely to force an unnecessary emergency brake." It then generates a defense strategy: "Recommended Action: 1. Immediately flag Camera, LiDAR, and V2X data streams as untrustworthy. 2. Prioritize internal sensors (gyroscopes, wheel speed sensors) for stability control. 3. Suppress automated emergency braking. 4. Alert the driver to the sensor anomaly."

3. **Action layer:** The Policy Translator converts these commands into actions, preventing the AEB system from being triggered and ensuring the vehicle's

stability, thereby thwarting the attack. This case study demonstrates C-VIDS's ability to reason beyond raw data and defend against complex, unseen threats.

4.5 Open research challenges and future directions

Though a wonderful opportunity to utilize LLMs as standalone reasoning engines for VANET security, its practical implementation depends on overcoming a host of stringent research challenges. Not only are they products of the very constraints of current-day LLM technology itself, but they are further intensified by the special, safety-critical requirements of the automotive environment. Overcoming these challenges will be critical for future work.

However, the immediate concern revolves around real-time computation and latency issues for LLMs. VANETs, as with CCAM, are real-time applications where processing safety messages must be completed within the realm of milliseconds. However, the computation latency of modern LLMs, with their billions of parameters and autoregressive inference processes, is significantly higher than that of lightweight ML models. Therefore, real-time applications at the edge of threat detection find it impractical to use a direct, end-to-end, all-LLM-based design. A significant area for future work thus becomes designing hybrid architectures capable of trading, in a knowledgeable manner, real-time speediness with richer reasoning. This would then entail designing systems where routine, standard traffic analyses are handled by lightweight models, with escalation to an LLM only for novel, complex anomalies just in case of novel, sophisticated anomalies requiring richer, non-time-critical analysis. In addition, research involving closing said latency gap by way of model compression, quantization, and designing smaller, domain-specific LLMs specifically with regard to being applied to matters involving cybersecurity could substantially narrow said latency gap.

Also, because the LLM occupies the center of the IDS, the integrity and robustness of the LLM itself are of primary concern. The LLM is a novel, high-value attack surface. Defense against attacks on the learning and reasoning capabilities of the model is a primary research focus. These include data poisoning attacks, where an attacker gradually poisons the massive external knowledge bases on which the LLM queries to bias future decision-making, and adversarial prompting or evasion attacks, where malicious traffic is specifically crafted to leverage quirks in the LLM's reasoning in an attempt to induce a misclassification. Having strong mechanisms to attest to the integrity of the LLM's knowledge base and to detect and invalidate adversarial inputs is an essential challenge that must be solved to make a trustworthy system possible.

Lastly, the traditional problem of hallucination and reliability is a treacherous threat in a safety-critical system such as VANETs. An LLM that is able to generate a believable but false analysis of a danger, a false positive or negative, has the potential to cause devastating effects, such as making one car stop suddenly or neglecting to register a valid threat. The future should focus on developing strict validation and fact-checking layers for an LLM's output. This might include systems in which justification by an LLM is cross-checked against several sources of evidence or formal methods before any defensive measure is taken. The use of "guardrails" that constrain an LLM's decision-making ability and make its conclusions rational and data-verifiable will be critical to unleashing these powerful reasoning machines into our world with safety and sense. **Figure 8** shows the research challenges for LLM-based security in VANETs.

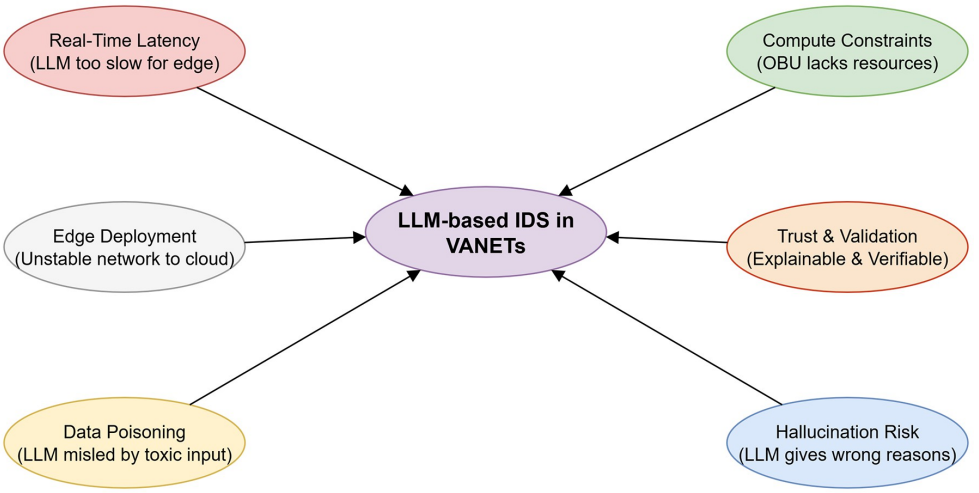


Figure 8.
Research challenges for LLM-based security in vanets.

5. Conclusions

The primary contribution of this work, however, lies in looking beyond current paradigms to the future frontier of truly autonomous security. We have proposed C-VIDS, a novel cognitive defense framework driven by a large language model reasoning engine (Section 4.3). This framework moves beyond mere pattern recognition to enable contextual understanding, logical inference, and adaptive strategy generation. Through a detailed conceptual case study (Section 4.4), we demonstrated C-VIDS's potential to defend against complex zero-day attacks that would evade traditional systems.

While significant research challenges remain – particularly concerning real-time latency and computational constraints – the pursuit of an intelligent, self-evolving, and agent-driven security system is not merely a technical exercise. It is, we argue, the foundational step required to build the trust and resilience necessary to unlock the full safety, efficiency, and societal potential of the Cooperative, Connected, and Autonomous Mobility ecosystem.

Author details

Yunfan Huang
Universiti Malaya, Kuala Lumpur, Malaysia

*Address all correspondence to: 23086929@siswa.um.edu.my

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] Eshetu AA, Valilai OF, Wicaksono H. Unveiling the potential of Artificial Intelligence in Cooperative, Connected, and Automated Mobility (CCAM) solutions: A systematic literature review. In: 2024 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). 2024; p. 1272–1276. Available from: https://ieeexplore.ieee.org/abstract/document/10857172

[2] Ferreira J. Cooperative, Connected and Automated Mobility (CCAM): Technologies and applications. Electronics. 2019;**8**(12):1549. DOI: 10.3390/electronics8121549

[3] Naudts D, Maglogiannis V, Hadiwardoyo S, van den Akker D, Vanneste S, Mercelis S, et al. Vehicular communication management framework: A flexible hybrid connectivity platform for CCAM services. Future Internet. 2021;**13**(3):81. DOI: 10.3390/fi13030081

[4] Dutta A, Samaniego Campoverde LM, Tropea M, De Rango F. A comprehensive review of recent developments in VANET for traffic, safety & remote monitoring applications. Journal of Network and Systems Management. 2024;**32**(4):73. DOI: 10.1007/s10922-024-09853-5

[5] Berlato S, Centenaro M, Ranise S. Smart card-based identity management protocols for V2V and V2I communications in CCAM: A systematic literature review. IEEE Transactions on Intelligent Transportation Systems. 2022;**23**(8):10086–10103. DOI: 10.1109/TITS.2021.3118721

[6] Campo OC, Martínez VG, Encinas LH, Muñoz AM, Fernández RÁ. Cybersecurity trends in Cooperative, Connected and Automated Mobility. Logic Journal of the IGPL. 2024. DOI: 10.1093/jigpal/jzae072

[7] Shetty SR, Manjaiah DH. A Comprehensive Study of Security Attack on VANET. In: Sharma N, Chakrabarti A, Balas VE, Bruckstein AM, editors. Data Management, Analytics and Innovation: Proceedings of ICDMAI 2021, Volume 2. Lecture Notes on Data Engineering and Communications Technologies, vol. **71**. Singapore: Springer; 2022. p. 407–428. DOI: 10.1007/978-981-16-2937-2_25

[8] AlMarshoudMishri KS, Security A-BH. Privacy, and decentralized trust management in VANETs: A review of current research and future directions. ACM Computing Surveys. 2024. DOI: 10.1145/3656166

[9] Almehdhar M, Albaseer A, Khan MA, Abdallah M, Menouar H, Al-Kuwari S, Al-Fuqaha A. Deep learning in the fast lane: A survey on advanced intrusion detection systems for intelligent vehicle networks. IEEE Open Journal of Vehicular Technology. 2024;**5**:869–906. DOI: 10.1109/OJVT.2024.3422253

[10] Borah A, Paranjothi A, Thomas JP. A survey on distributed approaches for security enhancement in vehicular ad-hoc networks. Computer Networks. 2025;**261**:111140. DOI: 10.1016/j.comnet.2025.111140

[11] Agbedanu PR, Musabe R, Rwigema J, Gatare I, Maginga TJ, Amenyedzi DK. Towards achieving lightweight intrusion detection systems in Internet of Things, the role

of incremental machine learning: A systematic literature review. F1000Research. 2022. Available from: https://f1000research.com/articles/11-1377

[12] Bhuyan MH, Bhattacharyya DK, Kalita JK. Survey on incremental approaches for network anomaly detection. arXiv. 2012. Available from: https://arxiv.org/abs/1211.4493

[13] Shyaa MA, Ibrahim NF, Zainol Z, Abdullah R, Anbar M, Alzubaidi L. Evolving cybersecurity frontiers: A comprehensive survey on concept drift and feature dynamics aware machine and deep learning in intrusion detection systems. Engineering Applications of Artificial Intelligence. 2024;**137**:109143. DOI: 10.1016/j.engappai.2024.109143

[14] Zhou D-W, Wang Q-W, Qi Z-H, Ye H-J, Zhan D-C, Liu Z. Class-Incremental learning: A survey. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2024;**46**(12):9851–9873. DOI: 10.1109/TPAMI.2024.3429383

[15] Boutahala R, Fouchal H, Ayaida M, Mao S. Trust verification scheme for cooperative, connected, and automated mobility (CCAM). Rochester, NY: Social Science Research Network. 2024. Available from: https://papers.ssrn.com/abstract=5006699

[16] Almalki SA, Abdel-Rahim A, Sheldon FT. Adaptive IDS for cooperative intelligent transportation systems using deep belief networks. Algorithms. 2022;**15**(7):251

[17] Nagarajan J, Mansourian P, Shahid MA, Jaekel A, Saini I, Zhang N, et al. Machine Learning based intrusion detection systems for connected autonomous vehicles: A survey. Peer-to-Peer Networking and Applications. 2023;**16**:2153–2185

[18] Anbalagan S, Raja G, Gurumoorthy S, Suresh RD, Dev K. IIDS: Intelligent intrusion detection system for sustainable development in autonomous vehicles. IEEE Transactions on Intelligent Transportation Systems. 2023;**24**(12):15866–15875

[19] Yu Y, Zeng X, Xue X, Ma J. LSTM-Based intrusion detection system for VANETs: A time series classification approach to false message detection. IEEE Transactions on Intelligent Transportation Systems. 2022;**23**(12):23906–23918

[20] Huang Y, Ma M. ILL-IDS: An incremental lifetime learning IDS for VANETs. Computers & Security. 2023;**124**:102992

[21] Bangui H, Ge M, Buhnova B. A hybrid machine learning model for intrusion detection in VANET. Computing. 2022;**104**(3):503–531

[22] Huang Y, Ma M. AILL-IDS: An automatic incremental lifetime learning intrusion detection system for vehicular Ad Hoc networks. IEEE Transactions on Intelligent Transportation Systems. 2025;**26**(2):2669–2678

[23] Hbaieb A, Ayed S, Chaari L, "Federated learning based IDS approach for the IoV," In: Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES '22); Vienna, Austria. New York, NY, USA: Association for Computing Machinery; 2022. **123**, p. 6. DOI: 10.1145/3538969.3544422

[24] Arya M, Sastry H, Dewangan BK, Rahmani MKI, Bhatia S, Muzaffar AW,

et al. Intruder detection in VANET data streams using federated learning for smart city environments. Electronics. 2023;**12**:894

[25] Gurjar D, Grover J, Kheterpal V, Vasilakos A. Federated learning-based misbehavior classification system for VANET intrusion detection. Journal of Intelligent Information Systems. 2025;**63**(3):807–830

Section 3

Human Factors and Trust

Chapter 10

Designing Trustworthy Futures: Research Priorities for Human-Centered, Connected, and Autonomous Mobility

Sharon L. Burton

Abstract

Connected, cooperative, and autonomous mobility (CCAM) is fundamentally reshaping interactions among people, vehicles, and infrastructure to enhance transportation safety, efficiency, and convenience. As digital technologies are increasingly woven into vehicles and roadway networks, there is a critical need for research that propels innovation while addressing challenges in control, management, and validation. This chapter offers a forward-looking assessment of essential research priorities and societal considerations in developing intelligent, connected transportation systems. At the core of this transformation are artificial intelligence (AI), big data analytics, and advanced communication protocols, which enable real-time decision-making and hold the potential to minimize human error, improve traffic flow, and personalize mobility services. However, integrating these technologies introduces new concerns regarding ethical practices, data transparency, and system accountability. Robust, secure, and interoperable frameworks are necessary to foster public trust and ensure equitable access across diverse user groups. The chapter highlights the significance of designing mobility systems that are inclusive, environmentally sustainable, and adaptable to urban and rural needs. It advocates for multidisciplinary research, combining behavioral analysis, system modeling, and participatory design, to better comprehend user requirements and system performance. Special emphasis is placed on validating autonomous functions in real-world environments through structured testing and simulations. The chapter concludes with a call for collaborative research to support long-term planning, resilience, and fairness in future mobility systems. By addressing technical and societal challenges, this chapter aims to guide researchers, practitioners, and policymakers in creating intelligent, responsible transportation solutions that serve the public interest.

Keywords: connected autonomous vehicles, ethical artificial intelligence, human-centered mobility, intelligent transportation systems, mobility innovation frameworks

1. Introduction

As transportation technologies evolve, societies face critical and salient questions about how emerging systems, such as autonomous and electric vehicles (AEVs), will integrate into daily human routines [1, 2]. Will these technologies enhance collective mobility while preserving the dignity, safety, and agency of every passenger, or will they introduce new layers of exclusion, opacity, and control? Such concerns point to a deeper analytical problem: How can a human-centered design (HCD) approach ensure that the development of autonomous electric vehicles (AEVs) aligns with users' psychological, behavioral, and ethical needs across diverse populations? There exists a precarious deficiency of validated frameworks and empirical evidence steering the development, deployment, and governance of agentic vehicle (AgVs) that reliably address human-centered needs, ethical challenges, technical robustness, and cross-sector trust in real-world connected and autonomous mobility systems. Additionally, there is an initial need to comprehend CCAM. CCAM encompasses a transformative vision that integrates digital connectivity, collaboration, and automation within transportation systems, fundamentally changing how individuals, vehicles, and infrastructures interact [3]. As connected, cooperative, and autonomous mobility (CCAM) matures, distinctions among autonomous vehicles (AVs), AEVs, and AgVs gain critical significance: AVs are primarily guided by preprogrammed autonomy, AEVs build on this by integrating sustainable electric propulsion, and AgVs advance the paradigm further by employing agentic AI capable of contextual reasoning and social adaptability. The shift from autonomy to agency within the CCAM framework marks a wider historical and societal evolution, moving from viewing individuals and machines as isolated autonomous agents toward recognizing that, whether AV, AEV, or AgV, they are contextually embedded, shaped by social interactions, and expected to interpret and respond to complex human environments flexibly. This reconceptualization calls for the integration of perception, situational sensitivity, and adaptability as foundational criteria for next-generation intelligent mobility [3].

This chapter argues that HCD is indispensable to the successful widespread adoption of AEVs. While technological refinement is essential, trust, usability, and social acceptance are the true gatekeepers to practical deployment. Thus, the central thesis of this chapter is that AEVs must evolve from being merely autonomous systems that follow preprogrammed instructions to becoming AgVs, adaptive ones that can reason and are socially responsive systems that can interact logically [4]. Such vehicles should be co-designed with the human experience at the vanguard [4].

The originality of this research lies in addressing a significant gap in current AV literature. In the last decade alone, 74 peer-reviewed studies have systematically analyzed technical advancements and adoption factors for AVs [5, 6]. Collectively, these research teams [7–9] have sampled data from over 20,000 participants to assess performance, communication protocols, and control technologies. Despite this wide-ranging technical focus, literature reviews note that the majority of academic output in intelligent transportation systems mainly addresses methodologies for sensing, communication, modeling, and algorithmic optimization but pays less attention to user-centered or societal factors [10]. The result is a clear research gap: while technical innovation persists at a rapid pace, authoritative sources recognize the need for more emphasis on HCD, inclusivity, and the social implications of autonomy in mobility systems.

The conceptual framework adopted in this research is the Human-Centered Agentic Mobility Systems Framework, which integrates HCD, agentic intelligence, and sociotechnical analysis to guide the advancement of CCAM ecosystems [11]. This framework asserts that the evolution from static AVs (AuVs, AVs, AEVs) to social, context-aware AgVs must prioritize not only technological performance but also ethical reasoning, user inclusion, transparency, and iterative stakeholder engagement. By centering on adaptive intelligence and participatory design, the framework furthers the development of mobility systems that can learn from context, reason about user intent, and adjust behaviors dynamically, thereby strengthening trust and social acceptance. The framework's significance lies in its capacity to bridge gaps generally found in conventional intelligent transportation paradigms, which focus on efficiency and automation but inadequately address human factors and value-sensitive interactions. Through its holistic approach, the framework advances the roles of interpretability, ongoing system auditing, and ethical governance, inspiring multidisciplinary research that proactively predicts risks such as algorithmic bias, data poisoning, and exclusion of marginalized groups. Conversely, the framework faces two notable critiques: limited empirical evidence on real-world human-vehicle interactions may slow responsiveness to unpredicted risks, and practical application across regions with differing social norms can introduce operational complexity and delayed consensus.

The shift from autonomy to agency reflects a broader historical and societal transformation. This information is significant as it encapsulates an entrenched evolution in the manner in which individuals are comprehended within today's society [3]. The researcher, Yu, posits that no longer is the thought of societal beings existing as independent actors (autonomy), but rather as socially entrenched people whose selections and capacities are formed by affiliations, foundations, rituals, and environments (agency) [3]. The term autonomy conventionally specifies self-governance, associated with machines acting independently of human control, usually governed by preprogrammed logic [3]. A research team argues that, as real-world applications reveal themselves, AVs must traverse complex social environments, which include interpreting human social signals and managing uncertainty in human-centric everyday interactions [12]. This progression imposes a reconceptualization of autonomy, one that integrates perception, situational sensitivity, and adaptability.

According to Yu [3], AgVs are anticipated next-generation systems that represent a new class of smart transportation, moving beyond traditional AuVs. They introduce and systematically develop the concept of AgVs as a new class of intelligent transportation systems that surpass traditional and static autonomy (i.e., AVs [AuVs]). AgV vehicles use large language models, multimodal perception, and long-term goal-directed planning to reason, communicate, and adapt within complex mobility ecosystems. AgVs leverage forward-thinking large language models, sophisticated multimodal perception, and robust long-term goal-directed planning to reason, communicate, and dynamically adapt within complex mobility ecosystems. As posited by Yu [3], AgVs exemplify a human-centered approach to mobility by assimilating agentic intelligence capable of contextual analysis and social interaction. Accompanying this perspective, Li et al. [13] provides an inclusive evaluation of the manner in which large language models and multimodal large models augment perception, planning, and responsiveness, shaping the

technological support of intelligent transportation systems. The emergence of AgVs presents capabilities and complexities that necessitate holistic frameworks, including ethics, inclusion, transparency, and reliability [14].

Research offers a critique of traditional engineering approaches to AEV development; this critique highlights that even though safety and performance are addressed, the overall engineering is frequently deficient regarding usability, inclusivity, and human factors [15]. Muhammad's critique is significant because it emphasizes the necessity for a more all-inclusive engineering philosophy. This approach integrates user experience studies, designing solutions with the people who will use them, and all-encompassing practices from the earliest stages of development [15]. According to Muhammad [15], this approach could enable the AEV ecosystem to more effectively offer equitable access, build public trust, and create meaningful value for society. The question may be: how does Muhammad's research connect to AvGs? The information regarding the need for greater attentiveness to usability, inclusivity, and human factors in AEVs precisely links to the concept of AvGs by reinforcing the importance of the evolution from traditional autonomy to agentic design. In essence, this data highlights why engineers must shift their paradigm beyond a narrow focus on metrics and meticulously address the lived realities and perspectives of all users to achieve societal and technological progress. Trust breakdowns often occur not because vehicles malfunction, but because users cannot comprehend system logic or interact meaningfully with the interface [16]. In this regard, HCD offers ergonomic guidelines, as well as a co-operative philosophy that positions the user as a co-creator in system design. As stated by Sharma [17], accessibility remains a profoundly overlooked criterion in early deployments. Elderly users, persons with disabilities, or passengers unfamiliar with digital technology often encounter exclusionary barriers, ranging from inaccessible human-machine interface (HMI) elements to a lack of feedback or alternative control methods [18, 19]. Human-centered methods explicitly challenge these barriers by embracing universal design principles that accommodate a wide range of capabilities from the outset.

A further rationale for a design-centered focus is that technical flawlessness does not parallel user satisfaction [20]. Systems that fail to justify themselves or acknowledge indecision may function optimally, yet the system may seem frightening or untrustworthy to users. Studies accentuate that transparency, applicable rationalizations, and adaptive interfaces are crucial for ascertaining user trust; without these, even forward-looking and dependable vehicles can be identified as erratic or menacing [21, 22]. Thus, the achievement of future AEVs is contingent on co-adaptive, transparent, and interpretable interaction ideas entrenched in user behavior and psychosocial needs [23].

View **Table 1** of terms to comprehend the differences between the vehicles.

This research investigates the historical background of autonomy versus agency vehicles, outlines significant assumptions, limitations, and delimitations, and recognizes the exact research gap influencing this work to offer an ample analysis of this issue. This research then continues through a structured methodology section, followed by a critical literature review. A detailed conceptual framework is developed and critiqued, and the originality of the work is established. The following sections – results, discussion, and conclusions – synthesize key findings and propose forward-looking implications for design, ethics, and policy.

Agentic artificial intelligence:	A type of artificial intelligence designed with the capacity for autonomous decision-making, contextual understanding, and goal-directed behavior, enabling it to interpret complex environments, reason about outcomes, and interact socially or adaptively in response to human or environmental cues.
Agentic vehicles (AgVs):	A new class of intelligent vehicles, equipped with agentic artificial intelligence, enables them to not only drive autonomously but also reason contextually, communicate, adapt goals dynamically, and interact meaningfully with both occupants and their external environment as social participants in mobility systems.
Autonomous Electric vehicles (AEVs):	Vehicles that operate without direct human control, using automated driving systems powered exclusively by electric propulsion, and typically featuring on-board sensors, perception systems, and environmentally sustainable energy sources.
Autonomous vehicles (AVs)	Motor vehicles capable of navigating and performing driving tasks without continuous human input rely on programmed decision logic and advanced sensor-based automation to execute journeys under defined conditions.
Connected, cooperative, and autonomous mobility (CCAM):	A transformative paradigm in transportation that integrates digital connectivity, collaboration among vehicles and infrastructure, and varying levels of driving autonomy to improve safety, efficiency, user experience, and systemic coordination within intelligent transport ecosystems.

Created by Dr. Sharon L. Burton.

Table 1.
Differentiating the Vehicles.

2. Background

The purpose of this background is to provide context and explain the significance of this research. Introduced is a summary of existing knowledge regarding AgVs, theories, and previous studies related to the research concern. The gaps in the current understanding of AgVs that this research aims to address are highlighted. This background is intended to justify the need for the research and establish the foundation for this research's objectives and questions.

2.1 Agentic vehicles (AgVs): Concept and societal relevance

AgVs have moved beyond conventional autonomy by integrating agentic AI into complex environments. These vehicles, AgVs, are designed to reason, adapt, and interact unaided, negotiating goals and responding dynamically to human occupants and environmental stimuli [3]. AgVs are dissimilar to AVs (AuVs), which adhere to preset instructions and rely on external input [3]. AgVs differ from AEVs in that AgVs possess agentic artificial intelligence (AI), enabling them to reason, adapt, and interact dynamically within complex environments [24]. AEVs primarily rely on preprogrammed autonomy without advanced context-driven reasoning or human-like interaction capabilities.

These distinctions are essential as transportation technology advances, with AGVs envisioned as interactive participants in human-centered mobility systems.

The rationale for introducing AgVs stems from growing limitations in the current autonomous frameworks, such as those set by the Society of Automotive Engineers (SAE) Standard J3016, which focus primarily on technical driving abilities without adequately addressing human-machine interaction and ethical reasoning [3]. Further, according to Yu [3], AgVs are relevant to society as they mark a systemic transformation in mobility by considering human-centric needs, ethical dilemmas, and context-sensitive decision-making (i.e., rerouting during medical emergencies or anticipating and responding to dynamic hazards on the road).

The significance of this research lies in identifying gaps in current approaches and shaping new standards for intelligent transportation systems. By exploring AgVs, this work positions itself at the intersection of technology, behavioral analysis, and participatory design, with the goal of guiding long-term planning, safety assurance, and ethical grounding in future mobility systems. Next is to review three corresponding critiques.

Critique 1: Current research emphasizes that AgV frameworks frequently project an optimized future scenario, often modulating the intricacies of regulatory harmonization, regional infrastructure disparities, and the pace at which public agencies can adopt compulsory data and privacy standards. For example, Yu [3] notes that the vision for interoperable, ethical, and human-centered AgVs is contested by jurisdictional fragmentation (uneven regulatory readiness and the lack of universally adopted digital mobility protocols), uneven regulatory readiness (some governments or regulatory bodies are well-prepared to oversee and manage new technologies, having lucid standards, review procedures, and enforcement mechanisms, while others are underprepared or lag behind), and the lack of universally adopted digital mobility protocols (there is no single, widely agreed-upon set of technical guidelines or standards that dictate how digital systems in vehicles communicate with each other, the road infrastructure, and users). These voids leave gaps in privacy, cybersecurity, and equitable service access. Thorough frameworks that advocate for open standards remain aspirational among differing levels of technological maturity and policy dedication across global markets. A second critique is next.

Critique 2: Literature emphasizes advances in agentic AI and multiagent systems; scholars highlight a dearth of critical attention to emergent risks [25, 26]. It details how real-world deployment of agentic AI can lead to unpredictable system behaviors (i.e., agents pursuing conflicting objectives or exhibiting vulnerabilities to data poisoning, adversarial manipulation, and tool misuse). Further critiqued by Yu [3] is the predominant research focus on technological capability instead of threat modeling and resilience, asserting that agentic AI's flexibility can become a liability in rapidly evolving, interconnected environments. A third critique follows next.

Critique 3: As given by Yang and Kim [27], there is a void of empirical data validating how AgVs perform under real driving conditions. Furthermore, there is minimal research addressing how these systems handle ethical decision-making or how users perceive and accept AgVs [28]. This absence of robust evidence complicates attempts to create consistent standards and effective regulatory frameworks for these intelligent agents [28].

These critiques emphasize the necessity for multidimensional research, incessant auditing, and robust user studies before widespread AgV deployment. There is a sound need for continuing system auditing to ensure that AgVs consistently meet safety, ethical, and performance standards. Comprehensive user studies are also

essential before AgVs can be widely deployed, as they help validate user acceptance and system reliability.

2.2 Critique of agentic frameworks: Safety, security, and transparency

As noted by Silva [29], recent scholarship challenges the robustness of current agentic frameworks in autonomous mobility, revealing distinctive gaps that have explicit implications for societal safety and security. The research team [30] suggested that traditional frameworks falter in modeling the unpredictable actions of AgVs. This [30] information is significant for three distinct reasons: (1) their autonomy and machine learning capabilities introduce threats such as the deliberate alteration of inputs in order to mislead, confuse, or exploit the weaknesses of an AI or machine learning system (adversarial manipulation), (2) the objectives of an AI system diverge from, or fail to entirely reflect, the intents, values, or priorities of its human designers or users (goal misalignment), and (3) the deliberate corruption or manipulation of the data that autonomous and connected vehicles rely on (i.e., traffic patterns, sensor inputs, or mapping information) in order to cause errors, disruptions, or unsafe behavior, otherwise referred to as data poisoning within the mobility ecosystem [30]. This unpredictability is highly relevant to society, given the stakes of road safety and cybersecurity in highly automated environments.

A vital concern for this research is explainability and auditability. According to [31], these two qualities determine whether AgVs' decisions and actions can be clearly understood and traced. Without transparent and auditable architectures, it becomes challenging to diagnose incidents, confirm compliance, and preserve stakeholder trust in AgVs.

The criticality of these points is amplified by AgVs' reliance on complex, frequently unclear artificial neural networks, and the exchange of information between autonomous entities or agents (i.e., vehicles, drones, or roadside sensors) without direct human involvement. As stated in Yu [3], within mobility ecosystems, this work enables vehicles to coordinate actions (e.g., merging safely, rerouting in response to congestion, or warning one another of hazards).

Supply chain security for AI models is a precarious, yet repeatedly underrated susceptibility in autonomous mobility systems, as it opens the door to poisoned datasets or malicious code that can compromise safety-critical functions [32]. In the mobility ecosystem, opponents may insert pollutants into traffic datasets or road-sign image collections used to train perception models, leading AgVs to misidentify signs or fail to sense pedestrians [32]. Research has shown that even imperceptible poisoning of deep neural networks (DNNs) in traffic sign identification can severely degrade model accuracy, with attacks diminishing functionality from approximately 99.90% to as low as 10.6% [33]. Additionally, tainted pretrained models obtained from external repositories may conceal stealth access channels activated under distinctive conditions, permitting stealthy rerouting or denial-of-service behaviors within autonomous fleets [33]. Such threats are particularly treacherous because tarnished training data or embedded malware can remain dormant and unnoticed until deployment, possibly triggering calamitous outcomes such as abrupt vehicle braking on highways or misdirecting traffic flows [34]. Subsequently, robust defense mechanisms, which include cryptographic integrity checks, dataset provenance tracking, and continuous model auditing, are essential for maintaining safety and trust in mobility infrastructures [33].

This type of compromise can be practically indistinguishable, exposing downstream systems to illicit behavior like data exfiltration or algorithmic interference. Sensing and mitigating such risks is extremely perplexing, especially when AI models are deployed as hard-to-recognize artifacts (e.g., serialized model files). Without robust validation techniques (i.e., cryptographic integrity checks, sandboxed execution, or behavioral anomaly detection), these vulnerabilities can persist unnoticed and present grave perils to safety-critical systems like autonomous vehicles [34]. Three critiques are relevant here as follows:

Critique 1: Current agentic frameworks fail to provide comprehensive guidance on securing dynamic agentic behaviors, leaving open questions about intent transparency and resilience against adversarial attacks.

Critique 2: The absence of protocols for securing external tool invocation and conversational integrity increases exposure to harmful interactions or data leaks among interconnected AgVs.

Critique 3: Over-reliance on proprietary systems hampers independent review and system-wide explainability, leading to potential regulatory and legal challenges in postincident investigations.

These critiques are significant because they address systemic risks that could undermine public confidence and hinder the societal benefits of agentic mobility. The significance for the research lies in identifying and bridging these gaps through stronger risk monitoring, continuous real-time auditing, and multilevel governance strategies. Addressing these issues ensures that technical advancements in AgVs do not outpace institutional preparedness or ethical oversight.

2.3 Human-centered design in autonomous mobility: Relevance and implications

HCD was initially formalized by Donald A. Norman, a cognitive scientist and usability engineer, in his seminal work The Design of Everyday Things [35, 36]. Norman's work continues to gain prominence as a crucial principle for autonomous mobility systems, striving to align technology with user needs, psychological behaviors, and ergonomic requirements. In the context of AgVs and AEVs, HCD addresses concerns such as comfort, safety, transparency, and inclusivity – elements often overlooked in purely technical frameworks [14]. This approach is highly relevant to society, as it helps overcome adoption barriers and ensures equitable access for diverse user groups.

For this research, HCD provides a multidisciplinary lens to examine how AgVs can transition from static autonomy to adaptive, AgVs that proactively address human interaction, emotional responses, and situational ambiguity. By integrating the user's perspective in design (i.e., through iterative feedback loops, universal interfaces, and participatory development), mobility systems can better foster trust, usability, and social acceptance. However, while HCD offers valuable promise for advancing AgVs [3], critiques highlight significant limitations that must be addressed to ensure its effectiveness across technological, social, and cultural dimensions.

Critique 1: Despite its intent, HCD frameworks sometimes lack specificity in balancing technological capabilities with perceived user experience, leading to gaps in the practical application of inclusivity and comfort [37].

Critique 2: Early deployment of AEVs often overlooks the needs of marginalized or technologically unfamiliar user segments, reinforcing exclusionary practices and limiting broader societal impact [38].

Critique 3: Many models underplay cultural and regional variance in user expectations, potentially reducing relevance and adoption in diverse contexts [39].

These critiques emphasize the essential need for nuanced research methodologies, cross-cultural studies, and iterative user-centered evaluation in AgV and AEV expansion. Strengthening HCD with these elements should allow autonomous mobility systems to progress beyond technical innovations toward socially responsible and ethically grounded infrastructures. This action ensures that progressions in AgVs and AEVs are technologically sound and equitably aligned with the diverse needs of global users.

2.4 Technical limitations in existing agentic mobility systems

Technical limitations in AgVs affect their scalability, vigor, and adaptability to real-world scenarios [3]. Although advancements in machine learning and real-time sensor integration strengthen the capacity for intelligent decision-making, significant technical barriers hamper seamless deployment. Concerns such as operational safety under dynamic traffic conditions, cyber-physical security, and adaptive response in unforeseen events remain unsolved challenges, threatening the reliability and effectiveness of agentic mobility systems [40].

The relevance of these limitations to society is pronounced: unreliable AgV performance could introduce risks of accidents, malfunctions, or adversarial exploitation, negatively influencing public acceptance and regulatory confidence [41]. For researchers, scrutinizing these barriers is vital to constructing more resilient, verifiable, and standardized agentic architectures for future mobility [42].

Three interrelated criteria emerge from current scholarship to evaluate these limitations: behavioral robustness in high-stakes contexts, rigorous verification and validation under diverse operating conditions, and resilience against adversarial manipulation of external data inputs. Behavioral robustness emphasizes the concern that AgVs' learning capabilities and adaptability do not consistently translate into foreseeable, safe performance in emergencies [32]. Verification and validation frameworks remain immature, with simulation-heavy testing struggling to capture the variability of real-world road environments [43]. Finally, the increasing dependence on external data sources, including vehicle-to-everything (V2X) communication and cloud services, exposes AgVs to vulnerabilities such as data poisoning, spoofing, or denial-of-service attacks, demanding coordinated cybersecurity safeguards [44].

Addressing these critiques is significant for policy, research, and industry, safeguarding AgVs to achieve technological advancement and social trust. Doing so necessitates forming rigorous standards for testing and verification that extend beyond simulations to encompass diverse, real-world driving conditions. Equally significant is the development of cross-sector governance frameworks that integrate cybersecurity, ethics, and user inclusion as core pillars of agentic mobility.

2.4.1 Integrating big data analytics and communication protocols

The outlook of human-centered mobility pivots on effective big data analytics and robust communication standards [1]. Modern CCAM systems produce

enormous volumes of sensor data, user feedback, and environmental inputs. Channeling this information through secure, real-time analytics pipelines enables predictive traffic management, dynamic rerouting, and system-wide efficiency improvements [41]. Establishing open, interoperable protocols (i.e., standardized V2X messaging) ensures seamless coordination across heterogeneous fleets and infrastructure networks [36, 37]. Mobility systems can offer adaptability and resilience, all while safeguarding privacy and fostering public trust by embedding data governance and cybersecurity in analytics design. Emphasized here is the indispensable role of transparent data flows and communication in enabling actionable, trustworthy intelligence.

2.4.2 Advancing personalized mobility services

Personalized mobility changes the one-size-fits-all idea, permitting services to adjust proactively to the distinctive needs and preferences of different users [14]. Leveraging machine learning and adaptive interfaces, connected vehicles can respond to individual accessibility needs, foresee routine destinations, or suggest the best travel modes based on real-time context and user history [13]. This type of personalization establishes a more comprehensive, intuitive experience; however, it must be implemented with clear guardrails to protect autonomy, fairness, and user consent. For example, preference-aware routing helps those with limited mobility avoid barriers, while ensuring data sovereignty prevents exploitation or bias. This information highlights the manner in which personalization complements universal design, enhancing usability and social equity, provided it is implemented with ethical rigor.

2.4.3 Emphasizing environmental sustainability and adaptability

CCAM systems must entrench environmental sustainability and contextual adaptability at their nucleus to meet global mobility and climate challenges [3]. Sustainable design principles should give precedence to energy-efficient propulsion, integration with renewable energy infrastructure, and optimization algorithms that minimize emissions and resource use. Equally significant is the capability to flex system operations to the various realities of urban and rural environments: dense cities may require shared electric fleets and congestion-aware routing. On the other hand, rural regions may require adaptable coverage models that ensure inclusion without overextension. Embedding these priorities within the technical limitations and solutions sections will ensure that research recommendations address the full range of operational, social, and ecological needs, enhancing the impact and legitimacy of future mobility proposals.

2.5 Social and ethical critiques of agentic vehicle adoption

As noted by Ranjan et al. [45], deploying AgVs presents pressing ethical and societal dilemmas. Additionally, the capacity of AgVs to make independent, value-sensitive decisions redefines traditional relationships between humans, machines, and public policy. Societal approval of agentic mobility hinges significantly on transparent ethical reasoning, clear accountability measures, and participatory governance that incorporates diverse stakeholder standpoints [45].

This topic is highly relevant, given the potential for value misalignment between AgVs and societal norms, as well as concerns about privacy, surveillance, and data governance. For this research, evaluating these ethical dimensions is essential for guiding policymakers and engineers toward responsible, inclusive development frameworks that anticipate unintended consequences [46]. It is essential to examine three interrelated challenges that currently hinder responsible and inclusive development to critically assess the ethical landscape surrounding AgVs.

Critique 1: Many agentic frameworks do not sufficiently address moral dilemmas or establish protocols for resolving conflicting value judgments, leaving ambiguity in critical scenarios [47].

Critique 2: There is inadequate engagement with public stakeholders in shaping the ethical direction of AgVs, risking alienation or opposition from segments of society [48].

Critique 3: The lack of standardized regulatory frameworks and oversight increases the risk of fragmented, inequitable deployment of agentic technologies, exacerbating social tensions and accountability gaps [49].

These critiques are significant as they pinpoint areas for cross-disciplinary research, participatory governance models, and the formulation of transparent accountability structures in the evolution of agentic mobility. They also highlight the significance of embedding ethical reasoning and human-centric appraisal into technical design processes, ensuring that societal values remain aligned with innovation. By incorporating these dimensions, AgVs can progress toward functional excellence and responsible stewardship of future mobility ecosystems.

3. Research framework

The progression of far-reaching research into human-centered AgVs compels a structured approach that systematically ascertains the core problem, establishes suitable methodological foundations, acknowledges research boundaries, and reveals the originality of the investigation. This section presents an integrated framework that addresses the significant void of validated frameworks and empirical evidence guiding AgV development, deployment, and governance through a qualitative multiple case study design. By investigating the fundamental research problem within the context of methodological assumptions, limitations, and delimitations, this framework determines the foundation for advancing human-centered, ethical, and technically robust CCAM systems. The originality of this research lies in addressing salient gaps in current AV literature, where, regardless of the extensive technical focus on performance and control technologies, inadequate attention has been paid to user-centered and societal factors in intelligent transportation systems.

3.1 Problem statement and justification

There is a salient void of validated frameworks and empirical evidence guiding the development, deployment, and governance of AgVs that reliably address human-centered needs, ethical challenges, technical robustness, and cross-sector trust in real-world connected and autonomous mobility systems. The justification for this problem statement is as follows: the transformation of mobility systems through CCAM, particularly with the emergence of AgVs employing adaptive, context-aware

AI, represents a foundational shift in the interaction between transportation technologies, humans, and infrastructure [3]. Despite these advancements, current frameworks and standards, such as SAE J3016, often remain focused on technical driving performance, ignoring essential dimensions like inclusivity, system interpretability, and ethical reasoning within sociotechnical contexts [14, 35]. A critical gap exists in the empirical verification of AgV performance, trustworthiness, and ethical decision-making during real-world deployment – a concern that complicates regulatory oversight and broad societal acceptance.

This problem is reinforced by fragmented agentic frameworks that suffer from inconsistent regulation, a scarcity of universally accepted digital mobility protocols, and inadequate threat modeling for emergent risks such as adversarial manipulation and data poisoning [26]. Effective implementation of AgVs also requires rigorous system auditing and robust user studies to validate safety, reliability, and public acceptance before widespread deployment [28]. Neglecting these foundational priorities risks reinforcing exclusionary practices in early deployments and alienating marginalized or technologically vulnerable user segments [38].

Furthermore, rising technical limitations include vulnerabilities in security, operational safety under dynamic traffic conditions, and resilience against adversarial manipulation of external data sources [43]. Over-reliance on proprietary systems and lack of continuous, independent auditing threaten accountability, explainability, and effective regulatory response after critical incidents [33]. Social and ethical gaps persist, particularly in engaging diverse stakeholder perspectives and ensuring transparent decision-making in value-sensitive scenarios [45, 48]. For AgVs to realize their full societal potential, research must prioritize developing validated, human-centered, and ethical frameworks that support technological advancement, social trust, and resilient governance in next-generation mobility systems [46].

3.2 Methodology/research design

This research employs a qualitative multiple case study design. This approach enables an in-depth, comparative analysis of how trust, user experience, inclusivity, ethical governance, and technological adaptation unfold across varying CCAM ecosystems, encompassing AgVs, AVs, and AEVs [50]. By deliberately selecting diverse cases (i.e., urban and rural deployments, public and private fleet operations, and technologically advanced versus emerging markets), the research systematically uncovers patterns, context-specific challenges, and best practices that shape trustworthy and resilient mobility futures.

As given by Chiesa et al. [51], the multiple case study design surpasses single-case or purely narrative methods through its capacity to enhance external validity and generate more transferable insights about evolving transportation technologies. Also, it permits systematic exploration of recurring themes, including transparency, accessibility, ergonomic interface design, governance, and public trust, while enabling nuanced cross-comparisons that recognize regional, cultural, and infrastructural variation within CCAM frameworks. This approach is essential for mobility research, given the dynamic interplay among user needs, technological innovation, organizational readiness, and societal acceptance in real-world environments [51].

Alternative designs, such as mixed methods, might offer quantitative perspectives, but the present research's qualitative focus is optimal for achieving a context-rich, detailed understanding of human-centered mobility challenges. Ultimately, the multiple case study design provides a rigorous, adaptive framework for identifying, analyzing, and recommending solutions that address technical and societal concerns. It is ideally suited for generating action-oriented insights that empower researchers, policymakers, and industry leaders to design equitable, secure, and trustworthy mobility ecosystems that respond to diverse user needs and evolving technological opportunities.

3.3 Research assumptions and conceptual foundations

The introductory approach of this research centers on analyzing the assumptions, limitations, and delimitations, emphasizing the growth of human-centered, intelligent transportation systems. Addressing these elements is vital for comprehending how CCAM solutions align with technological capabilities, social needs, and ethical considerations, and for setting precise boundaries for the scope of inquiry. By clearly articulating these aspects, this research clarifies its methodological focus, augments the reliability of its findings, and supports the advancement of equitable and trustworthy AgV ecosystems.

Assumptions in this research include the premise that integrating AgV vehicles into mobility networks will require technological innovation and extensive behavioral, participatory, and ethical analysis to ensure widespread adoption and public trust. The research further assumes that robust multidisciplinary methods can accurately capture user requirements and system performance across diverse contexts, and that regulatory adaptation will evolve in tandem with mobility innovation. These assumptions are necessary because they provide the conceptual framework supporting the interventions and recommendations proposed, ensuring that research outcomes remain practically grounded and relevant to real-world transportation challenges. Building upon these fundamental assumptions about AgV integration and HCD requirements, the conceptual foundations of this research establish the conceptual lens through which human-vehicle interactions, ethical considerations, and sociotechnical systems will be analyzed and understood.

This research adopts the human-centered agentic mobility systems Framework, which integrates HCD, agentic intelligence, and sociotechnical analysis to guide the advancement of CCAM ecosystems [3, 14, 35]. The framework asserts that the evolution from static AVs (AuVs, AVs, AEVs) to social, context-aware AgVs must prioritize not only technological performance but also ethical reasoning, user inclusion, transparency, and iterative stakeholder engagement. By centering on adaptive intelligence and participatory design, the framework fosters the development of mobility systems that can learn from context, reason about user intent, and adjust behaviors dynamically, thus strengthening trust and social acceptance.

The significance of this framework lies in its capacity to bridge gaps routinely found in conventional intelligent transportation paradigms, many of which focus on efficiency and automation but insufficiently address human factors and value-sensitive interactions. Through its holistic approach, the framework elevates the roles of interpretability, ongoing system auditing, and ethical governance, encouraging multidisciplinary research that proactively anticipates risks such as algorithmic bias, data poisoning, and exclusion of marginalized groups [45, 52].

Incorporating these dimensions foregrounds the necessity of co-designing with affected communities, enhancing accessibility and public trust in next-generation mobility technologies.

For this research, the framework is significant because it aligns directly with the chapter's investigation into the limitations and societal challenges of deploying AgVs. It structures the literature review and guides critical analysis of regulatory gaps, empirical insufficiencies, and problematic overemphasis on technical metrics to the detriment of user perspectives and ethical considerations [27, 50, 51]. The framework additionally informs the case study methodology, ensuring that comparisons between system deployments foreground transparency, inclusion, and stakeholder-driven evaluation alongside technical robustness. This approach enables the research to generate practical recommendations for establishing resilient, fair, and trustworthy future mobility systems beyond technologically deterministic perspectives.

However, two notable critiques arise. First, the framework's effectiveness is partially constrained by the limited availability of empirical evidence on real-world human–vehicle interactions, which may slow responsiveness to unforeseen risks or emerging social concerns [25, 53]. Second, while promoting ethical harmonization and user inclusivity, the practical application across regions with divergent social norms and regulatory infrastructures can introduce operational complexity and delayed consensus, creating inertia for policy innovation and system improvement [46, 49]. Addressing these critiques is essential to evolving the framework beyond conceptual integration toward actionable, evidence-based transformation in CCAM research and practice.

3.4 Study limitations and constraints

Limitations are recognized in the current research landscape, notably a lack of comprehensive real-world data validating AgV performance in dynamic environments, alongside insufficiently developed resilience frameworks against emergent cyber-physical threats [53]. Methodological reliance on simulations and modeled interactions may restrict the applicability of results to uncontrolled, real-world settings, while regional disparities in infrastructure and policy further impact the generalizability of findings. Another limitation of this chapter is that, even though it draws on expansive international literature and best-practice proposals, it does not include a specified analysis of recent pilot deployments or empirical postimplementation results. Future research and succeeding editions should incorporate large-scale real-world case studies for further validation. Furthermore, conceivable sources of bias in this qualitative case research comprise restricted data access in certain regions, variability in local stakeholder engagement processes, and the likelihood that rapidly emerging AI or CCAM risks may not be fully captured in the present literature, thereby limiting the generalizability of findings across varied situations and over time. These limitations must be identified to acknowledge constraints on the research's scope, improve transparency, and direct future investigations toward closing empirical, security, and standardization gaps.

3.5 Research delimitations and scope

Delimitations are set to confine the study's analysis to public road users and the intersection of agentic intelligence, HCD, and ethical evaluation, excluding

industrial, military, and legacy transportation systems [52]. The research further restricts its recommendations to democratic and regulatory policy frameworks, focusing on issues of inclusivity, trust, and interoperability within advanced connected mobility environments. Defining these boundaries is vital to maintaining methodological coherence, sharpening the relevance of the findings, and enhancing the practical value of the study for targeted audiences and future research directions.

3.6 Originality of the research

In the last decade alone, more than 70 peer-reviewed studies have systematically analyzed technical advancements and adoption factors for AVs, collectively sampling data from over 32,000 participants and stakeholders to assess performance, communication protocols, and control technologies [54]. Despite this extensive technical focus, literature reviews observe that the bulk of academic output in intelligent transportation systems (e.g., those found in leading journals like IEEE Transactions on Intelligent Transportation Systems) primarily addresses methodologies for sensing, communication, modeling, and algorithmic optimization but pays less attention to user-centered or societal factors [54]. The result is a clear research gap: while technical innovation continues at a rapid pace, authoritative sources recognize the need for greater emphasis on HCD, inclusivity, and the social implications of autonomy in mobility systems [55].

4. Solutions

The future of CCAM requires technical progress and a holistic focus on user trust, interdisciplinary research, and adaptive policy frameworks [3, 14]. Achieving trustworthy and human-centered mobility systems demands actionable strategies that respond directly to the structural critiques discussed in the previous sections [45]. These strategies are vital, given the quickening deployment of CCAM technologies across Europe and North America, where over 341 standards have been published [56]. However, critical gaps remain in areas such as trustworthy AI certification, socio-economic transition planning, and infrastructure harmonization, which directly impact public acceptance and equitable access. Below are prioritized solutions and recommendations spanning governance, technical assurance, inclusivity, ethics, and societal engagement.

Solution 1. **Advance collaborative and transparent governance frameworks**: A central challenge for next-generation mobility is bridging gaps in regulation, data standards, and stakeholder engagement [49]. Current regulatory fragmentation is evidenced by 25 different state-level AV statutes in the United States of America and varying certification requirements across EU member states. Policymakers must harmonize legal frameworks that govern the deployment of AgVs, focusing on common data privacy, auditability, and cybersecurity protocols [46]. This approach should mirror the European CCAM Partnership model, which has successfully grown from 170 to 230 members through effective multistakeholder coordination. Establishing multilateral agencies or public-private councils can unify standards for digital mobility and ensure consistent compliance reviews across jurisdictions [3]. These frameworks should operate through thematic cluster leadership similar to the Open Mobility Foundation's governance structure and include standardized

assessment protocols covering safety performance, algorithmic transparency, and stakeholder impact evaluation. These organizations should require periodic independent auditing of all deployments, with results made transparent to regulators and the public to bolster trust [28]. Success metrics should include the harmonization of 80% of core mobility standards across participating jurisdictions within five years and measurable increases in public trust through regular stakeholder engagement.

Solution 2. Embed robust technical risk management: Emergent risks, such as data poisoning and adversarial attacks on AI modules, must be proactively addressed in all stages of system architecture [32, 33]. These risks have become precarious as CCAM systems shift from controlled testing environments to complex real-world deployments, where traditional validation methods prove inadequate for addressing evolving AI vulnerabilities. Developers and integrators should employ cryptographic verification, continuous dataset provenance tracking, and routine behavioral anomaly detection to secure training data and deployed models [34]. Implementation should be guided by recognized safety assurance frameworks (i.e., the SUNRISE project), which stress scenario-based testing methodologies and hybrid validation methods that combine virtual simulation with real-world testing. Additionally, fleets of AVs should utilize sandboxed model validation and immediate response protocols for suspected security incidents, extending safeguards to V2X communications and cloud infrastructure [44]. These technical safeguards should be integrated with comprehensive verification and validation frameworks that address individual vehicle security and fleet-wide system resilience through coordinated threat intelligence sharing.

Solution 3. Mandate inclusive and universal design across interfaces: Universal accessibility must be treated as a primary standard rather than a secondary consideration [37, 38]. This approach addresses the pressing need identified by accessibility advocates, emphasizing that standards must be instituted before extensive deployment, as retrofitting accessibility features after-market launch proves significantly more costly and less effective than integrated design from the outset. Regulatory policies should require that all user interfaces support multilanguage, multimodal interaction, including voice, tactile, and visual cues, allowing elderly, disabled, or digitally unfamiliar passengers to participate fully [14, 17]. Implementation should comprise very straightforward interfaces that require no instructions, layered interfaces presenting ongoing complexity options, and natural language processing capabilities that accommodate users with accents, nonnative speakers, and those who communicate through sign language. Tech vendors must demonstrably conform to universal design criteria and provide evidence of usability and satisfaction via field studies with diverse populations [18, 19]. Success metrics should include exhibited compliance with established accessibility frameworks, measurable enhancements in user satisfaction across diverse populations, and evidence of diminished barriers to independent mobility for traditionally underserved communities.

Solution 4. Strengthen participatory and empirical human-centered research: Effective solutions require research that is co-designed with the communities they impact [35, 52]. This method should move beyond traditional expert-driven development to embrace citizen engagement methodologies that capture diverse mobility imaginaries and lived experiences, addressing the gap between technological promises and actual community needs. Stakeholder councils,

including persons with disabilities, older adults, and underrepresented regions, should be institutionalized to inform all phases of agentic system development, from requirements gathering to pilot testing [50, 51]. Implementation should apply structured participatory frameworks such as Futures Making Ateliers, collaborative sketching sessions, and narrative analysis workshops that permit participants to envision and critique mobility futures rather than just evaluate predetermined options. Real-world trials and qualitative studies should go beyond technical metrics and document perceptions of safety, transparency, and social value [14, 27]. These feedback loops allow continuous design adaptations and validation of human trust and acceptance [28]. These studies should employ crowdsourced participatory approaches that combine the scale advantages of large participant pools with the depth of co-design methodologies, ensuring that user insights are captured from the earliest creative stages rather than relegated to postdevelopment evaluation. Success necessitates forming systematic processes for translating community input into technical specifications and policy recommendations, with transparent mechanisms for exhibiting how stakeholder contributions directly influence system design and deployment decisions.

Solution 5. Operationalize ethics review and conflict resolution: Public acceptance hinges on the visible presence of ethical reasoning, conflict resolution, and accountability [47, 48]. This action necessitates moving beyond traditional institutional review board models to embrace ongoing operational oversight that addresses the distinctive trials of AI systems making real-time ethical decisions in complex traffic scenarios. Dedicated, independent ethics boards should review major design decisions and system incidents, with the authority to recommend technical and organizational changes [45]. Implementation should draw from established frameworks. These boards must have clear, transparent processes and facilitate communication among technical teams, policymakers, and the communities affected by mobility innovation [46]. These boards must utilize structured ethical decision models that assimilate legal compliance, risk assessment, stakeholder impact evaluation, and continuous monitoring capabilities, with precise mechanisms for translating ethical principles into specific technical requirements and system modifications.

Solution 6. Guarantee user control over personal data: Users should retain meaningful control over their mobility data, with standardized rights to access, correct, or erase personal information [40, 46]. Implementation should align with emerging legislative frameworks (i.e., the Auto Data Privacy and Autonomy Act), which mandate opt-in features for vehicle data collection and prohibit manufacturers from sharing customer data without explicit consent, addressing the current separation between vehicle ownership and data ownership that leaves drivers vulnerable to opaque practices. Transparent opt-out procedures and strong, culturally sensitive privacy policies are essential to prevent misuse, discrimination, or exclusion [38]. Where agentic decisions affect access or outcomes, clear justifications must be communicated, and avenues for user appeal or complaint must be easy to access [31]. Achievement necessitates forming standardized data deletion capabilities that permit users to delete personal information from vehicle infotainment systems, combined with transparent reporting mechanisms that demonstrate compliance with privacy protections and provide users with comprehensible clarifications of how their mobility data affects system decisions and service access.

Solution 7. Incentivize cross-sector collaboration and continuous monitoring: Finally, ongoing cross-disciplinary cooperation between technical experts, social scientists, and users should be incentivized through funding, pilot opportunities, or regulatory sandboxes [45, 50]. Implementation should leverage established models (i.e., Singapore's CETRAN facility), which offer controlled urban testing environments for AVs, and California's comprehensive AV testing program that has facilitated real-world trials for multiple companies while producing critical safety and performance data under regulatory supervision. Longitudinal studies should monitor social equity, real-world safety outcomes, and emerging risks throughout the lifecycle of deployment [42, 53]. These mechanisms ensure solutions remain adaptive as social expectations and technologies evolve [14]. By executing these recommendations, anchored in transparency, safety, inclusivity, and ethical reasoning, researchers, practitioners, and policymakers can address the real and perceived gaps that shape public trust and the equitable adoption of next-generation mobility systems [3, 14]. These studies must employ the World Economic Forum's four-step framework approach that integrates regulatory sandbox development, systematic pilot selection, structured implementation phases, and clear scaling strategies, ensuring that collaborative insights translate effectively from controlled testing environments to widespread deployment scenarios. Success requires establishing multisectoral coordination mechanisms similar to Thailand's Innovation Sandbox model, which addresses cross-regulatory challenges involving road usage, radio frequency management, consumer protection, and data privacy, while incorporating systematic feedback loops that enable continuous refinement of both technical specifications and collaborative governance structures. This multifaceted strategy positions AgVs and intelligent transport ecosystems to achieve not just technical progress, but resilient social legitimacy and lasting benefit.

The comprehensive solutions offered, covering collaborative governance, technical risk management, comprehensive design, participatory research, ethical oversight, data sovereignty, and cross-sector collaboration, collectively address the essential challenges identified in current CCAM deployment and offer actionable lanes toward trustworthy, human-centered mobility systems that prioritize technological excellence and social responsibility. Success in realizing these solutions requires continuous commitment from researchers, policymakers, industry leaders, and communities to work collaboratively across traditional boundaries, ensuring that technological progression serves the diverse needs and values of all users while maintaining robust safeguards for safety, privacy, and equity. By integrating these multifaceted approaches into comprehensive policy frameworks and implementation strategies, the CCAM ecosystem can achieve the transformative potential of AgVs while building the public trust and institutional resilience necessary for widespread, beneficial adoption across diverse social and geographic contexts.

5. Conclusion and recommendations

The evolution of CCAM signals profound shifts in how technology, humans, and infrastructure interact within modern transportation systems [3]. This chapter has explored the essential challenges facing AgVs, AVs, and EVs while offering research priorities that emphasize HCD, ethical reasoning, robust validation, and inclusive deployment [14, 35].

A central conclusion is that advancing mobility futures requires moving beyond solely technical performance toward holistic frameworks that integrate user agency, trust, and social value [27]. Multidisciplinary approaches that unite behavioral analysis, participatory design, and system modeling are essential to ensuring these vehicles are not only safe and efficient but also widely accepted and understood across diverse communities [51]. The significance of empirical evidence from real-world deployment is paramount, as simulation-based testing alone cannot capture the full spectrum of operational, ethical, and experiential variables present in everyday mobility environments [28].

Persistent gaps remain in regulatory harmonization, data governance, and explainability. Addressing these challenges will require institutional collaboration among technologists, policymakers, users, and ethics boards [46, 48]. Transparent auditing, continuous system monitoring, and mechanisms for public feedback should be institutionalized to uphold safety, accountability, and equitable service access [49].

The rapid rise of CCAM is transforming the interface between technology, society, and infrastructure, creating unprecedented opportunities and challenges for mobility research [3, 14]. This chapter emphasizes the need to look beyond technical performance by advancing frameworks that place user agency, inclusivity, and adaptive system validation at the forefront of next-generation transportation systems. Real-world empirical validation must become foundational, as simulation-based metrics are insufficient to capture the full complexity of safety, equity, trust, and user behavior in everyday mobility environments [28].

Persistent gaps in data governance, system auditing, and universal accessibility remain unresolved [46]. These deficiencies highlight the necessity for multidisciplinary collaboration and ongoing stakeholder engagement to build trustworthy and resilient mobility futures [51]. Achieving this transformation will depend on fully integrating transparent regulatory oversight, continuous user feedback mechanisms, and robust ethical stewardship [35]. Noted are five targeted recommendations: advance real-world testing and validation in diverse conditions, institutionalize ethical oversight and participatory governance, strengthen cybersecurity and system resilience, promote cross-sector collaboration and knowledge sharing, and mandate universal and inclusive design principles. Each recommendation offers a concrete pathway to strengthen the design, deployment, and governance of human-centered, trustworthy, connected, and autonomous mobility systems.

5.1 Advance real-world testing and validation in diverse conditions

Empirical, long-term studies must be prioritized to capture how AgVs, AVs, and AEVs perform in uncontrolled environments across urban, suburban, and rural areas. Real-world testing is critical for surfacing unanticipated challenges in safety, user interaction, and system resilience that simulations cannot fully replicate. These efforts are essential to ensure public trust and regulatory confidence, especially among underrepresented user groups [43]. While comprehensive real-world testing provides the empirical foundation for understanding AgV performance across diverse populations and environments, the insights gained from these studies necessitate robust governance structures to ensure that ethical decision-making

processes systematically incorporate stakeholder perspectives and address the societal implications revealed through empirical validation.

5.2 Institutionalize ethical oversight and participatory governance

Future research should develop robust, transparent ethical review structures, ensuring that decisions about system behavior, data use, and conflict resolution reflect the values and rights of all stakeholders. Systematic inclusion of public input, through community consultations and stakeholder panels, will help align technology development with societal expectations and foster broader acceptance. Engaging diverse perspectives is crucial to bridge the gap between technical advancement and social responsibility [47]. The transparent ethical review structures and extensive stakeholder data collection inherent in participatory governance frameworks create new vulnerabilities and attack surfaces that demand comprehensive cybersecurity measures to protect sensitive community input, preserve public trust, and ensure the integrity of ethical decision-making processes within interconnected mobility systems.

5.3 Strengthen cybersecurity and system resilience

As mobility systems become more interconnected, research must prioritize identifying and mitigating emerging security threats, adversarial attacks, and vulnerabilities in supply chains and communications. Proactive scenario-based stress testing and the implementation of multilayered defense mechanisms, such as cryptographic verification and continuous monitoring, will help safeguard critical infrastructures. Coordinated response frameworks involving manufacturers, infrastructure operators, and regulators will further enhance resilience [32]. The coordinated response frameworks essential for cybersecurity resilience, involving manufacturers, infrastructure operators, and regulators, underscore the broader imperative for sustained cross-sector collaboration, as the interconnected nature of security threats demands comprehensive partnerships that extend beyond traditional organizational boundaries to encompass academic, commercial, and civil society stakeholders working collectively toward standardized, globally responsive mobility systems.

5.4 Promote cross-sector collaboration and knowledge-sharing

Advancing future mobility depends on durable partnerships among academic, regulatory, commercial, and civil society organizations. Establishing international consortia and best-practice networks can accelerate the harmonization of standards, reduce policy fragmentation, and support continuous innovation. Cross-sectoral learning ensures that policy and practice remain responsive to global and local developments in technology and society [50]. The diverse stakeholder perspectives brought together through cross-sector collaboration, particularly the inclusion of civil society organizations representing marginalized communities, illuminate the critical significance of embedding universal and inclusive design principles throughout mobility system development, as these collaborative networks provide the essential feedback mechanisms needed to ensure that

technological innovations serve all users equitably from the outset, rather than retrofitting accessibility as an afterthought.

5.5 Mandate universal and inclusive design principles

All interfaces and services in mobility systems should be designed for accessibility and usability, regardless of age, ability, or digital literacy, to maximize societal benefit and equity. Iterative user testing and incorporating feedback from marginalized and diverse groups must become standard practices in the development process. This approach will reduce exclusion and foster adoption by making systems intuitive and valuable for everyone [37].

In conclusion, the future of CCAM depends on an enduring commitment to multidisciplinary research, real-world validation, and inclusive, adaptive governance. As new technologies reshape transportation ecosystems, the test of progress will not be technical sophistication alone but the degree to which these systems earn and sustain public trust, serve the needs of all users, and demonstrate resilience in the face of evolving risks. Achieving this vision requires active collaboration among engineers, policymakers, ethicists, and diverse communities, ensuring that advances in mobility reflect shared values and address societal priorities. By embracing rigorous testing, ethical oversight, robust cybersecurity, cross-sector partnerships, and universal design, the field can move toward mobility solutions that are not only intelligent and efficient but also trustworthy, fair, and human-centered.

6. Future research directions

The evolution of CCAM necessitates a comprehensive research agenda that transcends traditional technical boundaries to address the complex interplay between technological innovation, HCD, and societal integration. While significant progress has been achieved in advancing AEV technologies, critical gaps persist in empirical validation, ethical frameworks, cybersecurity resilience, and inclusive design principles that are essential for realizing the full potential of AgVs and human-centered mobility systems. The rapid advancement of AI and machine learning in transportation contexts demands interdisciplinary research approaches that systematically integrate user experience, behavioral analysis, and participatory governance to ensure that emerging mobility technologies serve diverse populations equitably and sustainably. Future research must prioritize real-world validation studies, strengthen ethical oversight mechanisms, enhance cybersecurity frameworks, foster cross-sector collaboration, and mandate universal design principles to bridge the critical gap between technological capability and societal acceptance, ultimately ensuring that CCAM systems are not only technically sophisticated but also trustworthy, inclusive, and responsive to the lived realities of all users.

6.1 Real-world validation and testing

There is a pressing need for longitudinal studies and diverse pilot deployments to gather empirical data on AgVs and AEVs in uncontrolled, everyday traffic

environments [42, 43]. This action includes collecting feedback from marginalized user groups, older adults, and those with disabilities to ensure universal design principles are realized in practice [37]. Such inclusive, iterative testing frameworks can help identify context-specific safety, accessibility, and ethical challenges that may otherwise be overlooked in controlled research settings.

6.2 Ethics, explainability, and governance

Research should further develop transparent protocols for resolving moral dilemmas during autonomous decision-making and foster inclusive engagement with public stakeholders in the shaping of ethical frameworks [45, 47]. Interdisciplinary studies should elucidate how value alignment, privacy rights, and data governance affect perceptions of fairness and trust [46, 48]. Additionally, comparative policy analyses across regions can enlighten the manner in which cultural norms and regulatory traditions mediate societal acceptance of autonomous mobility systems.

6.3 Cybersecurity and resilience

As mobility systems become increasingly interconnected, continuous research must address emergent security risks, supply chain vulnerabilities, and adversarial threats to AI models and V2X communications [32, 44]. Robust resilience strategies will require technical safeguards and coordinated governance mechanisms that span manufacturers, infrastructure operators, and policymakers [57]. Furthermore, proactive scenario-based stress testing can help anticipate cascading failures and bolster public confidence in the reliability of next-generation mobility networks.

6.4 Cross-sector collaboration

Advancement depends on sustained cooperation among academic, commercial, regulatory, and civil society organizations. Future investigations should explore best practices for participatory governance, cross-sector risk assessment, and adaptive policy frameworks [50, 51]. Equally significant is the establishment of international knowledge-sharing consortia that can harmonize standards, accelerate innovation, and prevent fragmented regulatory approaches [58].

Ultimately, the promise of trustworthy, resilient, and equitable mobility will only be realized through ongoing, multidisciplinary, and iterative research, grounded in empirical validation and responsive to the lived realities of all users. This systemic integration of technical innovation, HCD, and ethical stewardship should remain the guiding blueprint for scholars, practitioners, and policymakers moving forward [3, 14, 35]. Four future recommendations are provided above, along with explanations for why they are given.

DOI: http://dx.doi.org/10.5772/intechopen.1013697

Author details

Sharon L. Burton
Embry-Riddle Aeronautical University, Daytona Beach, FL, USA

*Address all correspondence to: Burtons6@erau.edu

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] Chen D, Dong J, Lee H.Vehicle Connectivity and automation: A sibling relationship. Frontiers in Built Environment. 2020;**6**(590036). DOI: 10.3389/fbuil.2020.590036

[2] Shinde O, Eskandarian A SD-SORT-self driving sort for autonomous vehicle. In Proceedings of the International Conference on Pattern Recognition (pp.196–210), 2025

[3] Yu J From autonomy to agency: Agentic vehicles for human-centered mobility systems. (2025). arXiv preprint arXiv:2507.04996.

[4] Yu J, Frank R, Miranda-Moreno L, Jafarnejad S, Manzolli JA. From Autonomy to Agency: Agentic Vehicles for Human-centered Mobility Systems. Cornell University; 2026. p. 1–8. Available from: https://arxiv.org/pdf/2507.04996

[5] Garikapati D, Shetiya SS. Autonomous vehicles: Evolution of artificial intelligence and the current industry landscape. Big Data and Cognitive Computing. 2024;**8**(4):42. DOI: 10.3390/bdcc8040042

[6] Litman T (2022). Autonomous vehicle implementation predictions. Victoria Transport Policy Institute. Available from: https://www.vtpi.org/avip.pdf [Accessed: 2025-November-18]

[7] U.S. Department of Transportation National Highway Traffic Safety Administratoin. (2008). National motor vehicle crash causation survey: Methodology and findings. NHTSA Technical Report. Author. Available from: https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/811059 [Accessed: 2025-November-19]

[8] Craig Schlenoff CL, Prem Rachakonda S, N. V, Zhang T, Aboul-Enein O, Barbosa N, Miller C, Sawyer D, Virts A (2022). National Institute of Standards and Technology (NIST) – workshop report: Standards and performance metrics for on-road autonomous vehicles. NIST Internal Report NIST IR 8442. Available from: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8442.pdf [Accessed: 2025-November-19]

[9] Atakishiyev S, Salameh M, Yao H, Goebel R (2012). Explainable artificial intelligence for autonomous driving: An overview. arXiv preprint. Available from: https://arxiv.org/pdf/2112.11561v2

[10] Schlenoff C, Lightman S, Nguyen V, Rachakonda P. Standards and Performance Metrics for On-road Autonomous Vehicles. Gaithersburg: National Institute of Standards and Technology; 2022. NIST Internal Report NIST IR 8442. DOI: 10.6028/NIST.IR.8442 [Accessed: 2025-November-19]

[11] Yu J (2025). From autonomy to agency: Agentic vehicles for human-centered mobility systems. arXiv preprint arXiv, 2507. Available from: https://arxiv.org/pdf/2507.04996

[12] Bissell D, Birtchnell T, Elliott A, Hsu EL. Autonomous automobilities: The social impacts of driverless vehicles. Current Sociology. 2020;**68**(1):116–134. DOI: 10.1177/0011392118816743

[13] Li C, Ma Y, Cao X, Ye W, Zhou Y, Liang K, Chen J, Lu J, Yang Z, Liao K, Gao T, Tang K, Cao J, Zheng C A survey on multimodal large language models for autonomous driving. In Proceedings

of the IEEE/CVF Winter Conference on Applications of Computer Vision. IEEE; 2025. p. 958–979)

[14] Giri R, Neeraja B, Alhamad AM, Mamidi PL, Somasundaram R, Boopathi S. Human-centered design approach to autonomous electric vehicles: Revolutionizing mobility. In: Mohammed C, editor. Human-Centered Design for Mobility Systems. Hershey: IGI Global; 2024. DOI: 10.4018/979-8-3693-1862-1.ch006

[15] Muhammad AP Bridging Worlds: Integrating Human Factors in Agile Automated Vehicle Development. Doctoral dissertation Chalmers University of Technology & University of Gothenburg. Department of Computer Science & Engineering, Division of Interaction Design and Software Engineering. (2025)

[16] Walker F, Forster Y, Hergeth S, Kraus J, Payre W, Wintersberger P, Martens M. Trust in automated vehicles: Constructs, psychological processes, and assessment. Frontiers in Psychology. 2023;**14**:1279271. DOI: 10.3389/fpsyg.2023.1279271

[17] Sharma RE. Accessibility remains an overlooked priority. Magic EdTech. 2024. Available from: https://www.magicedtech.com/blogs/entering-2024-accessibility-remains-an-overlooked-priority/ [Accessed: 2025-November-19]

[18] Leo M, Tan F, Miao T, Anand G. From threat to trust: Assessing security risks of agentic AI systems. International Journal of Information Security. 2026;**25**:23. DOI: 10.1007/s10207-025-01185-y

[19] Zhang Q, Yang XJ, Robert LP. Individual differences and expectations of automated vehicles. International Journal of Human–Computer Interaction. 2022;**38**(9):825–836. DOI: 10.1080/10447318.2021.1970431

[20] Shukla M. Adaptive monitoring and real-world evaluation of agentic AI systems. AI Ethics. 2026;**6**(129):1–10. DOI: 10.1007/s43681-026-00990-y

[21] Atf Z, Lewis PR Is trust correlated with explainability in AI? A meta-analysis. arXiv preprint; 2024. Available from: https://arxiv.org/pdf/2504.12529

[22] Chen Z, Xu Y Engaging with AI: How interface design shapes human-AI collaboration in high-stakes decision-making. arXiv preprint; 2025. DOI: 10.48550/arXiv.2501.16627

[23] Lengkong A, Liu Q, Shi X, Jiang R, Zhang H, Lu L, Shibasaki R. Modeling interpretable social interactions for pedestrian trajectory. Transportation Research. Part C, Emerging Technologies. 2024;**162**:104617. DOI: 10.1016/j.trc.2024.104617

[24] Ajao Q, Sadeeq L (2024). Modeling and simulation of a fully Autonomous Electric Vehicle (AEV). arXiv preprint arXiv:2409.11641

[25] Vaishnavi P. Emergent behaviors in large-scale multi-agent systems: A study of unpredictable phenomena in distributed AI networks. International Journal of Research Publication and Reviews. 2024;**5**(1):5707–5714. Available from: https://ijrpr.com/uploads/V5ISSUE1/IJRPR22235.pdf [Accessed: 2025-November-19]

[26] Cloud Security Alliance. Agentic AI Threat Modeling Framework: MAESTRO. Cloud Security Alliance;

2025. Available from: https://cloudsecuritytalliance.org/blog/2025/02/06/agentic-ai-threat-modeling-framework-maestro# [Accessed: 2025-November-19]

[27] Yang Y, Kim M-Y. Promoting sustainable transportation: how people trust and accept autonomous vehicles—focusing on the different levels of collaboration between human drivers and artificial intelligence—an empirical study with partial least squares structural equation modeling and multi-group analysis. Sustainability. 2024;**17**(1):125. DOI: 10.3390/su17010125

[28] Gros C, Werkhoven P, Kester L, Martens M. A methodology for ethical decision-making in automated vehicles. AI & Society. 2025. DOI: 10.1007/s00146-025-02370-2

[29] Silva P. Revolutionizing safety and security with agentic AI. Security Industry Association. 2025. Available from: https://www.securityindustry.org/2025/04/25/revolutionizing-safety-and-security-with-agentic-ai/ [Accessed: 2025-November-19]

[30] Deering J, Black R, Christensen R. Agentic misalignment: When AI becomes the insider threat. DLA Piper. 2025. Available from: https://www.dlapiper.com/en-gb/insights/publications/2025/08/agentic-misalignment-when-ai-becomes-the-insider-threat [Accessed: 2025-November-20]

[31] Nandagopal S. Explainability in agentic AI: A conceptual framework for balancing interpretability, security, and performance. World Journal of Engineering Research and Technology. 2025;**11**(1):60–88. Available from: https://www.wjert.org/admin/assets/article_issue/85122024/1735637610.pdf [Accessed: 2026-March-03]

[32] Wang F, Wang X, Xuegang B. Data Poisoning Attacks in Intelligent Transportation Systems: A Survey. arXiv. 2024. Available from: https://arxiv.org/pdf/2407.15855 [Accessed: 2025-November-19]

[33] Hapuarachchi T, Dang L, Xiong K. Securing Traffic Sign Recognition Systems in Autonomous Vehicles. ArXiv. 2025. Available from: https://arxiv.org/abs/2506.06563 [Accessed: 2025-November-19]

[34] Patel N, Krishnamurthy P, Garg S, Khorrami F. Bait and Switch: Online Training Data Poisoning of Autonomous Driving Systems. ArXiv. 2020. https://arxiv.org/abs/2011.04065 [Accessed: 2025-November-19]

[35] Norman DA. The Design of Everyday Things. Revised and expanded ed. Basic Books; 2013 [Accessed: 2025-November-20]

[36] Norman DA. The Design of Everyday Things. Revised and expanded ed. Basic Books; 1988 [Accessed: 2025-November-20]

[37] Attaianese E, Tosi F, Steffan IT From accessibility to inclusion in people-centered design. In Proceedings of the 21st Congress of the International Ergonomics Association. Springer; 2021. p. 357–366. Available from: https://link.springer.com/chapter/10.1007/978-3-030-74605-6_45 [Accessed: 2025-November-20]

[38] Borah A, Bansal G, O'Neill J. Agentic AI ecosystems: Navigating cultural-awareness, biases and misinformation in multi-agent and human-agent interactions. Microsoft Research. 2025. Available from: https://www.microsoft.com/en-us/research/video/agentic-ai-ecosystems-navigating-

cultural-awareness-biases-and-misinformation-in-multi-agent-and-human-agent-interactions/ [Accessed: 2025-November-20]

[39] Dave A. From UX to AX: The future of agentic experiences in the age of AI. Forbes Technology Council. 2025. Available from: https://www.forbes.com/councils/forbestechcouncil/2025/07/10/from-ux-to-ax-the-future-of-agentic-experiences-in-the-age-of-ai/ [Accessed: 2025-November-20]

[40] Dey V How tech giants are reinventing cybersecurity for the AI agent era. Forbes. (2025). Available from: https://www.forbes.com/sites/victordey/2025/08/06/how-tech-giants-are-reinventing-cybersecurity-for-the-ai-agent-era [Accessed: 2025-November-20]

[41] Sankaran N. Architectural evolution of software-defined vehicles: AI/ML-driven models for intelligent mobility. World Journal of Advanced Research and Reviews. 2020;**6**(2): 256–274. DOI: 10.30574/wjarr.2020.6.2.0101

[42] Escuela G, Dannebaum U, Rosenbusch J, et al. Safe automated driving: Requirements and architectures: Full report. The Autonomous Working Group on Safety & Architecture. (2023). Available from: https://www.the-autonomous.com/wp-content/uploads/2023/12/wg-safetyarchitecture-full-report.pdf [Accessed: 2025-November-20]

[43] Alemayehu H, Sargolzaei A. Testing and Verification of Connected and Autonomous Vehicles: A Review. Electronics. 2025;**14**(3):600. DOI: 10.3390/electronics14030600

[44] Durlik I, Miller T, Kostecka E, Zwierzewicz Z, Łobodzińska A. Cybersecurity in autonomous vehicles—are we ready for the challenge? Electronics. 2024;**13**(13):2654. DOI: 10.3390/electronics13132654

[45] Ranjan R, Gupta S, Singh SN Fairness in Agentic AI: A Unified Framework for Ethical and Equitable Multi-agent Systems. arXiv. (2024). Available from: https://arxiv.org/pdf/2502.07254 [Accessed: 2025-November-20]

[46] Farooq I Data governance: The contract layer that makes agentic systems possible. VentureBeat. 2025). Available from: https://venturebeat.com/ai/data-governance-the-contract-layer-that-makes-agentic-systems-possible [Accesses: 2025-November-20]

[47] Cecchini D, Brantley S, Dubljević V. Moral judgment in realistic traffic scenarios: Moving beyond the trolley paradigm for ethics of autonomous vehicles. AI & Society. 2025;**40**:1037–1048. Available from: https://link.springer.com/article/10.1007/s00146-023-01813-y [Accesses: 2025-November-20]

[48] Gabriel I, Keeling G, Manzini A, Evans J. We need a new ethics for a world of AI agents. Nature. 2025;**644**:38–40. Available from: https://www.nature.com/articles/d41586-025-02454-5 [Accessed: 2025-November-20]

[49] Dworkin O, Ortiz J, Xenakis N. Regulatory frameworks for smart mobility: Current U.S. regulation of connected and automated vehicles and the road ahead. Journal of Law and Mobility. 2024. Available from: https://lawandmobilityjournal.org/articles/regulatory-frameworks-for-smart-mobility [Accessed: 2025-November-21]

[50] Antonakopoulou A, Ballis C, Liazos A, Sioutis J D2.2 Study questions and KPIs of CCAM ecosystem (Deliverable No. D2.2). IN2CCAM. (2023). Available from: https://in2ccam.eu/wp-content/uploads/2024/05/D2.2_Study-questions-and-KPIs-of-CCAM-ecosystem.pdf [Accessed: 2025-November-20]

[51] Chiesa S, Irrera D, Aguzzi S. Acceptability and Inclusivity of CCAM: What strategies and methods should be used to engage stakeholders? In: Duffy VG, Krömker HA, Streitz N, Konomi S, editors. HCI International 2023: Late Breaking Papers. Cham: Springer; 2023. p. 264–276. Available from: https://link.springer.com/chapter/10.1007/978-3-031-48047-8_17 [Accessed: 2025-November-20]

[52] Desolda G, Esposito A, Lanzilotti R, Piccinno A Designing and evaluating human-centred AI systems: Best-practices from a multidisciplinary view. Joint Proceedings of the ACM IUI Workshops. (2025). Available from: https://ceur-ws.org/Vol-3957/BEHAVEAI-paper05.pdf [Accessed: 2025-November-20]

[53] Segovia-Ferreira M, Rubio-Hernan J, Cavalli AR, Garcia-Alfaro J. A survey on cyber-resilience approaches for cyber-physical systems. ACM Digital Library. 2024. DOI: 10.1145/3652953

[54] Alsabaan M, Alsharif MH, Alghamdi T, Alzahrani A. Factors affecting autonomous vehicles adoption: A systematic review, proposed framework, and future roadmap. International Journal of Human–Computer Interaction. 2024;**40** (24):8397–8418. DOI: 10.1080/10447318.2023.2286089

[55] van Nes N A human-centred design approach to self-driving vehicles. Delft Design Stories, TU Delft. 2025. Available from: https://www.tudelft.nl/en/ide/delft-design-stories/a-human-centred-design-approach-to-self-driving-vehicles [Accessed: 2025-November-20]

[56] CCAM Association. 2025. Launch of the integrated CCAM technologies cluster. Author. Available from: https://www.ccam.eu/launch-of-the-integrated-ccam-technologies-cluster/ [Accessed: 2025-November-21]

[57] Organisation for Economic Co-operation and development (OECD). (2021). Building resilience: New strategies for strengthening infrastructure resilience and maintenance. OECD Public Governance Policy Papers No. 5. OECD Publishing. DOI: 10.1787/354aa2aa-en

[58] European Commission. The Global approach to research and innovation: Europe's strategy for international cooperation in a changing world (COM/2021/252 final). Author. 2021. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0252 [Accessed: 2025-November-21]

Chapter 11

Impacts of Autonomous Vehicles in a Mixed Roadway Environment: A Diamond Interchange Case Study

Khaled Hamad and Mohamad Tulimat

Abstract

This chapter examines the impacts of autonomous vehicles (AVs) on traffic operations, safety, and environmental outcomes in a mixed roadway environment where freeway and arterial flows interact. Unlike prior studies focusing exclusively on freeway or arterial settings, this research evaluates a diamond interchange, representing a mixed context where uninterrupted freeway traffic interfaces with signalized arterial operations. Using microscopic traffic simulation, surrogate safety assessment, and emissions modeling, results indicate that AV penetration yields significant benefits in congestion reduction, queue management, and conflict frequency reduction, with moderate environmental improvements. The findings underscore the importance of analyzing AVs in mixed networks to inform policy and infrastructure planning.

Keywords: autonomous vehicles, mixed roadway environment, freeway–arterial interactions, surrogate safety, emissions, simulation, diamond interchange

1. Introduction

Autonomous vehicles (AVs) are widely expected to reshape the future of transportation by improving safety, efficiency, and sustainability. The anticipated benefits of AVs are grounded in their ability to reduce human error, optimize vehicle control, and enable cooperative driving strategies [1]. While a growing body of research has investigated the performance of AVs across different roadway environments, a key limitation of much of this work is its focus on homogeneous settings – either uninterrupted freeway segments or signalized arterial corridors.

Some of the most critical bottlenecks in transportation systems are found in mixed roadway environments, where freeways and arterials intersect. A prominent example is the diamond interchange, which connects high-speed freeway traffic to signalized arterials through ramp terminals. This configuration introduces both uninterrupted freeway flows and interrupted, signal-controlled arterial flows within

a small geographic area, resulting in intense operational complexity. Interchanges of this type are not only common but also prone to congestion, delays, and crash risks.

Existing studies have provided important insights into AV performance; however, most fail to address this specific context. Freeway studies emphasize the impacts of AVs on flow stability and capacity [2–6], while arterial studies highlight potential improvements in signal coordination and queue management [7–9]. However, few have examined environments where freeway merges and diverges are directly coupled with signalized intersections. This gap is particularly significant because interchanges often act as system bottlenecks, limiting the effectiveness of network-wide improvements.

This chapter addresses the gap by focusing on the impacts of AV penetration in a diamond interchange environment. Using microscopic traffic simulation (VISSIM), surrogate safety assessment (SSAM), and emissions modeling (MOVES), the study evaluates traffic operations, safety, and environmental outcomes under varying demand levels and AV penetration rates. Unlike prior research, this analysis captures the combined effects of freeway and arterial dynamics, providing new insights into AV deployment in real-world mixed environments.

The remainder of the chapter is organized as follows. Section 2 reviews the literature on AV impacts across freeway, arterial, and mixed contexts. Section 3 describes the methodology, including network design, demand scenarios, and evaluation methods. Section 4 presents results across traffic operations, safety, and environmental dimensions. Section 5 discusses implications for policy and practice, and Section 6 concludes with key findings and directions for future research.

2. Literature review

2.1 Traffic operations in freeway settings

Freeways have been the primary focus of AV research, largely because uninterrupted flow conditions simplify modeling. Numerous simulation studies have demonstrated that AVs can enhance roadway capacity, mitigate stop-and-go oscillations, and stabilize traffic flow [2–6]. For example, Talebpour and Mahmassani [2] demonstrated that connected and automated vehicles enhance flow stability, particularly at moderate to high penetration levels. Chen et al. [3] formulated roadway capacity for mixed traffic, showing that even partial AV penetration can increase throughput, although the magnitude depends on lane management and demand.

Experimental studies further confirm the stabilizing influence of AVs. Stern et al. [4] conducted field tests, showing that a single automated vehicle in a platoon could dissipate stop-and-go waves. Similarly, Milanes and Shladover [6] modeled cooperative adaptive cruise control (CACC) using empirical data, finding smoother dynamic responses and improved capacity.

Despite these encouraging results, some research has identified transitional challenges. Interactions between AVs and conventional vehicles at low penetration rates may reduce efficiency or destabilize flow [5, 10]. In general, capacity benefits become most visible when penetration exceeds 40–50% [3]. Moreover, freeway-focused studies often neglect signalized intersections, thereby limiting their relevance to urban settings.

2.2 Traffic operations in arterial settings

Although less abundant, arterial-focused studies suggest that AVs can improve performance at signalized intersections. Islam and Hajbabaie [7] demonstrated that connected and automated vehicles, integrated with adaptive signal control, can significantly reduce delays and stops. Lee and Park [8] proposed a cooperative vehicle-intersection control algorithm, showing improvements in throughput and reduced lost time.

Environmental benefits have also been highlighted in arterial settings. Zhao et al. [9] showed that cooperative eco-driving strategies at signalized intersections can reduce fuel consumption by smoothing vehicle acceleration and deceleration profiles.

Nonetheless, challenges remain. Heterogeneous traffic with low AV penetration may exacerbate delays, as conventional drivers fail to benefit from the coordination of AVs. Arterials also introduce variability from pedestrian crossings, turning movements, and signal phasing, complicating the transfer of freeway-based findings.

2.3 Mixed roadway environments

Mixed roadway environments combine elements of freeways and arterials, creating unique operational challenges. Interchanges, where freeway ramps connect to signalized intersections, are particularly important because they concentrate congestion and crash risk within localized areas. Despite this, most AV research isolates freeways or arterials, leaving mixed contexts underexplored.

Some recent work has begun to address this gap. Hamad and Alozi [11] examined shared versus dedicated lanes for AV deployment, finding that lane management strategies can significantly influence system-level outcomes. However, their analysis did not extend to full interchange environments. Comprehensive evaluations that consider the combined effects of merges, diverges, and signalized intersections remain scarce, despite their importance in real-world networks.

2.4 Safety implications of AVs

Safety is frequently cited as the most important motivation for AV deployment, since human error accounts for more than 90% of crashes [1]. Surrogate safety measures, particularly time-to-collision (TTC) and post-encroachment time (PET), are widely used in simulation-based AV studies [12]. Results consistently show reductions in rear-end and lane-changing conflicts as AV penetration rises, reflecting smoother and more cooperative driving behavior [2, 5, 12].

Nevertheless, safety improvements vary depending on the context. Freeway studies highlight reductions in rear-end collisions [2, 12], while arterial studies emphasize crossing and turning conflicts at intersections [7, 8]. Mixed settings, where merging and signal-related conflicts coexist, remain largely unexamined.

2.5 Environmental impacts of AVs

The environmental impacts of AVs have also attracted attention. By enabling smoother driving and reducing stop-and-go cycles, AVs can lower energy consumption and emissions [13–15]. Zhou et al. [13] demonstrated that vehicle

emission estimation integrated with traffic simulation provides valuable insights into sustainable traffic management. Vahidi and Sciarretta [14] observed that increased roadway capacity from AVs could induce additional travel demand, potentially offsetting environmental benefits. Hoogendoorn et al. [15] similarly cautioned that efficiency improvements may be partially negated by induced demand. Importantly, few analyses examine mixed networks, where emissions result from both freeway cruising and arterial idling.

2.6 Research gaps and contribution

The literature reveals three main gaps. First, most AV studies focus exclusively on freeways or arterials, neglecting mixed settings like interchanges that combine both operational types [16]. Second, surrogate safety analyses rarely consider environments with overlapping merge and signal conflicts [8, 12]. Third, environmental impacts in mixed environments remain largely unexplored [9, 13].

This chapter addresses these gaps by analyzing a diamond interchange using an integrated methodology. Evaluating operations, safety, and environmental outcomes under varying AV penetration levels provides novel insights into how AVs influence performance in complex, real-world traffic environments.

3. Methodology

This study employed a simulation-based approach to evaluate the impacts of autonomous vehicles (AVs) on traffic operations, safety, and environmental outcomes within a diamond interchange. The methodology consisted of five main steps: (1) defining the study network and scenarios, (2) specifying vehicle behavior for conventional vehicles and AVs, (3) conducting microscopic traffic simulations, (4) evaluating surrogate safety performance, and (5) estimating emissions. Each component was designed to ensure realism, consistency with prior research, and comparability across scenarios.

3.1 Study network

The analysis focused on a prototypical diamond interchange, which was selected because it represents a common form of freeway–arterial interface in North America and internationally. Diamond interchanges create operational challenges, as freeway traffic merges onto arterials through ramp terminals controlled by signals. This introduces interactions between uninterrupted freeway flows and interrupted arterial flows, which makes them ideal testbeds for studying mixed roadway environments.

The geometry of the interchange was based on standard configurations outlined in the Highway Capacity Manual (HCM) [16]. The modeled network (**Figure 1**) included:

- Two freeway mainline segments (upstream and downstream of the interchange), with four travel lanes per direction and operational speeds of 120 km/h for light vehicles (LVs) and 80 km/h for heavy goods vehicles (HGVs).

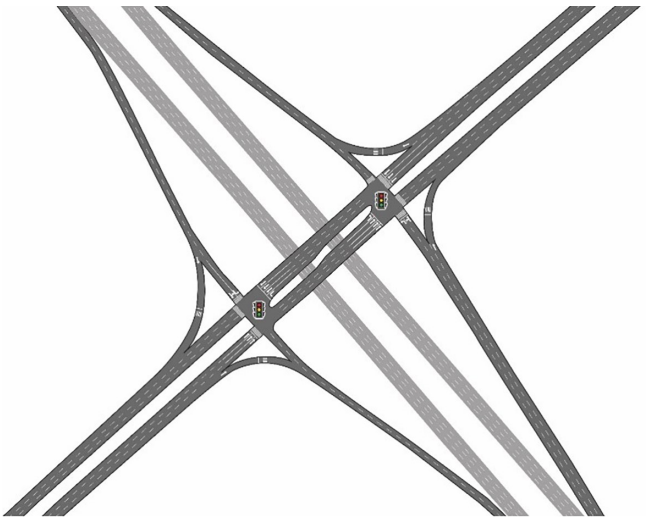


Figure 1.
The modeled network of a diamond interchange.

- An arterial corridor with two signalized intersections at the ramp terminals, featuring three travel lanes per direction and operational speeds of 80 km/h for LVs and 60 km/h for HGVs.

- Four ramps: Two off-ramps connecting the freeway to the arterial, and two on-ramps connecting the arterial to the freeway. All ramps were assumed to have two travel lanes each.

Lane numbers, lengths, and signal timings were consistent with typical urban freeway interchanges. Although site-specific calibration was not the primary goal, the configuration was chosen to be representative of interchanges that experience recurrent congestion during peak periods.

3.2 Scenarios considered

To capture a wide range of operating conditions, simulations were conducted across three traffic demand levels:

1. Low traffic volumes (under-saturated), which correspond to LOS C (V/C = 0.7).

2. Medium traffic volumes (at-capacity), which correspond to LOS E (V/C = 1).

3. High traffic volumes (over-saturated), which correspond to LOS F (V/C = 1.2).

To estimate traffic demands for each of these demand levels, saturation flow rates of 2,200, 1,900, and 1,500 vehicles/hour/lane were assumed for the freeway segment, through movement at a signalized intersection, and left movement at a signalized intersection, respectively. The lane utilization factor for signalized

intersection lanes was assumed to be 0.95, and a fixed cycle length of 100 seconds was used with optimized green times. Traffic was assumed to be composed of 95% LVs and 5% HGVs.

Each demand level was evaluated under six AV penetration rates: 0% (No AVs), 20%, 40%, 60%, 80%, and 100% (All AVs). This produced a total of 18 scenarios (3 demand levels × 6 penetration rates), ensuring coverage of uncongested, moderately congested, and severely congested conditions. By systematically combining demand and AV penetration, the analysis isolated the incremental contribution of automation to performance under varied traffic states. Each scenario was simulated for one hour, with 15-minute warm-up and cool-down intervals, and replicated five times to account for stochastic variation.

3.3 Simulation platform and vehicle behavior parameters

Traffic conditions were simulated in PTV Vissim 2023, enabling the integrated modeling of freeway and arterial operations. Key differences in driver behavior between conventional vehicles and AVs were represented through parameter settings in PTV Vissim. As illustrated in **Table 1**, AVs were modeled with shorter reaction times (0.6 s vs. 1.2 s), smaller desired headways (0.9 s vs. 1.5 s), and smoother acceleration/deceleration values compared with human drivers. Cooperative lane-changing behavior was also implemented, reflecting findings from prior research [5, 6, 10].

These parameters capture the smoother, more coordinated movement of AVs, while remaining consistent with empirical studies and simulation practice.

3.4 Calibration and validation

Since this study is not site-specific, direct validation of the simulation model using local traffic data was not required. This offers greater flexibility in generalizing the findings to a broader range of freeway contexts. However, to enhance the credibility of the results and improve confidence in the model's ability to realistically capture AV impacts, a structured calibration and internal validation process was implemented. This approach builds on prior microsimulation studies conducted in the UAE context, which investigated the impacts of connected and automated vehicles on traffic operations at freeway and interchange facilities [17, 18].

The calibration process consisted of two main stages.

Parameter	Conventional vehicles	AVs	Source
Reaction time (s)	1.2	0.6	[5, 6]
Desired headway (s)	1.5	0.9	[6, 10]
Max acceleration (m/s^2)	2.5	2.0	[10]
Max deceleration (m/s^2)	4.0	3.0	[5]

Table 1.
Comparison of vehicle behavior parameters for conventional vehicles and AVs.

In the first stage, key driver behavior parameters were tuned to reflect realistic human and AV interactions. These included desired time headway, reaction time, standstill distance, car-following sensitivity, and lane-change aggressiveness. AV parameters were set based on established values reported in the literature [1–4, 6, 10], representing smoother following behavior and lower reaction times compared to human-driven vehicles.

In the second stage, traffic demand was calibrated to align with target volume-to-capacity (v/c) ratios corresponding to specific Levels of Service (LOS) as defined by the Highway Capacity Manual [16]. The baseline scenario (0% MPR) was first used to determine freeway capacity per lane, which then served as the reference point for computing volumes for each LOS. These calibrated volumes were applied consistently across all mixed penetration rate (MPR) scenarios to ensure comparability.

Calibration performance was assessed by comparing simulated average delays and queue lengths against HCM reference values, ensuring deviations remained within an acceptable tolerance (typically ± 10%), consistent with standard microsimulation practice. Additionally, multiple replications were run for each scenario to minimize the effects of stochastic variability.

Although no external field data were used, this two-stage calibration procedure – supported by standardized capacity relationships, established AV behavior parameters, and replicated simulations – functions as an internal validation mechanism. This ensures that the model reproduces operational patterns consistent with theoretical and empirical benchmarks, thereby increasing confidence in the robustness of the simulated AV impact.

3.5 Safety evaluation

Safety performance was assessed using surrogate safety measures derived from vehicle trajectory data. Specifically, simulations were exported from Vissim to the Surrogate Safety Assessment Model (SSAM) developed by the U.S. Federal Highway Administration [19].

Two widely used indicators were employed:

1. Time-to-Collision (TTC) is the time remaining before two vehicles collide if they continue at their current speed and trajectory. Conflicts with TTC <1.5 s were flagged as critical [19].

2. Post-Encroachment Time (PET) is the time between a vehicle leaving a potential conflict point and another vehicle arriving at the same point. PET <5.0 s was flagged as critical [19].

These thresholds are consistent with prior AV safety studies [7, 12] and reflect the potential likelihood of crashes. Conflict types (rear-end, lane-changing, crossing) were also classified to distinguish between freeway and arterial effects.

3.6 Environmental evaluation

Environmental impacts were estimated by combining simulated vehicle trajectories with the U.S. EPA's MOVES (Motor Vehicle Emission Simulator). This approach has been widely used in prior work on AVs and emissions [9, 13].

Key pollutants included:

1. Carbon dioxide (CO_2): As a measure of greenhouse gas emissions.
2. Nitrogen oxides (NOx): As indicators of air quality impacts.
3. Fuel consumption: As a proxy for energy efficiency.

Trajectory-level data from Vissim captured vehicle speeds and accelerations, which were then aggregated in MOVES to estimate emissions under each scenario. By comparing results across AV penetration levels, the analysis quantified both absolute and relative improvements.

4. Results and findings

The simulation results are presented in three dimensions: traffic operations, safety outcomes, and environmental impacts. Each set of findings is discussed in relation to AV penetration levels and traffic demand scenarios. Where appropriate, results are compared with prior studies to highlight similarities, differences, and the unique contribution of this research in the mixed interchange setting.

4.1 Traffic operations

4.1.1 Average delay

As shown in **Figure 2**, the average delay decreased consistently as AV penetration increased across all demand levels. Under low demand, the effect was modest, with a reduction of less than 10% between 0% and 100% AV penetration. In contrast, at medium demand, delays fell by approximately 25% beyond 60% AV penetration, and at high demand, reductions reached nearly 40% at full AV penetration. These

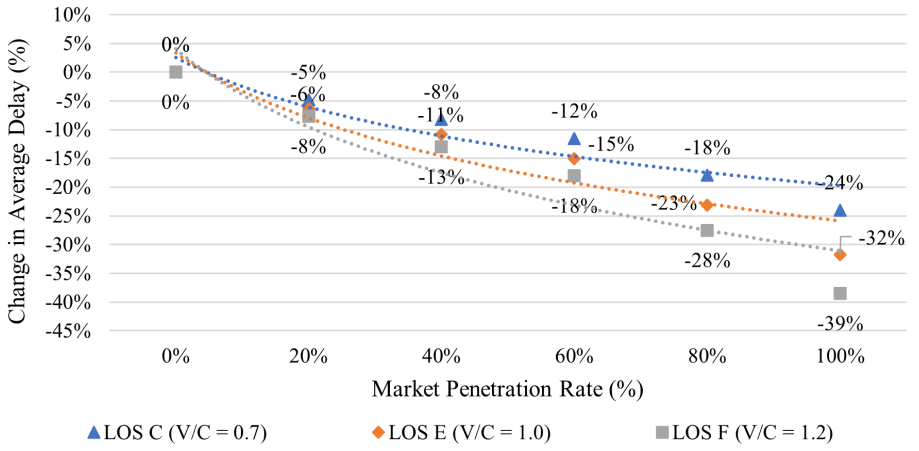


Figure 2.
Average delay by AV penetration and demand level.

patterns align with freeway-based studies reporting nonlinear improvements once AV penetration crosses threshold levels [2, 6]. The results also indicate that AVs can alleviate queues at ramp terminals, preventing freeway spillbacks and amplifying benefits across the interchange.

4.1.2 Average speed

Network-wide average speeds improved steadily with AV penetration, particularly under congested conditions. **Figure 3** shows that while speeds under low demand remained close to free-flow regardless of AV share, medium – and high-demand scenarios exhibited significant gains. At high demand, average speeds increased by 15–20% at full penetration compared with the baseline. This confirms the stabilizing influence of AVs observed in field experiments [4] and extends the evidence to mixed interchange networks, where freeway and arterial flows interact.

4.1.3 Travel time variability

As illustrated in **Figure 4**, travel time variability decreased with higher AV penetration. At high demand, the standard deviation of travel times declined by 10–15% once penetration exceeded 60%. This demonstrates that AVs not only improve mean travel times but also make performance more predictable, which is critical for freight and commuter reliability. The results are consistent with cooperative adaptive cruise control (CACC) simulations [6], but here the benefits extend to interchanges, where intersection queues directly affect freeway flows.

4.1.4 Queue lengths at ramp terminals

AV penetration also shortened arterial queues, as shown in **Figure 5**. Under high demand, ramp terminal queues extended into upstream intersections in the baseline (0% AV) scenario. At 60% penetration, maximum queues were shortened by about 30%, and by 80% penetration, spillbacks were largely eliminated. This supports arterial research showing that AVs improve throughput at signalized intersections

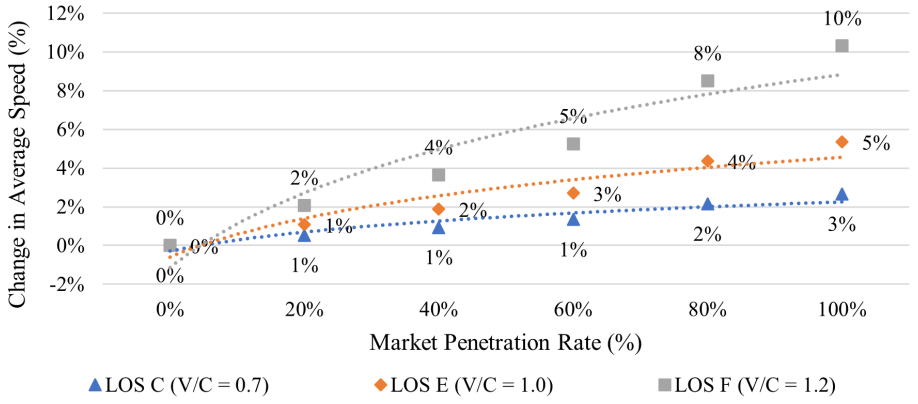


Figure 3.
Average speed by AV penetration and demand level.

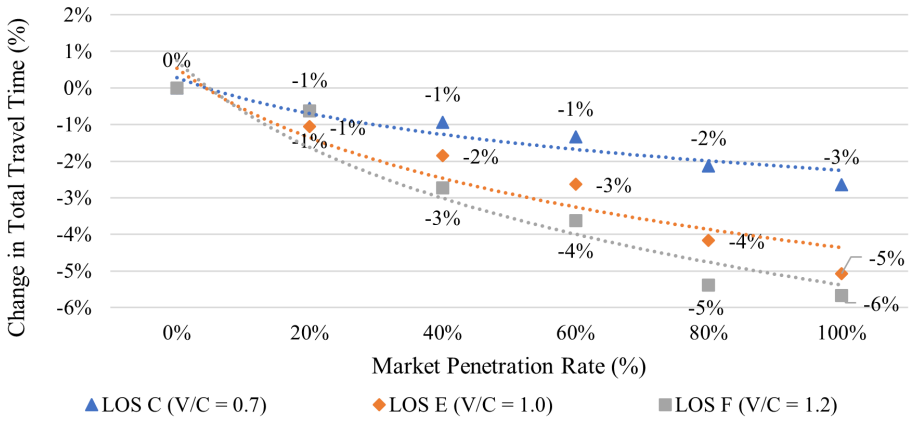


Figure 4.
Travel time variability across AV penetration rates.

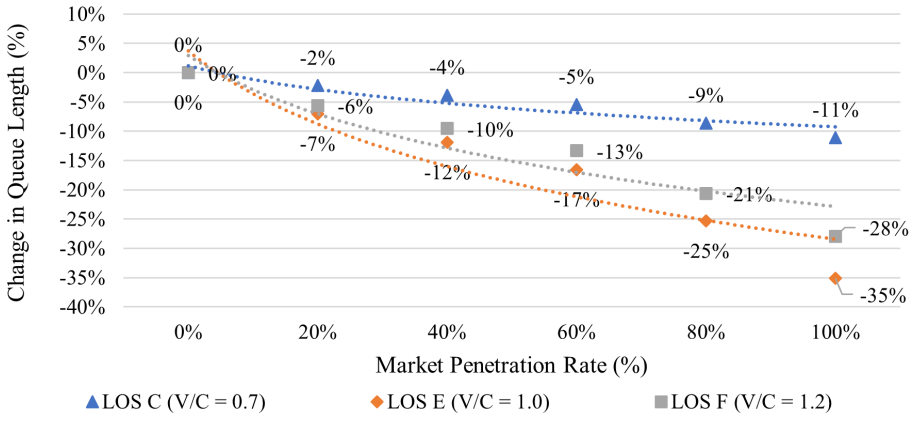


Figure 5.
Maximum queue lengths at ramp terminals under varying AV penetration levels.

[7, 8]. The results demonstrate systemic hybrid benefits, as shorter arterial queues also prevented blockages on freeway off-ramps.

4.2 Safety outcomes

4.2.1 Conflict frequency

As shown in **Figure 6**, conflict frequencies declined sharply as AV penetration increased; however, the magnitude of the reduction varied systematically across demand levels. Under medium demand, conflicts decreased by 25% at 60% penetration and by 50% at full penetration. Under high demand, the total number of conflicts fell by more than 60%. This disproportionate reduction under higher demand indicates that AV-induced stabilization of traffic flow is more effective

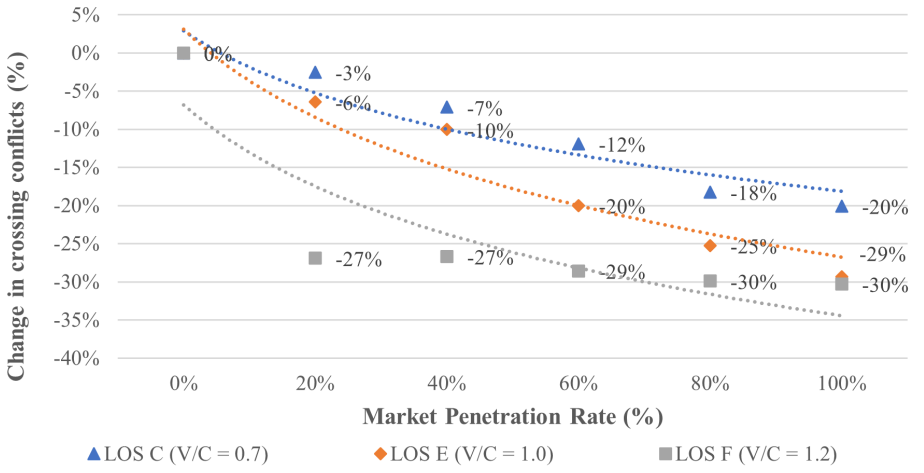


Figure 6.
Total conflict frequency by AV penetration and demand level.

under congested conditions, where human driving behaviors tend to generate more turbulence.

Rear-end conflicts experienced the greatest reductions across all scenarios, consistent with smoother AV following behavior [2, 5, 12], while lane-changing and crossing conflicts showed more gradual but steady declines. This sensitivity to conflict type suggests that AV benefits are most pronounced for longitudinal interactions, while lateral conflict reduction depends more heavily on penetration rate. These results extend prior freeway [2, 6] and arterial [7, 8] studies by demonstrating how mixed environments amplify safety improvements as the share of AVs grows.

4.2.2 Time-to-collision (TTC)

TTC values improved significantly with increasing AV penetration, with the largest gains observed under congested scenarios. As illustrated in **Figure 7**, minimum TTC values rose by 25–30% between 0% and 100% penetration at medium and high demand, compared to smaller gains under low demand. This pattern highlights sensitivity to traffic density, as higher congestion levels create more frequent critical gaps that AVs manage more smoothly.

Improvements were concentrated at ramp merges, where critical TTC values are common in conventional traffic. This aligns with prior freeway studies [6] but provides insight into how the presence of AVs mitigates merge-related critical events in hybrid traffic streams.

4.2.3 Post-encroachment time (PET)

PET values also increased with AV share, exhibiting demand-level sensitivity patterns similar to those of TTC. As shown in **Figure 8**, improvements were most pronounced at signalized ramp terminals. Under high demand, PET gains exceeded 20%, reflecting a reduction in the temporal overlap of vehicles entering the conflict

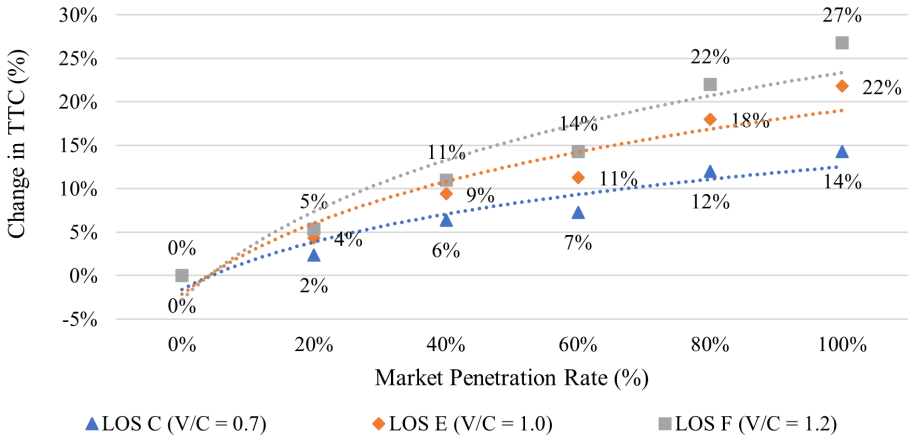


Figure 7.
Minimum TTC values across AV penetration levels.

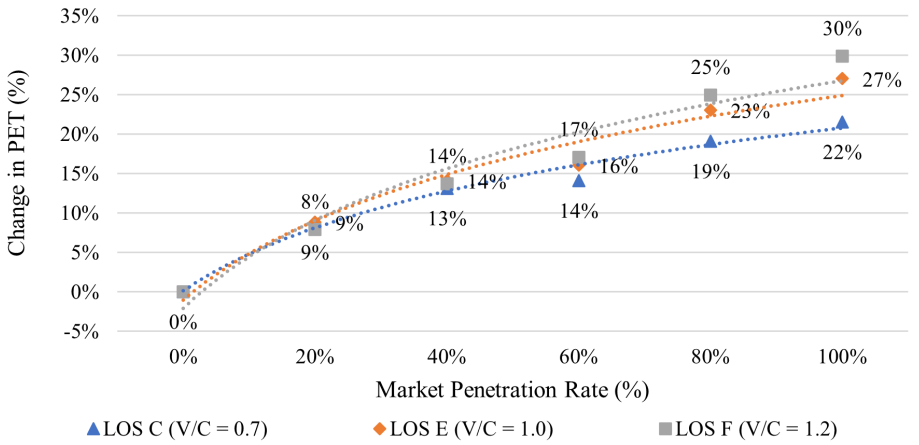


Figure 8.
PET values across demand levels and AV penetration.

zone. This shift indicates that AVs not only reduce the number of conflicts but also increase the temporal buffer between conflicting movements, thereby further reducing the likelihood of crashes.

These findings align with prior arterial analyses [7, 8], but by capturing both intersection and merge-related conflicts, they reveal how AVs enhance safety robustness across multiple conflict mechanisms in mixed settings.

4.3 Environmental outcomes

4.3.1 Carbon dioxide (CO_2) emissions

CO_2 emissions fell modestly with AV penetration, but the magnitude of reduction scaled with the demand level. As shown in **Figure 9**, reductions reached up to 7% at 100% penetration under high demand, whereas improvements under low demand

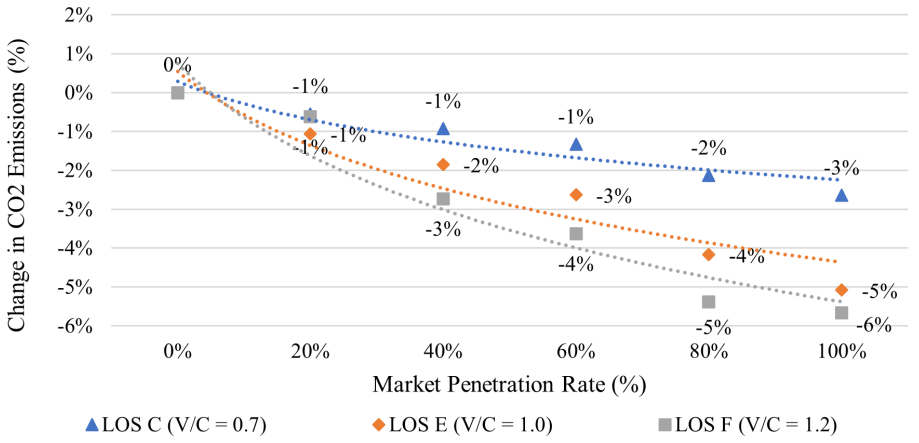


Figure 9.
CO_2 emissions by AV penetration across demand levels.

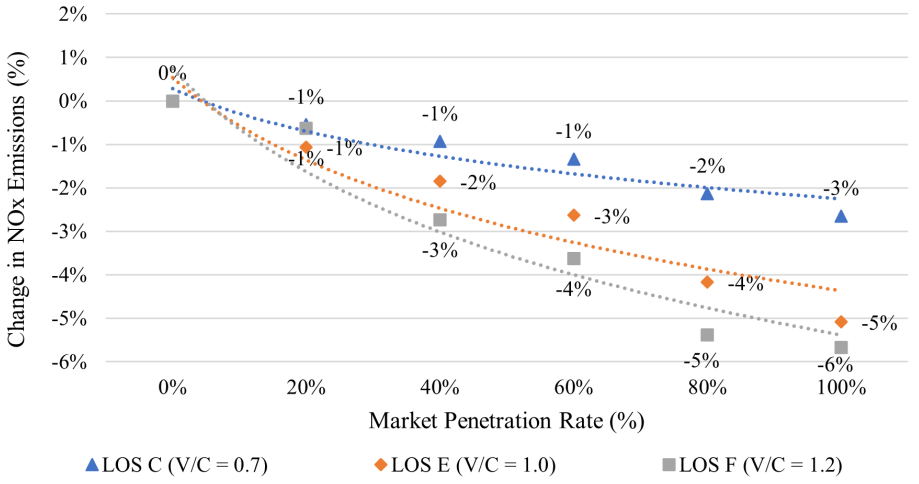


Figure 10.
NOx emissions by AV penetration across demand levels.

were comparatively minor. This demand sensitivity reflects the greater potential of AV control strategies to smooth traffic flow and reduce stop-and-go dynamics under congested conditions.

The environmental benefit is amplified by reductions in queue lengths and improved acceleration profiles, reinforcing previous eco-driving studies [11, 12] and demonstrating that arterial performance plays a significant role in total emissions outcomes.

4.3.2 Nitrogen oxides (NOx)

Similar trends were observed for NOx emissions (**Figure 10**), with reductions of 5–6% at full penetration under high demand and smaller gains at

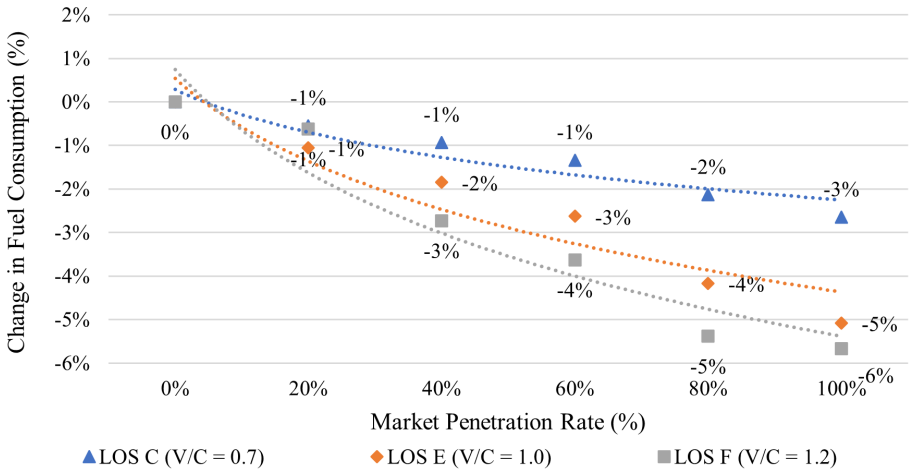


Figure 11.
Fuel consumption by AV penetration across demand levels.

lower demand levels. Reductions were most pronounced at ramp terminals, where aggressive acceleration events are common. This indicates that NOx emissions are particularly sensitive to localized operational conditions, such as merging and signal delay. These findings are consistent with Zhao et al. [9], while additional results suggest that the benefits of automation may vary with penetration levels.

4.3.3 Fuel consumption

Fuel consumption (**Figure 11**) decreased by 4–6% at full penetration under high demand, indicating a demand-sensitive pattern. Although the absolute improvements appear modest, sensitivity analysis suggests that the largest marginal benefits occur beyond the 60% penetration threshold, where traffic stabilization effects become more pronounced.

These results are consistent with projections by Vahidi and Sciarretta [14] and emphasize the cumulative network-level impact of even modest per-vehicle efficiency gains.

4.4 Summary of findings

The results across traffic operations, safety, and environment collectively demonstrate that AVs provide significant benefits in diamond interchange environments. Traffic operations improved most at high penetration levels. Safety benefits accrued steadily, with reductions in conflicts and improvements in TTC and PET, while environmental gains, although modest, were consistent across the various pollutants.

The findings confirm that studying mixed settings is critical: operational and safety benefits are compounded when freeway and arterial efficiencies reinforce one another, a result not captured in studies limited to homogeneous roadway environments.

It is important to note that both surrogate safety measures and emission estimation models provide indirect approximations rather than direct observations of crashes or real-world emissions. Their accuracy depends on modeling assumptions, traffic composition, and calibration parameters; therefore, results should be interpreted as indicative trends rather than absolute predictions.

5. Implications for policy and practice

The findings from this study have several implications for transportation policy, infrastructure planning, and AV deployment strategies.

First, the results demonstrate that AVs deliver the greatest benefits at higher penetration rates. While modest improvements in delay, safety, and emissions were observed at 20–40% penetration, substantial gains only emerged beyond 60%. This suggests that policymakers should prioritize strategies that accelerate AV adoption in order to realize meaningful system-level improvements. Such strategies might include incentivizing shared autonomous fleets, promoting early deployment corridors, or supporting pilot programs at high-demand interchanges.

Second, the study highlights the importance of mixed roadway environments, such as diamond interchanges, as focal points for AV deployment. Unlike freeways or arterials alone, interchanges concentrate congestion, crash risk, and emissions within small geographic areas. Improvements in these bottleneck locations can yield disproportionate benefits for the broader network. Transportation agencies may, therefore, consider targeting AV-friendly design treatments – such as adaptive ramp metering, signal coordination compatible with AV algorithms, or lane management strategies – specifically at interchange facilities.

Third, the safety findings suggest that AVs can reduce conflicts not only on freeways but also at intersections, where rear-end and crossing collisions are prevalent. This reinforces the need for integrated safety performance assessments that extend beyond crash frequencies to include surrogate measures such as TTC and PET. As agencies evaluate AV readiness, prioritizing safety performance at mixed freeway–arterial facilities is essential.

Fourth, while environmental benefits were modest compared to operational and safety improvements, even small percentage reductions in CO_2 and NOx emissions can translate into substantial cumulative impacts at the network scale. This indicates that AV deployment can play a supportive role in meeting sustainability targets, particularly when combined with broader demand management and electrification strategies.

Fifth, despite these promising outcomes, the practical implementation of AVs at diamond interchanges poses several challenges that must be addressed to fully realize these benefits. Diamond interchanges involve complex interactions among freeway, ramp, and arterial movements, requiring reliable vehicle-to-infrastructure (V2I) communication and precise trajectory coordination. Current infrastructure may need significant upgrades – such as high-resolution detection, connected signal controllers, and digital mapping – to support AV operations effectively. Additionally, during the transition period of mixed traffic, unpredictable interactions between human-driven vehicles and AVs can reduce the reliability of expected performance gains. Operational policies, such as dynamic lane allocation or AV-priority movements, may face institutional and regulatory hurdles, and their

effectiveness will depend on the agency's capacity to manage hybrid operational environments. Finally, ensuring interoperability across different AV manufacturers and communication protocols remains a critical technical barrier.

Overall, the implications are clear: AV deployment strategies, infrastructure investments, and regulatory frameworks must explicitly consider interchange environments. Failure to do so risks overlooking critical system bottlenecks and underestimating both the opportunities and the practical constraints of AV implementation.

6. Conclusion

This chapter examines the impacts of autonomous vehicles in a diamond interchange environment, a roadway type that combines freeway and arterial operations and has historically been underrepresented in AV research. Using microscopic simulation, surrogate safety assessment, and emissions modeling, the study evaluates traffic operations, safety outcomes, and environmental effects under varying traffic demand levels and AV penetration rates.

The findings can be summarized as follows:

1. Traffic operations: AVs reduced delay, improved average speeds, and enhanced travel time reliability, particularly at penetration rates above 60%. Queue lengths at ramp terminals declined significantly, preventing freeway spillbacks and alleviating interchange bottlenecks.

2. Safety: Surrogate measures demonstrated substantial safety improvements, with total conflicts decreasing by more than 50% at full penetration. TTC and PET values improved consistently, reducing both freeway-merge and intersection-related risks.

3. Environment: AVs lowered CO_2, NOx, and fuel consumption, with the most pronounced benefits under congested conditions. While modest in magnitude, these reductions reinforce the role of AVs in supporting broader sustainability goals.

The central contribution of this study lies in demonstrating that AV impacts in mixed environments cannot be fully inferred from studies conducted on freeways or arterials alone. Analyzing a diamond interchange highlights the compounded benefits of AVs in contexts where uninterrupted freeway flows and interrupted arterial flows converge.

The reported results should be viewed as indicative trends rather than exact forecasts. Future research should combine surrogate-based assessments with crash-based validation, integrate higher-fidelity emission modeling, and evaluate multi-source uncertainty to strengthen the robustness and transferability of the findings.

Future research should expand this line of inquiry by testing alternative interchange designs (e.g., diverging diamond, single-point urban interchanges), incorporating connected vehicle-to-infrastructure (V2I) technologies, and exploring heterogeneous fleets with varying levels of automation. Such efforts will further refine our understanding of AV impacts in complex, real-world networks.

In conclusion, autonomous vehicles hold considerable promise for enhancing traffic operations, improving safety, and reducing environmental impact. Their effectiveness, however, must be assessed in the contexts that matter most for system performance. Mixed interchange environments represent exactly such contexts, and this chapter contributes to filling that critical gap.

Author details

Khaled Hamad* and Mohamad Tulimat
University of Sharjah, Sharjah, United Arab Emirates

*Address all correspondence to: khamad@sharjah.ac.ae

IntechOpen

© 2026 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] Anderson JM, Kalra N, Stanley KD, Sorensen P, Samaras C, Oluwatola OA. Autonomous Vehicle Technology: A Guide for Policymakers. Santa Monica (CA): RAND Corporation; 2016. p. 189. DOI: 10.7249/RR443-2

[2] Talebpour A, Mahmassani HS. Influence of connected and autonomous vehicles on traffic flow stability and throughput. Transportation Research Part C: Emerging Technologies. 2016;**71**:143–163. DOI: 10.1016/j.trc.2016.07.007

[3] Chen D, Ahn S, Chitturi M, Noyce DA. Towards vehicle automation: Roadway capacity formulation for traffic mixed with regular and automated vehicles. Transportation Research Part B: Methodological. 2017;**100**:196–221. DOI: 10.1016/j.trb.2017.01.017

[4] Stern RE, Cui S, Delle Monache ML, Bhadani R, Bunting M, Churchill M, et al. Dissipation of stop-and-go waves via control of autonomous vehicles: Field experiments. Transportation Research Part C: Emerging Technologies. 2018;**89**:205–221

[5] Ghiasi A, Hussain O, Qian Z, Li X. A mixed traffic capacity analysis and lane management model for connected automated vehicles: A Markov chain method. Transportation Research Part B: Methodological. 2017;**106**:266–292. DOI: 10.1016/j.trb.2017.09.022

[6] Milanés V, Shladover SE. Modeling cooperative and autonomous adaptive cruise control dynamic responses using experimental data. Transportation Research Part C: Emerging Technologies. 2014;**48**:285–300. DOI: 10.1016/j.trc.2014.09.001

[7] Islam S, Hajbabaie A. Distributed coordinated signal timing optimization in connected transportation networks. Transportation Research Part C: Emerging Technologies. 2017;**80**:272–285. DOI: 10.1016/j.trc.2017.04.017

[8] Lee J, Park B. Development and evaluation of a cooperative vehicle intersection control algorithm under the connected vehicles environment. IEEE Transactions on Intelligent Transportation Systems. 2012;**13**(1):81–90. DOI: 10.1109/TITS.2011.2166837

[9] Zhao W, Ngoduy D, Shepherd S, Liu R, Papageorgiou M. A platoon based cooperative eco-driving model for mixed automated and human-driven vehicles at a signalised intersection. Transportation Research Part C: Emerging Technologies. 2018;**95**:802–821. DOI: 10.1016/j.trc.2018.05.025

[10] Calvert SC, van den Broek THA, van Noort M. Cooperative driving in mixed traffic networks — Optimizing for performance. 2012 IEEE Intelligent Vehicles Symposium, Madrid, Spain. 2012. p. 861–866. DOI: 10.1109/IVS.2012.6232138

[11] Hamad K, Alozi AR. Shared vs. Dedicated lanes for automated vehicle deployment: A simulation-based assessment. International Journal of Transportation Science and Technology. 2022;**11**(2):205–215. DOI: 10.1016/j.ijtst.2022.03.001

[12] Morando MM, Tian Q, Truong LT, Vu HL. Studying the safety impact of autonomous vehicles using

simulation-based surrogate safety measures. Journal of Advanced Transportation. 2018;**2018**:1–11. DOI: 10.1155/2018/6135183

[13] Zhou X, Tanvir S, Lei H, Taylor J, Liu B, Rouphail NM, et al. Integrating a simplified emission estimation model and mesoscopic dynamic traffic simulator to efficiently evaluate emission impacts of traffic management strategies. Transportation Research Part D: Transport and Environment. 2015; **37**:123–36. DOI: 10.1016/j.trd.2015.04.013

[14] Vahidi A, Sciarretta A. Energy saving potentials of connected and automated vehicles. Transportation Research Part C: Emerging Technologies. 2018;**95**:822–843. DOI: 10.1016/j.trc.2018.09.001

[15] Hoogendoorn R, van Arem B, Hoogendoorn SP. Automated driving, traffic flow efficiency, and human factors: Literature review. Transportation Research Record: Journal of the Transportation Research Board. 2014;**2422**(1):113–120. DOI: 10.3141/2422-13

[16] Transportation Research Board. Highway Capacity Manual (HCM 2016) 6th Edition: A Guide for Multimodal Mobility Analysis (HCM 2016). Washington, DC: National Academies Press; 2016

[17] Tulimat M, Obaid O, Obaid L, Hamad K. Quantifying impacts of connected and automated vehicles on traffic operation of a diamond interchange in UAE using micro-simulation. In: 14th International Conference on Developments in eSystems Engineering (DeSE); 2021. p. 682–687. DOI: 10.1109/DeSE54285.2021.9719571

[18] Alozi AR, Hamad K. Quantifying impacts of connected and autonomous vehicles on traffic operation using micro-simulation in Dubai, UAE. In: 5th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS 2019); Crete, Greece; 2019. DOI: 10.5220/0007753905280535

[19] Federal Highway Administration (FHWA). Surrogate Safety Assessment Model and Validation: Final Report. Report No: FHWA-HRT-08-051. Washington, DC: U.S. Department of Transportation; 2008

Chapter 12

Applications of Driving Simulators in Intelligent Transportation Systems: Investigating Driver Behavior under Variable Speed Limits

Behnood Baiky, Facundo Storani, Roberta Di Pace and Stefano de Luca

Abstract

This study explores driver perception and compliance with variable speed limits (VSLs) within Intelligent Transportation Systems (ITS), emphasizing the critical role of human behavior in traffic efficiency and safety. Using driving simulators (DSs), it bridges the gap between model-based and safety-oriented VSL studies and real-world driver responses, providing insights into behavioral realism and adaptive system performance. A structured narrative review was conducted to synthesize studies using DSs to analyze driver behavior and compliance under VSLs within ITS. Following strict inclusion criteria and database searches, 24 high-quality studies (1994–2025) were selected and systematically analyzed to identify methodological trends, research gaps, and behavioral insights. DSs prove to be powerful, cost-effective tools for analyzing driver perception, compliance, and behavioral adaptation under VSLs, offering realistic, safe testing environments for ITS research. Future studies should integrate DS experiments with connected vehicle data, artificial intelligence (AI)-driven behavioral models, and cross-cultural analyses to design adaptive, human-centered, and globally applicable VSL systems.

Keywords: intelligent transportation systems, driving simulator, perception, compliance, variable speed limits

1. Introduction

Intelligent Transportation Systems (ITSs) have emerged as multidisciplinary technological solutions designed to enhance the safety, efficiency, and sustainability of modern transport networks. By integrating communication, sensing, and control technologies, ITS enables real-time data exchange between vehicles and infrastructure, improving traffic management, reducing congestion and emissions,

and preventing accidents through adaptive control mechanisms. Despite their proven benefits, many developing countries still face challenges in implementing ITS due to inadequate road and telecommunication infrastructure [1] Current ITS research primarily focuses on three core components: the driver, the vehicle, and the road [2]. While substantial progress has been made in vehicle systems, control strategies, and infrastructure integration, driver behavior remains a critical factor for achieving adaptive and human-centered ITS. Understanding how drivers perceive and respond to ITS interventions is fundamental, as behavior directly influences traffic flow, safety, and system performance. This study concentrates on driver perception and compliance with variable speed limits (VSLs), key behavioral factors that shape traffic dynamics and congestion mitigation. Using driving simulator (DS) experiments, the research aims to advance the development of more intelligent and responsive ITS. The overall structure of ITS applications and their subsystems is shown in **Figure 1**, with particular emphasis on the VSL domain, the main focus of this study [1, 3].

In recent years, numerous studies have investigated VSL as part of intelligent ITS solutions that dynamically adjust posted speed limits in response to prevailing traffic, incidents, and weather conditions. Many of these studies have employed microscopic traffic simulation tools such as VISSIM, SUMO, and AIMSUN, where driver behavior is modeled through calibrated car-following models based on vehicle trajectory data rather than direct human observation. For instance, the study by[4] analyzed a Cooperative VSL System (C-VSLS) integrating infrastructure-to-vehicle communication and individualized speed limits as an improvement over traditional VSLs. Using microscopic traffic simulation in SUMO, the authors reported smoother traffic flow, reduced acceleration fluctuations, and lower emissions compared to standard systems. Similarly, the study by Khondaker and Kattan [5] proposed a microscopic Model Predictive Control-based VSL algorithm implemented in a VISSIM–MATLAB environment to enhance mobility, safety, and environmental performance. At full connected-vehicle penetration, the system achieved up to a 20% reduction in travel time, 6%–11% improvement in safety, and 5%–16% lower fuel consumption. Overall, both studies [4, 5] demonstrate the potential of simulation-based methods and connected vehicle (CV) data to develop proactive, data-driven VSL strategies capable of improving traffic efficiency and sustainability. However, a common limitation of such approaches lies in their reliance on rule-based driver behavior models and predefined compliance assumptions, which do not fully capture the variability and complexity of real-world driver perception and response to VSL systems. In parallel, most empirical studies have examined drivers' reactions to VSL primarily from a road safety perspective [6], focusing on adaptive control algorithms designed to reduce crash risk through technologies such as variable message signs (VMSs) and on-board units (OBUs). While valuable, these works similarly provide only a partial understanding of driver perception, interpretation, and compliance, especially under varying real-world traffic and environmental conditions. To address the limitations of model-based and safety-oriented VSL studies, driver-in-the-loop simulators provide a unique opportunity to observe real human behavior in controlled yet realistic environments. In contrast to traditional modeling approaches that rely on predefined behavioral assumptions, DSs allow researchers to capture both observable driver responses and underlying psychological factors involved in speed compliance and decision-making. In this review chapter, we focus on the application of DSs to the analysis of driver

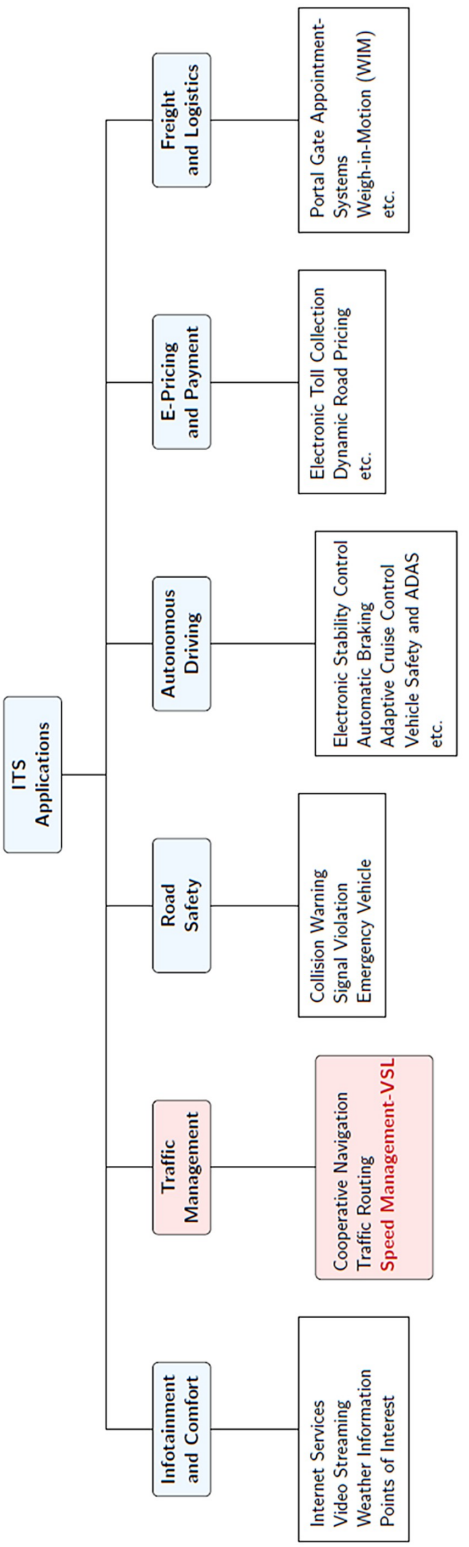


Figure 1.
ITS applications with emphasis on the VSL domain.

behavior and compliance with VSL systems, particularly how drivers perceive and respond to dynamic speed limit messages displayed through on-board interfaces and highway gantries. Building upon these insights, the next stage of this investigation transitions from algorithmic simulations to human-centered experimentation. This is implemented using a DS as the primary apparatus for capturing participants' driving trajectories and behavioral responses.

Thus, as highlighted by Aiman Affandi et al. [7], DSs have emerged as comprehensive and valuable tools for evaluating driver behavior and performance across various traffic scenarios. They combine the advantages of full experimental control with a high degree of realism in representing real-world driving conditions, making the results more relevant and transferable to actual road situations [8]. As a cost-effective and versatile virtual reality (VR) platform, the DS enables the design, evaluation, and optimization of complex traffic scenarios and facilitates the investigation of driver–vehicle interaction under controlled, repeatable, and safe experimental conditions. Their physical and functional complexity ranges from simple fixed-base units to immersive, high-fidelity motion platforms, tailored to the objectives of each study and the degree of realism required [9–11]. DSs are widely applied across three primary domains: driver behavior research, road and traffic design, and the development and testing of ITS, where simulation environments have become integral to advancing both ITS and Automated Highway Systems (AHS) [9, 12].

Building upon these core areas, the interdisciplinary role of VSL emerges, positioning VSL as a unifying concept that integrates technical, behavioral, and system-level dimensions within transportation research. DSs provide a risk-free setting for validating system performance and assessing user acceptance in both onboard and roadside applications. With recent technological integration, these virtual platforms now operate in tandem with traffic flow and communication network simulators, enabling real-time coordination analysis across complex traffic environments [13]. This theme is further developed in Section 3, which reviews a substantial body of research employing simulators to investigate driver behavior under VSL conditions, focusing particularly on perception, compliance, and broader ITS frameworks. These studies offer critical insights into compliance, perception, and safety outcomes. Empirical findings indicate that external factors such as surrounding traffic, passing rates, and route familiarity significantly influence speed choice and compliance, often through mechanisms such as social pressure or cognitive limitations like change blindness. Dynamic and context-sensitive conditions, including weather-responsive VSLs and sequential VMS warnings, have also been shown to affect driver speed consistency and decision-making, with CV and human–machine interface (HMI)-based advisory systems further shaping behavioral responses. Research further emphasizes the importance of designing credible, context-appropriate speed limits and understanding the roles of socio-demographic factors, workload, and driver expectations in achieving safe and effective speed management.

Collectively, these findings support the use of DSs as robust experimental tools for isolating and evaluating the multifaceted influences on driver behavior in VSL environments. By combining behavioral realism with experimental control, simulators effectively bridge the gap between simulation-based ITS design and the complex human factors that ultimately shape real-world system performance. Despite these advantages, broader adoption remains constrained by limitations such

as reduced ecological validity, simulator-induced discomfort, high operational costs, and diminished fidelity in lower-end systems. Persistent challenges in modeling vehicle dynamics, ensuring visual realism, and maintaining user engagement continue to affect the overall effectiveness of simulation studies. Nevertheless, ongoing technological advancements are steadily addressing these issues, enhancing both the practical value and research utility of simulator-based investigations [10, 14].

2. Methodology of literature selection

2.1 Design

This study adopts a structured narrative review approach aimed at summarizing and analyzing the applications of DSs within the context of ITS, with a particular emphasis on driver behavior under VSL. While the review does not conduct a formal meta-analysis, it considers and discusses relevant statistical findings from the literature to support its synthesis of key insights. The review explores how DSs have been employed to investigate driver perception, compliance, and behavioral adaptation in VSL environments. To facilitate a clearer understanding of the research domain, the study first situates VSL within the broader framework of ITS, specifically within the areas of traffic management and speed regulation, providing the conceptual foundation for subsequent discussions. The DS is then addressed as a distinct methodological component, highlighting its role as the central experimental apparatus for capturing detailed driver trajectory data and behavioral responses. This design allows for a comprehensive overview of simulator-based methodologies applied to VSL studies and supports the identification of current research trends and gaps that can guide future experimental investigations.

2.2 Inclusion and exclusion criteria

The reviewed literature included articles published in English in peer-reviewed journals, book chapters, or conference proceedings that employed a DS to analyze driver behavior or system performance related to VSL. Studies were required to provide clear methodological descriptions, including simulator setup, participant details, and behavioral metrics, and to present quantitative or qualitative findings on driver behavior, compliance, or perception in the context of VSL research. Publications spanning from 1994 to 2025 were considered, representing the evolution of driving simulator use over three decades. In contrast, non-English publications, theses, reports, and other forms of gray literature were excluded, along with studies based solely on microscopic traffic simulations (e.g., VISSIM, SUMO), such as those in literature [4, 5], which were only referenced in the introduction to illustrate the research gap. Likewise, works focusing mainly on road safety rather than traffic or transportation system performance, such as the study by del Serrone et al. [6], were not included in the main body of the review. Finally, studies lacking sufficient methodological information regarding simulator configuration, experimental design, or data analysis were also excluded.

2.3 Search strategy

The literature search followed a structured and replicable process designed to identify studies relevant to the application of DSs in ITS, with a specific focus on VSL. The search was conducted across major academic databases, including Scopus, Web of Science, IEEE Xplore, ScienceDirect, SpringerLink, and MDPI, complemented by targeted searches in Google Scholar and institutional repositories such as ResearchGate and White Rose ePrints. Search queries combined key terms such as "driving simulator," "variable speed limits," "intelligent transportation systems," "driver behaviour," "compliance," "human–machine interface (HMI)," and "connected and automated vehicles." Boolean operators (AND, OR) and wildcard truncations were applied to refine the results. The initial search yielded over 50 publications, which were filtered through inclusion and exclusion criteria to ensure scientific quality, relevance, and methodological transparency.

To ensure comprehensive domain coverage, the selected literature included:

- Foundational and systematic works on ITS technologies and frameworks [1–3];
- Simulation-based studies on VSL design and performance at the microscopic level [4–6];
- Reviews and methodological discussions on driving simulators, validation, and fidelity [7–14];
- Experimental DS applications focusing on driver behavior, compliance, and adaptation under VSL and related ITS scenarios [15–24].

Reference lists of included papers were manually screened to capture additional relevant studies not indexed in the databases. After the full screening process, 24 studies published between 1994 and 2025 were selected as the most representative and methodologically sound contributions to the topic. These works collectively provide a solid foundation for understanding the role of DSs in analyzing driver perception and compliance within dynamic speed management systems.

2.4 Data extraction and analysis

From each selected study, information on the objectives, methodology, simulator type, participant characteristics, experimental design, key findings, and limitations was extracted. These studies form the foundation of Section 3, *"Literature Review on Driver Behaviour under VSLs and Advisory Systems in ITSs Using DSs,"* which presents the core analysis of this chapter.

Papers mentioned in the "Introduction" were included primarily to provide background context and guide the deeper discussion. The role of DSs, outlined there in terms of their technological configurations, application domains, and advantages, served to establish the foundation for this literature-based investigation. The detailed review focused on identifying research gaps and highlighting critical aspects among the 10 selected simulator-based studies. Special attention was given to the statistical objectives and results of each work. Within this group, two papers focused on on-board VSL systems and HMI, and the remaining works investigated off-board

VSL systems using gantry-based displays. The analysis also aimed to provide a comparative quantitative overview of simulator-based research trends and outcomes across different experimental contexts.

3. Literature review on driver behavior under VSLs and advisory systems in ITSs using DSs

Recent advancements in traffic simulation have substantially enhanced the understanding of driver behavior under VSLs. This literature review synthesizes 10 key studies that collectively examine the interaction between external pressure, driver heterogeneity, psychological factors, spatial regulation, and behavior-informed speed limit design. The main thematic dimensions include External Pressure and Behavioural Variability, Internal Cognitive Determinants of Compliance, Spatial Heterogeneity and Lane-Specific VSLs, Informed Speed Limit Design, and the Integration of VMS, VSLs, and In-Vehicle Advisory Systems. All studies adopt DS as the core methodological approach, reflecting a shared emphasis on controlled experimentation and behavioral observation. Together, they illustrate a methodological and conceptual evolution in exploring speed compliance and adaptive traffic control.

Sections 3.1 and 3.2 present a detailed analysis of each study, organized into two major categories: off-board VSL display systems and on-board in-vehicle advisory systems, highlighting their key findings, limitations, and complementary contributions to identify remaining research gaps and future directions for advancing this domain.

3.1 Driver behavior under off-board VSL and advisory systems

Recent simulator-based research has advanced the understanding of driver compliance under VSLs, particularly by analyzing how external traffic pressure, operationalized as passing rates and overtaking frequency, interacts with driver heterogeneity to influence speed behavior and compliance dynamics.

Building on TRACSLab experiments, the first study by Ali et al. [15] showed that higher passing rates (P360) significantly increased initial speeds under pressure, upto +18.0 km/h in VSL-1 zones, compared to low-pressure (P90) conditions. In contrast, speeds in VSL-2 zones decreased by −2.16 km/h, attributed to slower artificial intelligence (AI)-controlled trailing vehicles. Speed variability also increased under pressure, with the standard deviation of lateral position (SDLP) and acceleration-deceleration profiles showing greater fluctuations; for instance, speed variation in VSL-1 reached 4.2 km/h under P360 versus 3.55 km/h under P90. These effects were moderated by demographics: younger drivers (18–26 years) increased speeds by upto +8.03 km/h, while older drivers (51–65 years) showed mixed responses, including reductions of −4.55 km/h in VSL-2. Female drivers consistently drove 3.17–3.79 km/h slower than males under pressure. Notably, compliance within five seconds of passing a VSL sign did not significantly vary across passing rates (Wald $\chi^2 = 2.16–3.99$; $p > 0.05$), suggesting external pressure affects speed and variability but not immediate binary compliance.

Ali et al. [16] expanded earlier findings by modeling the time drivers take to comply with speed limits under social pressure, using a Weibull-based accelerated

failure time (AFT) model with correlated random parameters. Under high passing rates (P360), drivers not only exhibited higher initial speeds (by up to +18 km/h) but also delayed speed reductions, with braking duration approximately 2.7 times longer than in low-pressure (P90) conditions. The initial speed was found to be a critical determinant: for every 1 m/s increase, braking time extended by 5.4%, while greater deceleration capacity (1 m/s^2) shortened braking duration by 36%. Acceleration noise, capturing driver uncertainty or hesitation, was also influential, with a 67% increase in braking time associated with a 1 m/s^2 increase in noise. The study distinguished compliant and non-compliant driver profiles, with adaptation shaped by age, gender, and behavior under traffic pressure, revealing significant cognitive and perceptual variability. These findings support adaptive VSL systems informed by driver heterogeneity and validated through advanced multi-level behavioral modeling.

Complementing the earlier findings in literature [15, 16], the study by Storani et al. [17] offered a qualitatively richer yet technically aligned perspective by examining driver compliance with VSLs in the absence of explicit external traffic pressure, thereby isolating the influence of latent behavioral factors. Conducted using the SimEASY fixed-base driving simulator at the University of Salerno, Storani et al. [17] explored driver responses to two VSL sequences across a 6 km two-lane corridor: one decreasing from 110 to 80 to 60 km/h, and the other from 110 to 60 to 80 km/h. With deceleration realistically modeled at 0.8 m/s^2, the study emphasized perceived safety, self-efficacy, and effort expectancy through pre- and post-experiment questionnaires and multi-phase simulation trials. These subjective measures introduced a more introspective dimension compared to the predominantly quantitative focus of earlier studies. While Ali et al. [15] quantified how traffic pressure increases speed variability and Ali et al. [16] expanded on this by modeling compliance delay using temporal survival analysis, Storani et al. [17] demonstrated that even without external stressors, drivers exhibited high compliance, attributed to clear signage, predictable transitions, and psychological comfort. In contrast to the 2.7 times longer braking durations under high pressure in literature [15, 16], Storani et al. [17] observed smoother speed adaptation and shorter braking response when drivers felt more in control, reinforcing the role of internal regulation mechanisms.

Viewed together, these three studies outline a progressive understanding of VSL compliance.

- Ali et al. [15] established the mechanical and demographic impacts of social pressure on speed behavior.
- Ali et al. [16] added depth by capturing temporal compliance dynamics and classifying driver types.
- Storani et al. [17] introduced psychological determinants, emphasizing how internal states can promote voluntary compliance, even in the absence of external triggers.

This progression reflects a methodological evolution: From statistical modeling in the study by Ali et al. [15], to stochastic and behavioral clustering in the study by Ali et al. [16], and finally to cognitive-behavioral assessment in the study by Storani et al. [17]. The integration of engineering analysis with

driver psychology across these studies signals a shift toward adaptive, human-centered VSL system design, where both external social context and internal cognitive readiness are recognized as critical to effective speed compliance.

Introducing a spatial dimension to VSL compliance [18], moves beyond the temporal and psychological factors emphasized in literature [15, 16, 17]. While those studies focused on uniform VSL conditions influenced by traffic pressure, compliance timing, or internal cognitive states, Shi and Liu [18] investigated how intra-lane speed differentiation affects driver decision-making and mental workload, adding a crucial spatial-operational perspective often absent from prior work.

Extending the discussion, Shi and Liu [18] evaluated differentiated per-lane speed limits (DPLSL) using a high-fidelity driving simulator over a 4 km two-lane freeway. Three scenarios were tested: a uniform speed limit (120 to 60 km/h), a simple DPLSL (same maximum limit of 120 km/h, differing minimums of 90 and 60 km/h), and a complex DPLSL with full lane-specific ranges (120–90 km/h inner lane; 100–60 km/h outer lane). Results from 37 drivers revealed that lane-change frequency declined in complex DPLSL scenarios (110 vs. 134/136 in uniform/simple), indicating increased caution. However, lane changes occurred more abruptly, with higher second-peak lateral acceleration (0.86 m/s^2 vs. 0.71 m/s^2), suggesting sharper maneuver corrections. Additionally, longitudinal speeds were lower, reflecting more deliberate driving behavior. NASA-TLX scores confirmed that DPLSL, particularly in complex setups, significantly elevated mental workload, frustration, and perceived cognitive demand, though physical demand remained stable. These findings illustrate that lane-specific VSLs introduce spatial and cognitive complexity, influencing both behavior and workload differently than uniform systems, and highlighting the importance of considering lane-level variability in future VSL design strategies.

While some studies [15–17] examined how drivers adjust to VSLs under varying social, cognitive, or environmental conditions, and Shi and Liu [18] extended this by assessing how lane-specific speed differentiation affects maneuvering and mental workload, Montella et al. [19] reverses the direction of inquiry. Rather than studying compliance with pre-set limits, it asks how speed limits should be set in the first place, grounded in how drivers actually behave and constrained by safety-critical design parameters.

To address this, Montella et al. [19] developed a credibility-based speed limit framework, defining the posted speed as a weighted average of an inferred design speed (based on curve stability and stopping-sight distance) and an operating speed (derived from calibrated prediction models and simulator data). This framework was implemented on two segments of the A16 Naples–Canosa motorway using a STISIM M300 simulator. Twenty-eight drivers completed repeated runs with and without posted limits. Findings showed substantial reductions in mean speeds, from 101.1–118.9 km/h to 85.2–94.3 km/h on Segment 1, and from 104.3–120.8 km/h to 86.9–93.9 km/h on Segment 2, when limits were present. Speed variability also decreased significantly, with the standard deviation reduced to as low as 2.5 km/h. Cross-validation between simulator results and external prediction models showed strong agreement (average deviation < 10%), supporting the reliability of the data fusion approach. Based on these results and a projected 23% crash reduction under Point-to-Point enforcement and geometric adjustments, the study recommended a uniform 100 km/h limit across both segments.

Despite the valuable insights offered by studies into drivers' interaction with VSLs, a critical factor remains underexplored: the influence of route familiarity and habituation on drivers' ability to perceive and respond to speed limit changes. While studies [15–19] have focused on how drivers respond to externally imposed speed conditions, whether through design-based credibility [19] or dynamic control under cognitive and traffic-related pressures [15–18], they often implicitly assume a level of constant attentiveness that may not reflect real-world driving behavior. This is especially problematic on habitual routes, which dominate daily travel patterns and can lead to overfamiliarity, reduced vigilance, and diminished responsiveness to dynamic regulatory cues.

To address this gap, Lee and Abdel-Aty [20] conducted a controlled, longitudinal simulation study that examined how repeated exposure to a fixed driving route influences change detection and compliance behavior in response to VSL modifications. Simulating a routine commuting scenario, the study assessed perceptual adaptation across 19 drives, revealing that only 41.7% of drivers detected an increase in the speed limit from 80 to 100 km/h, a figure drastically lower than the expected detection rate of 93.75% ($p < 0.001$). This finding highlights a pronounced case of change blindness, with tangible behavioral consequences: aware drivers increased their speeds appropriately (around 100 km/h), whereas unaware drivers maintained significantly lower speeds (around 87 km/h), reinforcing the link between situational awareness and behavioral adaptation. Familiarity-induced habituation was quantitatively confirmed through a statistically significant increase in average speeds across the first 18 drives ($p < 0.001$), indicating progressive attentional decline. Confidence ratings in VSL change detection were notably higher among aware drivers (M = 5.0) compared to unaware ones (M = 3.3), reinforcing a correlation between situational awareness and behavioral compliance. Additionally, verbal observational data dropped by 52%, from 150 in the initial session to 72 by the 19th, evidencing reduced active monitoring. Although overall sign importance ratings remained consistent between groups, differences in which signs were deemed most relevant pointed to a familiarity-driven shift in informational prioritization. These findings collectively highlight that habituation can compromise the perceptual effectiveness of VSL systems, underscoring the need for adaptive designs that account for cognitive desensitization over time.

3.1.1 Integration of VSL and VMS systems: Behavioral compliance and cognitive insights

Earlier studies on VSL [15–19] predominantly treated them as isolated, off-board control mechanisms, often overlooking the influence of complementary systems such as VMS. More recent research, however, has shifted toward a more integrated approach, examining the combined effects of VSL and VMS on driver behavior and compliance [21, 22]. Among the more recent contributions, study by Matowicki and Pribyl [21] employed a high-fidelity freeway simulator to evaluate how various VSL configurations and warning messages affect speed modulation across congested and uncongested traffic scenarios. In contrast, study by Yang et al. [22] delved into cognitive and perceptual factors, such as driver comprehension, education level, and visual attention, using a longer arterial simulation enriched with eye-tracking and psychometric data.

While differing in methodological orientation and traffic contexts, both studies converge on several key insights:

- Spatial response windows: Both studies empirically identified a ±200-meter zone around signage as critical for driver behavior adjustments. In the study by Matowicki and Pribyl [21], this was derived from speed data across multiple intervals; in the study by Yang et al. [22], eye-tracking and braking patterns revealed a 400-meter adjustment span, further validating the 200 m pre- and post-sign importance.

- Message framing and comprehension: Semantic clarity and relevance of VSL/VMS messages consistently predict compliance. In the study by Yang et al. [22], comprehension of VSL systems emerged as the strongest predictor ($\beta = 0.5656$, $p = 0.0016$), while Matowicki and Pribyl [21] found that safety-oriented messages, such as "High Accident Risk," significantly increased compliance ($\beta = 1.5263$, $p = 0.0117$).

- Behavioral elasticity under traffic conditions: Study by Matowicki and Pribyl [21] uniquely highlighted how driver compliance varies dynamically with traffic states. Under congestion, drivers adjusted less mid-course but showed recovery compliance downstream ($\beta = 1.2310$ at VMS2, $p = 0.0340$), revealing a form of contextual behavioral elasticity not captured by Yang et al. [22], which modeled only one traffic level.

- Individual differences: Both studies explored demographic factors, but age and gender effects were weak or inconsistent. However, education consistently influenced behavior [22], reporting a positive compliance effect ($\beta = 0.3249$, $p = 0.0389$), aligning with the notion that understanding VSL logic facilitates better behavioral alignment.

- Analytical approaches: Methodologically Matowicki and Pribyl [21] used binary logistic regression, focusing on statistically significant predictors ($p < 0.05$) for speed change and compliance metrics. In contrast, Yang et al. [22] combined regression with k-means clustering, identifying seven behavioral driver profiles that explained approximately 70% of variance in reaction distances, emphasizing the need for adaptive VSL strategies rather than uniform ones.

- Policy and design implications: The insights from both studies offer nuanced design recommendations with Matowicki and Pribyl [21] supporting progressive VSL transitions and context-sensitive warnings to enable smoother speed adaptation, while Yang et al. [22] stresses the importance of driver education and spatial timing in sign placement for enhanced message reception and compliance.

Together, these studies mark a shift from mechanistic to behavioral traffic management paradigms, underscoring the importance of integrated VSL–VMS systems, contextual messaging, and user-centered design for maximizing compliance and safety outcomes in dynamic roadway environments.

3.2 Driver behavior under on-board VSL and advisory systems

As discussed in the previous section (3.1), studies [15–22] primarily treated VSLs as off-board systems delivered via roadside infrastructure and signage. However, in

subsequent studies [23, 24], the focus shifted toward in-vehicle speed warning and advisory systems, enabling a more precise assessment of driver responses under hazardous conditions.

Specifically, Xu et al. [23] investigated a CV-based VSL (CV-VSL) application to examine truck driver behavior under adverse weather conditions, while Harms and Brookhuis [24] evaluated a Speed Limit Advisory System (SLAS). Together, these studies provide a more comprehensive understanding of VSL implementation by emphasizing driver behavior and safety improvements within in-vehicle contexts. Study by Xu et al. [23] conducted at the University of Wyoming's WyoSafeSim Laboratory, utilized a high-fidelity motion-based truck driving simulator replicating the snow- and ice-prone I-80 freeway corridor, where 18 professional snowplow truck drivers completed baseline and CV scenarios using a Sterling AT9500 cab mounted on a 3-DoF platform; in contrast, Harms and Brookhuis [24] employed a 6-DoF simulator with a real Besturn B50 cockpit and integrated SmartEye eye-tracking to simulate a 15 km mountainous route with five sharp curves, involving 70 drivers of varying experience levels and testing five advisory modalities ranging from single visual to gradient audio-visual (GAV) feedback. While Xu et al. [23] focused on progressive advisory speeds (65–40 mph) and contextual warnings through a visual HMI interface under winter weather scenarios, Harms and Brookhuis [24] compared static and gradient cues delivered via both visual and audio channels, highlighting the role of interface complexity in influencing driver behavior. Both studies found significant behavioral adaptation to in-vehicle advisories, with Xu et al. [23] reporting speed reductions of –10.2% at 50 mph ($p < 0.001$) and –8.3% at 45 mph ($p < 0.001$), and demonstrating smoother speed regulation, particularly under icy conditions where no skid-off events occurred in the CV scenario versus two in the baseline, while Harms and Brookhuis [24] observed statistically stronger outcomes for gradient modes, with lower approach speeds, smoother deceleration ($F \approx 16–29$, $p < 0.001$), and substantial effect sizes ($\eta_p^2 = 0.077–0.600$), especially at critical transition points such as 60 km/h ($F = 22.19$, $p < 0.001$). Although Xu et al. [23] did not explore modality variation, Harms and Brookhuis [24] confirmed that GAV feedback outperformed simpler advisory types in reducing speed and enhancing compliance, particularly among less-experienced drivers, while expert drivers preferred minimal cues, suggesting the need for adaptive interface design. Importantly, while Harms and Brookhuis [24] quantified visual demand and confirmed all gaze durations remained within the NHTSA 2-second safety threshold despite increased complexity ($F \approx 13$, $p < 0.001$), Xu et al. [23] assumed constant attentiveness without measuring distraction, highlighting an area for methodological enhancement. Despite limitations such as the small sample in the study by Xu et al. [23] ($n = 18$) and assumed 100% message reliability in both studies, the convergence of results supports a greater than 90% likelihood that in-vehicle advisory systems, particularly those delivering dynamic and context-sensitive information, can meaningfully improve speed compliance and reduce safety-critical events across varying roadway and environmental conditions.

Together, these findings underline a key bridge: while CV-based advisory systems like in the study by Xu et al. [23] are effective in harmonizing speeds under extreme weather, the enhanced modality design from Harms and Brookhuis [24], specifically gradient and multimodal delivery, offers additional benefits by promoting earlier and smoother behavioral adjustments, indicating that future systems should integrate contextual precision with user-tailored feedback mechanisms to optimize road safety performance.

4. Conclusions and future research directions

This section covers two main aspects. First, DSs are powerful tools for investigating complex traffic and transportation phenomena. Second, their application in studying VSL strategies is emphasized, particularly in compliance, driver perception, behavior, and cognitive responses.

DSs provide safe, cost-effective, and controllable environments for exploring driver–vehicle–infrastructure interactions, while integration with traffic and network simulators enhances realism and supports the evaluation of cooperative systems such as V2X and C-ITS. Future work should improve simulator fidelity, standardize evaluation frameworks, and expand cross-cultural studies for broader applicability.

In VSL environments, DSs offer valuable insights into how drivers perceive, interpret, and respond to dynamic control strategies. Findings indicate that VSLs enhance road safety and traffic stability when designed with behavioral and contextual sensitivity. Compliance varies with psychological, environmental, and situational factors. Higher passing rates increased average speeds (up to 18 km/h) and lateral variability, especially among younger or aggressive drivers, who also showed up to 2.7 times longer compliance delays and slower braking. Conversely, smoother compliance occurred when transitions aligned with perceived control and safety, underscoring the importance of psychological comfort. Complex or variable VSL zones reduced lane changes by approximately19% but raised mental workload and lateral acceleration, revealing a safety–cognitive demand trade-off. Behavior-informed, simulator-calibrated VSLs reduced mean speeds by up to 25 km/h and speed variability to around 2.5 km/h, lowering crash risk by an estimated 23%. Gradual speed drops and optimized message spacing (approximately 200 m) improved compliance by $\beta \approx 1.5$–3 times. Drivers who clearly understood VSL messages showed 76% higher compliance, adjusting speed within a 400 m window (approximately 200 m before and after the sign), while connected-vehicle systems improved safety by reducing speeds up to 13% in adverse weather and preventing skid-offs. GAV feedback enhanced deceleration smoothness, especially for inexperienced drivers, without reducing visual attention. However, only approximately 42% detected VSL increases; unaware drivers-maintained speeds, on average 13 km/h lower, suggesting habituation and low situational awareness weaken effectiveness. Overall, adaptive, data-driven, and context-aware VSLs, supported by personalized messages and connected-vehicle integration, significantly improve compliance and safety.

Future research should couple DS studies with real-world traffic data and connected-vehicle technologies to enhance external validity. Expanding multi-driver and networked simulations will enable realistic modeling of cooperative behavior. Further, enhancing sensory fidelity (visual, auditory, motion) and standardizing evaluation protocols will improve comparability. Research should prioritize adaptive, heterogeneity-aware speed management that reflects driver-specific variability, environmental factors, and roadway geometry. Integrating DS experiments with AI-driven behavioral modeling and machine-learning-based predictive control can enable proactive VSLs responsive to real-time conditions. Cross-cultural and cross-network studies are also essential to develop globally applicable, data-driven, human-centered VSL strategies.

Acknowledgements

This study was carried out within the MOST – Sustainable Mobility National Research Centre and received funding from the European Union Next-GenerationEU (PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR) – MISSIONE 4 COMPONENTE 2, INVESTIMENTO 1.4 – D.D. 1033 17/06/2022, CN00000023). This manuscript reflects only the authors' views and opinions, neither the European Union nor the European Commission can be considered responsible for them. It was also partially funded by the project I CAN BE "Progetti di Rilevante Interesse Nazionale" (PRIN 2022 -MUR).

AI-assisted tools were used solely for language refinement, including GPT-based grammar-checking and English-polishing systems, the Grammarly extension, and QuillBot; all scientific content and the overall structure of the chapter were developed entirely by the research team.

Author details

Behnood Baiky*, Facundo Storani, Roberta Di Pace and Stefano de Luca
University of Salerno, Salerno, Italy

*Address all correspondence to: bbaiky@unisa.it

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] Garg T, Kaur G. A Systematic Review on Intelligent Transport Systems. Journal of Computational and Cognitive Engineering. 2023;**2**:175–188

[2] Yan X, Zhang H, Wu C. Research and development of Intelligent Transportation Systems. In: Proceedings - 11th International Symposium on Distributed Computing and Applications to Business, Engineering and Science, DCABES 2012. IEEE Computer Society; 2012, pp. 321–327

[3] Avcı İ, Koca M. Intelligent Transportation System Technologies, Challenges and Security. Applied Sciences (Switzerland). 2024;**14**. DOI: 10.3390/app14114646

[4] Grumert E, Ma X, Tapani A. Analysis of a cooperative variable speed limit system using microscopic traffic simulation. Transportation Research Part C: Emerging Technologies. 2015;**52**:173–186

[5] Khondaker B, Kattan L. Variable speed limit: A microscopic analysis in a connected vehicle environment. Transportation Research Part C: Emerging Technologies. 2015;**58**:146–159

[6] Del Serrone G, Cantisani G, Peluso P. Peer-review under responsibility of the Scientific Committee of the Transport Infrastructure and Systems (TIS ROMA 2024). Dynamic Signs and Variable Speed Limits to Enhance Road Safety and Traffic Efficiency. In Transportation Research Procedia. Amsterdam, The Netherlands: Elsevier B.V 2025. p. 575–582

[7] Aiman Affandi M, Hazwani Mokhtar N, Zahir Hassan M, et al. Accelerating Insight: A Thorough Systematic Review on Driving Simulators and Their Transformative Effect on Driver Behaviour. Journal of Advanced Research Design Journal homepage. 2026;**140**:39–55

[8] Blana. A Survey of Driving Research Simulators Around the World. Available from: https://eprints.whiterose.ac.uk/ [Accessed: 2025-December]

[9] Zhang S, Zhao C, Zhang Z, et al. Driving simulator validation studies: A systematic review. Simulation Modelling Practice and Theory. 2025;**138**:103020

[10] Stall DA, Bourne S. The National Advanced Driving Simulator: Potential Applications To Its And Ahs Research. In: Proceeding of the 6th Annual meeting of the Intelligent Transportation Society. 1996

[11] Aramrattana M, Larsson T, Jansson J, et al. Extended driving simulator for evaluation of cooperative intelligent transport systems. In: SIGSIM-PADS 2016 - Proceedings of the 2016 Annual ACM Conference on Principles of Advanced Discrete Simulation. Association for Computing Machinery, Inc; 2016, pp. 255–258

[12] Blana. Driving Simulator Validation Studies: A Literature Review. Available from: https://eprints.whiterose.ac.uk/ [Accessed: 2025-December]

[13] Čulík K, Štefancová V, Kalašová A. Driving Simulator as a Tool for Reaction Time Measurement. IOP Conference Series: Materials Science and Engineering. 2022;**1247**:012034

[14] De Winter J, Van Leeuwen PM, De Winter JCF, et al. Advantages and Disadvantages of Driving Simulators: A Discussion, Available from: https://www.researchgate.net/publication/281593035 [Accessed: 2025-December]

[15] Ali Y, Raadsen MPH, Bliemer MCJ. Effects of passing rates on driving behaviour in variable speed limit-controlled highways: Evidence of external pressure from a driving simulator study. Transportation Research Part F: Traffic Psychology and Behaviour. 2024;**104**:488–505

[16] Ali Y, Raadsen MPH, Bliemer MCJ. Modelling speed reduction behaviour on variable speed limit-controlled highways considering surrounding traffic pressure: A random parameters duration modelling approach. Analytical Methods in Accident Research. 2023;**40**. DOI: 10.1016/j.amar.2023.100290

[17] Storani F, Baiky B, Bruno F, et al. Developing Variable Speed Limit Scenarios for Comparative Analysis of Questionnaire Surveys and Driving Simulations. In: 2025 IEEE International Conference on Environment and Electrical Engineering and 2025 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe). IEEE, pp. 1–6

[18] Shi J, Liu M. Impacts of differentiated per-lane speed limit on lane changing behaviour: A driving simulator-based study. Transportation Research Part F: Traffic Psychology and Behaviour. 2019;**60**:93–104

[19] Montella A, Calvi A, D'Amico F, et al. A methodology for setting credible speed limits based on numerical analyses and driving simulator experiments. Transportation Research Part F: Traffic Psychology and Behaviour. 2024;**100**:289–307

[20] Lee C, Abdel-Aty M. Testing effects of warning messages and variable speed limits on driver behavior using driving simulator. Transportation Research Record: Journal of the Transportation Research Board. 2008;**2069**:55–64

[21] Matowicki M, Pribyl O. A driving simulation study on drivers speed compliance with respect to variable message signs. Journal of Intelligent Transportation Systems: Technology, Planning, and Operations. 2022;**26**: 613–623

[22] Yang G, Ahmed MM, Gaweesh S. Impact of Variable Speed Limit in a Connected Vehicle Environment on Truck Driver Behavior under Adverse Weather Conditions: Driving Simulator Study. Transportation Research Record: Journal of the Transportation Research Board. 2019;**2673**:132–142

[23] Xu Q, Fu R, Wu F, et al. A speed limit advisory system provided by in-vehicle HMI considering auditory perception characteristics for connected environment. Transportation Research Part F: Traffic Psychology and Behaviour. 2023;**92**:353–368

[24] Harms IM, Brookhuis KA. Dynamic traffic management on a familiar road: Failing to detect changes in variable speed limits. Transportation Research Part F: Traffic Psychology and Behaviour. 2016;**38**:37–46

Chapter 13

Trajectory Prediction for Collision Avoidance of Vulnerable Road Users in CCAM Scenarios Using Stacking Regression and Deep Learning

Raúl Parada and Rafael Corvillo

Abstract

Road accidents remain a critical concern within the Cooperative, Connected, and Automated Mobility (CCAM) ecosystem, particularly for Vulnerable Road Users (VRUs) such as cyclists, moped riders, and motorcyclists. These users typically lack access to advanced onboard sensors, yet often carry electronic devices capable of emitting valuable geospatial data. This chapter proposes a hybrid trajectory prediction framework based on stacking regression and deep learning models to enhance collision avoidance systems within CCAM operational domains such as urban driving and protected zones. The methodology leverages lightweight models optimized for real-time inference, ensuring low latency and minimal energy consumption, which are key requirements in CCAM applications. A large-scale SUMO–TraCI co-simulation is used to generate realistic trajectories for thousands of road users, including VRUs, under heterogeneous urban conditions with signalized intersections and risky behaviours. From these simulations, time-windowed geospatial sequences of latitude, longitude, and heading are constructed to train and compare multiple regression and deep learning architectures. Performance is evaluated in terms of prediction error over a 5-second horizon, execution time, and estimated CO_2 emissions. The best-performing stacking regressor and LSTM-based model are then integrated into a geometric collision detection module based on polygon intersection and a Monte Carlo algorithm for probabilistic risk estimation. Experimental results show improvements in execution time and computational efficiency compared to traditional baselines, while maintaining competitive prediction accuracy. The proposed framework supports earlier and more reliable collision warnings for VRUs in CCAM environments and promotes a sustainable approach that balances safety performance with computational and environmental costs.

Keywords: collision avoidance, trajectory prediction, stacking regression, deep learning, vulnerable road users, vehicle to everything

1. Introduction

Vulnerable Road Users (VRUs), pedestrians, cyclists and scooters riders, remain a major safety concern in urban traffic. Worldwide, road traffic injures and fatalities disproportionately affect VRUs in mixed-traffic urban contexts, and their protection is a central objective of modern traffic-safety frameworks. Improving VRU safety requires a combination of sensing, prediction, and cooperative reaction across vehicles and infrastructure. To situate our work we adopt the commonly used automation taxonomy (SAE J3,016): automation Levels 0–2 cover driver assistance features (driver remains engaged), Level 3 introduces conditional automation with fallback requirements, and Levels 4–5 approach full driving automation under specified or all conditions. In this framework, Advanced Driver Assistance Systems (ADAS) typically refers to Level 1–2 functions (e.g., adaptive cruise, lane-keep, basic collision alerts) that assist the human driver; Assisted/Autonomous Driving (AAD) refers to Level 3 + functions where the system executes driving tasks under certain operational design domains. Cooperative, Connected and Automated Mobility (CCAM) is the ecosystem that enables ADAS and AAD to operate cooperatively, exchanging perception, intent and control information between vehicles, VRUs and infrastructure. As mentioned above, vehicular accidents pose a significant global public health issue. Road traffic accidents are the leading cause of death for individuals aged 15–29, resulting in approximately 1.35 million fatalities annually [1]. Drivers and passengers constitute the majority of road users involved in accidents, ranging from 60 to 80%. Pedestrians and cyclists, though a smaller percentage, still form a substantial proportion, with pedestrians accounting for up to 20% of road traffic deaths in some countries, and cyclists 2–3%. Unlike vehicles equipped with advanced hardware like cameras and LiDAR, VRUs often lack such technology. However, in CCAM scenarios, VRUs can still be integrated into the safety ecosystem by leveraging geopositional data from embedded devices for trajectory prediction using machine learning techniques. Our proposed solution aims to enhance prediction promptness while ensuring low precision error, contributing to collision avoidance between road users and minimizing false alarms. This work builds upon experimental results from a previously published paper [2], aligning with CCAM goals of improving safety and coordination among all road users. The objectives of this paper are:

- To explore advanced regression techniques such as stacking regression (SR) and deep learning (DL) techniques to enhance VRU collision avoidance systems.
- To provide a large vehicular-driving dataset composed of geospatial information.
- To propose trajectory prediction algorithms and a Monte Carlo algorithm to estimate the collision probability.

Imagine a cyclist navigating through busy city streets without advanced sensors to detect potential collisions. Despite following traffic rules, the cyclist remains vulnerable to unforeseen dangers posed by other vehicles. This scenario underscores the urgent need for improved collision avoidance systems, especially for vulnerable road users (VRUs) like cyclists and pedestrians.

2. Background

Trajectory prediction plays a crucial role in collision prevention by addressing the dynamic interactions between moving vehicles and VRUs. Traditional machine learning methods such as Linear Regression, Gaussian Process, Support Vector Regressor, Random Forest Regressor, and Dynamic Bayesian Network have been extensively studied and contribute to accurate trajectory prediction by considering factors like velocity, acceleration, heading, and position [3]. Promising results from these comparisons have spurred exploration into advanced methods like Stacking Regression (SR) [4]. SR is an ensemble learning technique used to improve predictive performance by combining multiple regression models. In recent years, there has been substantial growth in deep learning (DL) techniques, particularly in autonomous driving research [5]. Recurrent Neural Networks (RNNs), especially Long Short-Term Memory (LSTM) networks, capture temporal dynamics in time series data. Solutions vary from modeling each road user's trajectory based on relative coordinates [5, 6] to predicting all agents' paths from video sequences using LSTM [7, 8]. In [9], a comparison is made between different solutions for predicting the trajectory of vehicles on a highway. The dataset used is NGSIM (Next Generation Simulation) US-101 [10], which is publicly available and contains 45 minutes of vehicle trajectories on US-101 between 7:50 and 8:35. The set contains over 6,000 vehicles captured at a rate of 10 Hz, and the trajectory is recorded with the (x, y) coordinates of the vehicle's front center. The compared models, in terms of the root mean square error (RMSE) of the forecasts over a 5-second prediction horizon, are a constant velocity (CV) Kalman filter (6.68 m), similar to the one used in [11]; a Gaussian mixture variational model based on maneuvering with a vehicle interaction module based on random Markov fields (C-VGMM + VIM) (5.99 m) [12]; a closed recurrent unit Gated Recurrent Units (GRU) model based on generative adversarial imitation learning (GAIL-GRU) (4.71 m) [13]; and a maneuver-based LSTM model (Maneuver-LSTM or M-LSTM) (4.66 m) [9]. The values in parentheses represent distance error in meters (m), calculated using the Haversine formula.

As described above, the M-LSTM and GAIL-GRU models achieved the best prediction results. This suggests that models employing deep learning and reinforcement learning techniques offer superior prediction performance compared to probabilistic machine learning models, such as C-VGMM. Additionally, when comparing the M-LSTM and GAIL-GRU models, M-LSTM exhibits a greater reduction in RMS values as the forecast horizon increases. While these results demonstrate satisfactory prediction accuracy, they were obtained under controlled highway conditions devoid of intersections or abrupt driver maneuvers, such as running a red light. Baixuan et al. [14] introduce a dynamic activity region prediction algorithm for pedestrian trajectory prediction in collision avoidance systems, enhancing road safety through precise trajectory forecasting. Nengchao et al. [15] present a trajectory prediction and collision warning model in a connected vehicle environment, enhancing road safety through improved cut-in collision avoidance strategies. Meng et al. [16] propose a multitask framework using raw LIDAR data for accurate vehicle trajectory prediction, enhancing road safety and collision avoidance in intelligent driving systems. Hou et al. [17] introduce an interactive trajectory prediction system using a structural-LSTM network that aids in collision avoidance by accurately forecasting surrounding road users' trajectories in autonomous driving systems, significantly reducing longitudinal and lateral RMS errors. Wang et al. [18] provide a real-time trajectory prediction method

using V2X communication that enhances the accuracy of intelligent connected vehicles (ICVs), reducing collision risks on urban roads, as demonstrated in the study. Gao et al. [19] propose a trajectory prediction method based on a graph attention network for accurately predicting human driver vehicle trajectories around ICV under mixed traffic flow on highways. This approach requires the interaction of surrounding vehicles. Guo et al. [20] investigated the kinematic response of electric two-wheelers in collisions, including the Head Injury Criterion (HIC 15) to establish injury prediction models for various scenarios. Zhu et al. [21] utilize intention information along with current state to predict and control the future trajectory of multiple vehicles at intersections. Furthermore, they incorporate collision cost penalty during training which significantly improves performance, especially in preventing V2V collisions. Li et al. [22] conducted simulations in a T-intersection and an 8-way roundabout, demonstrating that the prediction-based reachability method significantly reduces collision risk and minimizes conservatism in safety control. Yu et al. [23] introduce a deep learning-based prediction method for autonomous driving lane change behavior to improve road safety. Duan et al. [24] propose the CVAE-VGAE model for trajectory prediction. It incorporates a self-attention mechanism for enhanced learning. Gao et al. [25] introduce the Multi-Dimensional Uncertainties Collision Risk Assessment (MDU-CRA) method. This work utilizes an Extended Kalman Filtering for sensor perception uncertainty. Cai et al. [26] introduce the V-DGNN model for vehicle interaction, which captures temporal and spatial dependencies among vehicles. It incorporates spatiotemporal attention mechanisms for motion pattern extraction. A novel framework based on multiscale spatial-temporal graph is proposed by Tang et al. [27] where stacked spatial-temporal layers capture interactions at different temporal levels. Li et al. [28] developed a real-time optimal trajectory planning for autonomous driving for collision-free trajectory in longitudinal and lateral motions. The study improves vehicle trajectory prediction accuracy. Alsanwy et al. [29] use LSTM and GRU networks fed with data collected from 17 drivers in a simulator and incorporating driver braking patterns into predictions. To provide a more realistic representation of urban driving environments, where a significant portion of VRU accidents occur, we incorporate traffic lights, crossroads, and other traffic elements into our simulations. This study builds upon our prior research [2, 3] by integrating advanced regression techniques with a specific focus on vulnerable road users (VRUs). Unlike previous works that primarily addressed vehicle trajectories, this study incorporates diverse VRU types in realistic urban scenarios using SUMO simulations. Additionally, the use of deep learning models, such as LSTM, enhances prediction accuracy, providing a more comprehensive and robust collision avoidance system that addresses a wider array of real-world situations. Our approach includes diverse VRU types within SUMO simulations, providing a realistic urban scenario that was not previously addressed. The use of LSTM models represents a significant advancement in accurately predicting trajectories, offering a robust solution to real-world challenges faced by collision avoidance systems.

3. Methodology

This section presents the different phases of our work: A) data generation (SUMO co-simulation + TraCI), B) Stacking Regression model design and selection, C) Deep Learning architecture design and tuning, D) trajectory prediction and collision detection (polygon intersection), and E) probabilistic collision estimation via Monte

Carlo sampling. Each stage has a specific purpose: (A) produces realistic time-series trajectory windows for both colliding and non-colliding road users; (B–C) produce candidate predictors optimized for accuracy and execution efficiency; (D) converts predictions to geometric occupancy for collision checks; (E) quantifies uncertainty and yields collision probability estimates for decision thresholds.

3.1 Dataset generation

In our simulations, parameters for VRUs are randomly selected and modified using the Traffic Control Interface (TraCI) [30]. These parameters include acceleration, deceleration, size, maximum speed, and driver imperfection, tailored to represent realistic VRU behaviors. The following values represent an example of those used for a regular-sized car, with these same parameters specified for each road user type:

- **Acceleration (m/s^2)**: Follows a Gaussian distribution $\mathcal{N}(3.3, 0.5)$.
- **Deceleration (m/s^2)**: Follows a Gaussian distribution $\mathcal{N}(5.5, 0.5)$.
- **Length and Width (m)**: The size of the road user changes depending on its type. For instance, the passenger class has the dimensions of 5.5 m x 1.5 m.
- **Maximum speed (m/s)**: Follows a Gaussian distribution $\mathcal{N}(8.3, 4)$, and only accepts values larger than 7.
- **Sigma**: The driver imperfection (0 denotes perfect driving). Follows a Gaussian distribution $\mathcal{N}(0.5, 0.3)$, but only accepts values from 0 to 1.
- **Tau**: The driver's desired (minimum) time headway, based on the net space between the leader's back and the follower's front. Follows a Gaussian distribution $\mathcal{N}(1, 0.25)$, but only accepts values from 0 to 1.
- **Apparent deceleration (m/s^2)**: The apparent deceleration of the road user in m/s^2. The follower uses this value as the expected maximal deceleration of the leader. Follows a Gaussian distribution with a deviation of 0.5 from the original declaration of the leader, $\mathcal{N}(\text{decel}, 0.5)$.

Certain simulated vulnerable road users exhibit reckless behavior, enabling the generation of frontal collisions due to discrepancies in acceleration, deceleration, and safety distance between VRUs. SUMO manages the decision engine that controls VRU movements, attempting to simulate safe driving and avoid potentially hazardous scenarios. However, we have modified the SPEED MODE parameter of some road users to increase the frequency of accidents, allowing them to ignore traffic signals and potentially cause lateral collisions at intersections. The SPEED MODE value is set to 39, permitting road users to proceed through a red traffic light even if the intersection is occupied. Consequently, by implementing these modifications, both frontal and lateral collisions can be recreated within the SUMO simulator. **Figure 1** illustrates the SUMO simulation setup for the Via Augusta scenario, where VRU trajectories are simulated under realistic urban conditions. The TraCI tool can also generate an output file containing a record of the simulation's



Figure 1.
SUMO simulation of barcelona via augusta scenario.

collisions, along with the positions and velocities of all simulation VRUs, to extract information about the collisions. Drawing upon the extracted information, we constructed an initial large dataset encompassing 7,914,246 observations. These observations correspond to the trajectories of 9,981 road users, of which 4,002 experienced collisions. Given that trajectories are considered time-series data associated with thousands of road users, we generated records with trajectory windows of 20 seconds as input and the window with the subsequent 5 seconds as output. The procedure for this is illustrated in **Figure 2**. Additionally, the dataset windowing procedure generated a test set containing the final trajectories of the road users involved in collisions and those that experienced no collisions. Hence, the dataset consists of geospatial data for various road users, including attributes such as latitude, longitude, speed, heading, and vehicle dimensions. It includes thousands of road users, with detailed tracking for those involved in collisions. Features like acceleration, deceleration, and road user behavior under different traffic conditions were incorporated to improve the model's realism and diversity. Building on the findings presented in [3], we conducted further analysis and selected the attributes *latitude*, *longitude*, and *heading* for training the models. To ensure representativeness,

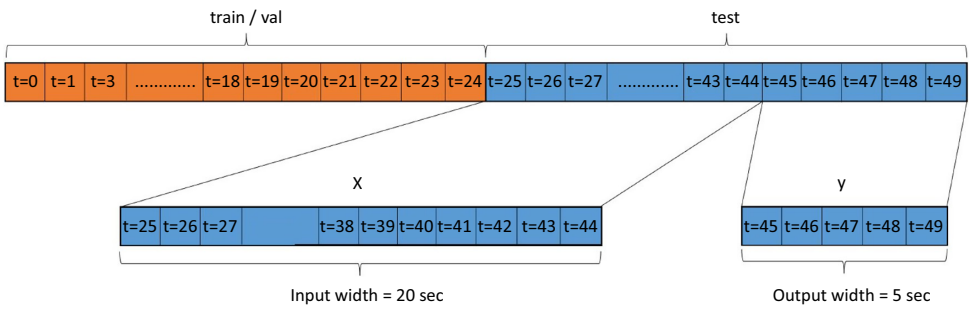


Figure 2.
Generation of data windows.

our dataset includes geospatial information from diverse urban traffic scenarios, incorporating different weather conditions, times of day, and environmental factors. However, biases may still exist, particularly in over-representing urban environments. To mitigate this, we applied random sampling techniques to ensure a balanced dataset and are working on expanding our data collection to include rural and suburban settings.

3.2 Stacking regression architecture design

Stacking Regression, or Stacked Generalization [4], is an ensemble learning technique used in regression tasks to amalgamate predictions from various base regression models, enhancing predictive performance. SR exploits diverse models with varying strengths and weaknesses, allowing them to complement each other for more accurate predictions. The SR process involves:

- **Base Regression Models**: Diverse models like Linear Regression, Decision Trees, Random Forests, and Support Vector Regression are individually trained on the data.
- **Feature Generation**: Predictions from base models create a new feature matrix, serving as input for the next level.
- **Meta Model**: A meta-model, or meta-regressor, is trained on the new feature matrix, learning to predict the target variable based on combined base model predictions.
- **Prediction**: The trained SR model predicts new data by feeding base model predictions into the meta-model.

The idea behind SR is to leverage diverse base models to capture complex patterns, creating a robust predictor. Choosing base regression models is crucial, employing a diverse set to capture various data patterns. The meta-model can be any regression model, such as Linear Regression (LR) or ensemble techniques like Gradient Boosting. Techniques from Scikit-Learn, including LR, RANSAC Regression (RR), Support Vector Regressor (SVR), Gaussian Process Regression (GPR), Multilayer Perceptron Regressor (MPR), Decision Tree Regressor (DTR), XGBoost Regressor (XR), Ridge Regressor (RiR), KNeighbors Regressor (KNR), Kernel Ridge Regressor (KRR), Lasso Regressor (LaR), LGBM Regressor (LGBMR), and Elastic Net Regressor (ENR), are utilized. The goal is to explore stacking regressor combinations, analyze model performance patterns, and identify the best model for accurately predicting collision probabilities. Different base models and architectures are studied:

- **No middle-layer models, two base-models:** One base layer with two models. (e.g., Linear Regression and RANSAC Regressor in the first level layer, and Decision Tree Regressor as Meta Learner)
- **No middle-layer models, three base-models:** One base-layer with three models. (i.e., Linear Regression, RANSAC Regressor, and Gaussian Process Regressor in the first level layer, and Linear Regression as Meta Learner).

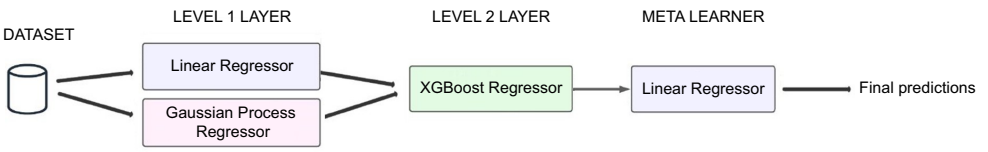


Figure 3.
Example of one middle-layer, two base-models.

- **No middle-layer models, four base-models:** One base layer with four models. For instance, Linear Regression, RANSAC Regressor, Gaussian Process Regressor, and XGBoost Regressor in the first level layer, and Decision Tree Regressor as Meta Learner.

- **One middle-layer, two base-models:** In **Figure 3**, we can observe how this Stacking Regression architecture is built. For instance, Linear Regression and Gaussian Process Regression in the base layer, XGBoost Regressor in the second layer, and Linear Regressor as Meta Learner.

The selection of meta-learners in the second and fourth architectures was based on their ability to handle non-linear data patterns. Decision Tree Regressors were not used in all architectures because alternative learners such as XGBoost and Gaussian Process were tested for their superior performance in capturing more complex interactions between variables. We selected stacking regression due to its ability to combine multiple base models and improve predictive accuracy, particularly in environments with complex, nonlinear data. While alternatives such as reinforcement learning (RL) offer dynamic, adaptive capabilities, RL typically requires extensive training and computational resources, which may limit real-time applicability. Our models were chosen for their balance between accuracy and computational efficiency, particularly in predicting the trajectories of VRUs in urban environments.

3.3 Deep learning architecture design

With reference to our prior work [3], we possess a larger sample size, enabling exploration of DL techniques. To facilitate comparison, we designed and tested various DL architectures, detailing the layer configuration (LC) and total number of parameters (TNP) for each model to ensure reproducibility:

- **Simple models (SM):** Metrics include GRU and LSTM layers with varying cell numbers. LC: gru/lstm, dense, reshape. TNP: 4,047/5,103.

- **Stacked model (SaM):** Combining two LSTM vs GRU layers, testing different unit combinations. LC: lstm, lstm, dense, reshape. TNP: 13,423.

- **Bidirectional model (BM):** Incorporates a bidirectional LSTM layer, training the network with input sequences in both directions. LC: bidirectional, dense, reshape. TNP: 10,191.

- **Encoder-decoder model (EDM):** Utilized for sequence-to-sequence predictions. LC: lstm, repeat vector, lstm, time distributed. TNP: 13,027.

- **Simple model with attention mechanism (SMwAM):** Employs an attention mechanism to focus on specific inputs. LC: lstm, attention, dense, reshape. TNP: 26,095.

Model configurations include:

- **Epochs:** Number of times the entire training set is used.

- **Batch size:** Size of batches for training set division.

- **Optimizer:** Adam algorithm, which is an adaptive gradient descent method, with a learning rate of 0.001.

- **Early stopping:** Halts training when the model ceases to learn.

- **ReduceLROnPlateau:** Slows learning when the model's improvement stalls. Values for these parameters were determined through initial testing, balancing performance, and training time.

After model training, metrics include:

- **Prediction error ϵ (m):** This distance will be determined using the haversine function. It will calculate the distance between the last predicted value and the actual values, which provides the distance in meters between the predicted and real positions. This evaluation metric allows for quantifying the models' effectiveness in capturing the true trajectory and provides insights into their predictive capabilities. The prediction error will be measured at each horizon step, up to 5 seconds.

- **Execution time (ET)(s)**: Indicates the total time, in seconds, that the training has lasted.

- **Emissions CO_2 (ECO2)(g)**: Indicates the CO_2 emissions, in grams, that have occurred during the execution of the training code. We use the Python library CodeCarbon to perform this measurement[31].

- **Evaluation metrics**: Accuracy is the percentage of predictions that a model gets correct. Precision is the percentage of positive predictions that are actually positive. Recall is the percentage of positive instances that are correctly identified. Specificity is the percentage of negative instances that are correctly identified. F1–Score is a measure of accuracy that takes into account both precision and recall.

3.4 Trajectory prediction

For collision detection, we employ a method that computes the intersection of each road user's polygons, involving the following steps:

1. Predict the trajectory for the next 5 seconds for both road users.

2. Extract the predicted latitude, longitude, and direction for the fifth second of both road users, considering potential collisions in the last second of the sequence.

3. Using the three aforementioned attributes and road users' dimensions, calculate the points of the rectangle containing each road user.

4. Generate the polygon for each road user based on the calculated points.

Check if the polygon intersection is greater than zero, denoted as $v_1 \cap v_2 \neq \emptyset$, where v_1 is the polygon of road user 1, v_2 is the polygon of road user 2 and $\emptyset$ is the empty set.

We applied these steps to 1,000 pairs of colliding and non-colliding road users, resulting in a confusion matrix for model performance evaluation.

3.5 Estimation of collision probability

To compute collision probability, we developed Algorithm 1 inspired by [32]. This algorithm is a Monte Carlo algorithm that estimates the probability of collision from the probabilistic models of the road users. The probability of collision is computed from integrals of Gaussians and takes into account the uncertain configurations and the volume of both the road user and the obstacles. In simpler terms, the paper uses mathematical models to estimate the likelihood of a collision between a road user and an obstacle, taking into account the uncertainty in the position and size of both the road user and the obstacle. The vehicle's motion is modeled by standard kinematic equations, where velocity $v(t)$, position $p(t)$, and acceleration $a(t)$ are functions of time. We use a probabilistic model to estimate future trajectories, with uncertainty modeled by Gaussian distributions. The collision probability is derived from the Monte Carlo algorithm, where the likelihood of intersection between two road users' paths is computed using the formula:

$$P_{\text{collision}} = \int_{\text{domain}} f_{\text{trajectory}}(x)\, dx$$

The algorithm 1 represents the probability density function (PDF) of both road users' predicted trajectories. We compute the PDF of the 5-second trajectories of each road user, which includes the latitude, longitude, and angle of each road user at each time step. Thereby, calculates the distance between the two trajectories at each time step using the haversine formula, which takes into account the curvature of the Earth. Later, calculates the probability of a collision at each time step using a Gaussian distribution, which is based on the distance between the two trajectories. Finally, the algorithm calculates the overall collision probability by taking the average of the collision probabilities at each time step. This procedure is performed N times, it means, an N random samples are drawn from these PDFs to check if a collision is detected (c.f. Section 3.4). Ultimately, the collision probability is calculated by dividing the total number of detected collisions by the total number of samples.

Algorithm 1 Probability estimation of collision between two road users

Require: 5-second trajectory from each road user $x_v = (lat_t, long_t, \theta_t)$.
Ensure: Collision probability P_{coll}.

1: $P_{coll}(v_1, v_2) \leftarrow 0$
2: **for** $j \leftarrow 1$ *to* N **do**
3: $x_{v1} \leftarrow randc(\hat{x}_{v1}, \Sigma_{v1})$
4: $x_{v2} \leftarrow randc(\hat{x}_{v2}, \Sigma_{v2})$
5: **if** $v_1 \cap v_2 \neq \varnothing$
6: $P_{coll}(v_1, v_2) \leftarrow P_{coll}(v_1, v_2) + 1$
7: **end if**
8: **end for**
9: $P_{coll}(v_1, v_2) \leftarrow \frac{P_{coll}(v_1, v_2)}{N}$
10: **return** $P_{coll}(v_1, v_2)$

The algorithm estimates the collision probability between two road users using Monte Carlo simulations. The Algorithm 1 does:

- **Line 1–2**: The algorithm initializes the collision probability $P_{coll}(v_1, v_2)$ to 0 for two road users v_1 and v_2, based on their 5-second trajectory data x_v, which consists of latitude, longitude, and heading angle θ_t.
- **Line 3**: A loop runs N times, where N is the number of Monte Carlo samples used for the simulation.
- **Lines 4–5**: In each iteration of the loop, the algorithm generates random samples of the trajectories for both road users using the function *randc*, which returns a random sample from the Gaussian distribution of predicted trajectories $\hat{x}_v$ with covariance Σ_v.
- **Line 6–7**: The algorithm checks whether the two road users' trajectories intersect (denoted by $v_1 \cap v_2 \neq \varnothing$). If an intersection is detected, the collision probability P_{coll} is incremented by 1.
- **Line 9**: After all iterations, the collision probability is averaged by dividing the number of collisions by the total number of samples, N, resulting in the final estimated collision probability.
- **Line 10**: Finally, the algorithm returns the estimated collision probability $P_{coll}(v_1, v_2)$, which can be used to assess the likelihood of a collision between the two road users over the 5-second prediction horizon.

To enhance the clarity of the algorithm and ensure that the notations used are well understood, we provide **Table 1** that explains the key symbols used in the collision probability estimation algorithm. This table will help the reader follow the pseudocode and equations more easily.

The mathematical models employed in this work estimate collision probabilities by calculating the intersection of predicted trajectories, taking into account

Symbol	Meaning
θ	Heading angle of the road user
x,y	Latitude and longitude coordinates
$P_{\text{collision}}$	Probability of collision
v_1, v_2	Road users involved in potential collision
Σ_v	Covariance matrix of predicted trajectories
$\hat{x}_v$	Predicted trajectory of the road user
N	Number of Monte Carlo samples

Table 1.
Table of notations.

uncertainties in position and movement. The trajectory is modeled as a time series, and the collision probability is computed using the Monte Carlo method, where the random sampling of trajectories helps approximate the likelihood of interSect.

4. Experimental results

This section compiles executions employing both Stacking Regression (SR) and Deep Learning (DL) approaches. Google Colab is utilized for all experiments, divided into three blocks: A) Prediction Accuracy, showcasing the precision of 5-second trajectory predictions; B) Model Evaluation, emphasizing common metrics for assessing AI model performance; and C) Collision Probability Estimation, crucial for accident prevention systems.

4.1 Prediction accuracy

We compare the models described in Sect. 3.2 in terms of average distance error (ϵ), execution time (ET), and CO2 emissions (ECO2) for 4,000 road users. We have chosen this number of road users since they are enough for experimental comparing. First, in **Table 2**, these metrics are shown for individual models.

The results obtained in terms of average distance error (ϵ), execution time (ET), and CO2 emissions (ECO2) reveal interesting insights into the performance of each individual model in predicting the trajectory over a 5-second interval.

- **Average distance error:** In terms of trajectory distance error, some models stand out with lower error distances at each time interval. Linear Regression (LR) (15.91 m), Decision Tree Regressor (DTR) (17.69 m), XGBoost Regressor (XR) (18.52 m), KNeighbors Regressor (KNR) (18.81 m.), and Lasso Regressor (LaR) (19.77 m) exhibit relatively lower error distances compared to other models. These models demonstrate better precision in predicting the coordinates at each time step, indicating higher accuracy in capturing the trajectory. On the other hand, models such as Supported Vector Regressor (SVR) (60.30 m), Ridge Regressor (RiR) (45.60 m), Multilayer Perceptron Regressor (MPR) (63.27 m), Kernel Ridge Regressor (KRR) (58.86 m) and LGBM Regression (LGBMR) (30.23 m) show significantly

Model	t = 1 ϵ (m)	t = 2 ϵ (m)	t = 3 ϵ (m)	t = 4 ϵ (m)	t = 5 ϵ (m)	ET(s)	ECO2(g)
LR	2.86	5.79	9.18	12.40	15.91	158	0.94
RR	5.08	9.65	12.95	17.05	20.28	250	1.48
GPR	3.66	8.16	15.40	19.35	20.65	159	2.49
DTR	3.68	6.99	10.52	14.13	17.69	139	0.64
XR	4.20	7.72	11.34	15	18.52	1,141	5.23
KNR	5.33	7.89	11.58	15.26	18.81	168	1.55
SVR	63.89	63.45	61.91	60.86	60.30	202	1.21
MPR	60.72	62.77	64.87	66.16	63.27	1,605	31.54
ENR	5.10	9.47	13.60	17.65	21.31	725	60.2
LaR	4.70	8.51	12.40	16.20	19.77	876	71.5
RiR	19.07	29.87	37.33	41.55	45.60	138	1.02
KRR	38.33	47.61	52.29	56.24	58.86	331	2.13
LGBMR	15.99	20.56	24.04	27.32	30.23	1,068	90.1

Table 2.
Error distance and execution time for each individual model.

higher error distances. This suggests that these models struggle to accurately capture the trajectory, resulting in larger deviations between the predicted and actual coordinates.

- **Execution time:** Regarding execution time, the models vary considerably. Linear Regression (LR) (158.09 s), Decision Tree Regressor (DTR) (139.15 s) and KNeighbors Regressor (167.75 s) show relatively shorter execution times, indicating faster predictions. In contrast, models like Multilayer Perceptron Regressor (MPR) (1604.78 s) and LGBM Regressor (LGBMR) (1067.95 s) require considerably more time to run the model, suggesting higher computational complexity.

- **CO2 emissions:** CO2 emissions provide insights into the environmental impact of using each model. Notably, MPR (31.54 g), ENR (60.2 g), LaR (71.5 g), and LGBMR (90.1 g) generate significantly higher emissions compared to other models. On the other hand, DTR (0.64 g) and LR (0.94 g) emit relatively lower amounts of CO2.

4.2 Stacking regression models

Next step, according to the previous results, we build diverse Stacking Regression architectures by combining the tested traditional machine learning techniques. Thereby, **Table 3** presents the created SR models.

Based on the information provided in **Table 3**, a comprehensive analysis of the models reveals that certain combinations of techniques have exhibited more promising results. Specifically, models that incorporate Linear Regression (LR), Decision Tree Regressor (DTR), RANSAC Regression (RR), XGBoost Regressor (XR), KNeighbors Regressor (KNR), and Elastic Net Regressor (ENR) have shown

Model	t = 1 ϵ (m)	t = 2 ϵ (m)	t = 3 ϵ (m)	t = 4 ϵ (m)	t = 5 ϵ (m)	ET(s)	ECO2(g)
No middle-layer, two base models							
LR–RR/DTR	3.37	6.95	10.71	14.58	18.34	1,334	97
LR-SVR/RiR	44.44	52.25	56.53	59.55	60.91	217	32
LR-DTR/LR	5.91	11.76	17.70	23.73	28.50	1,341	54
LR-MPR/LR	5.89	11.77	17.67	23.75	28.87	3,791	155
LR–XR/RiR	17.20	31.35	41.92	47.42	51.91	9,000	336
XR-GPR/RiR	37.94	49.96	55.29	57.88	58.04	2,719	12
LR-GPR/LR	4.40	9.26	14.53	20.12	25.57	1,291	41
KNR-XR/LR	4.11	8.81	13.98	19.53	25.28	5,916	242
KNR-DTR/LR	3.36	6.95	10.70	14.56	18.31	651	51
KNR-XR/DTR	4.09	8.75	13.88	19.35	25.02	6,189	198
LR-KNR/XR	4.74	9.93	15.42	21.16	26.96	7,522	297
LR–XR/KNR	4.09	8.75	13.86	19.33	25.01	5,633	204
KNR-LR/KNR	3.36	6.94	10.69	14.55	18.30	631	45
XR-GPR/LR	4.08	8.73	13.83	19.29	24.82	7,391	495
ENR-RR/LR	6.12	11.85	17.87	23.54	28.44	4,656	184
LaR-LR/DTR	5.02	10.68	16.45	22.52	28.64	3,716	148
No middle-layer, three base models							
LR-DTR-KNR/LR	4.09	8.75	13.88	19.35	25.00	631	72
LR-DTR-KNR/DTR	4.14	8.82	14.10	19.64	25.21	919	49
LR-DTR-KNR/KNR	4.44	9.42	14.84	20.66	26.40	872	59
XR-DTR-LaR/LR	4.10	8.81	13.97	19.52	25.24	7,307	267
LaR-KNR-ENR/DTR	5.01	10.60	16.35	22.44	28.57	7,415	289
No middle-layer, four base models							
LR–XR-KNR-DTR/LR	5.02	10.67	16.45	22.51	28.58	6,598	232
LR–XR-KNR-DTR/KNR	5.02	10.67	16.44	22.52	28.63	6,435	231
LR–XR-KNR-DTR/DTR	4.28	9.19	14.73	21.06	26.73	7,456	243
LR–XR-KNR-DTR/XR	4.44	9.00	13.84	19.32	24.53	8,297	254
Two base models, one level 2 model							
LR-GPR/XR–LR	4.47	9.06	14.04	19.42	24.73	6,331	242

Table 3.
Error distance and execution time for each stacking regression model.

superior performance in terms of accuracy and computational efficiency. Comparing the error metrics across different time intervals, these models consistently demonstrate lower errors, indicating a higher degree of accuracy in predicting the trajectory of a vehicle within the given time frame. Notably, the LR–RR/DTD model stands out as one of the top performers (18.34 m), showcasing consistently low

errors across all time intervals. The superior performance of the LR–RR/DTD model can be attributed to its ability to capture linear relationships in the data while also leveraging decision trees for handling more complex, nonlinear interactions. In contrast, models that involve Multilayer Perceptron Regressor, Gaussian Process Regressor (GPR), and Support Vector Regressor (SVR) exhibit relatively poorer performance, as evidenced by higher error values. These models, while more complex, fail to achieve the same level of accuracy as the aforementioned LR, DTR, XR, KNR, RR, and ENR models. Furthermore, it is crucial to consider the computational implications of the models. Models with a larger number of base models or higher levels of stacking tend to have longer execution times. This is evident in **Table 3**, where certain models show significantly higher execution times, such as LR–XR-KNR-DTR/XR (8,297 s). Additionally, higher execution times often correlate with increased carbon emissions, as indicated by the emissions values in **Table 3**. Given these findings, it is recommended to prioritize the models that combine LR, DTR, XR, KNR, and ENR techniques. These models strike a favorable balance between accuracy, computational efficiency, and environmental impact. Their ability to achieve accurate predictions while maintaining reasonable execution times and emissions makes them more practical choices for trajectory prediction tasks.

4.3 Deep learning models

Since we dispose of a large dataset and the results from both individual and Stacking Regression techniques did not improve considerably. We execute the deep learning architectures described in Sect. 3.3 using different combinations. It is worth mentioning that for simplicity, we have named each combination as the following: the abbreviated DL model plus the type of architecture (GRU or LSTM) and the number of cells separated with a dash. In case there are two layers, their number of cells will be shown with an underscore between these values. The results of the models tested are presented in **Table 4**, summarizing their prediction precision and other relevant metrics.

As we can observe in **Table 4**, deep learning techniques outperformed in terms of position error, execution time and the CO2 emission. The worst average distance error at the fifth step is the Simple Model using the LSTM approach with 32 cells, resulting in 13.18 meters of error. This result is lower than the best model from all Stacking Regression architectures. We will further study the above models to evaluate their performance. The optimal model is identified as the Simple Model using the LSTM approach with 64 cells, resulting in 12.088 meters of error and the highest F1-score (see **Figure 4**). Validation evaluation confirms the suitability of the selected DL model, surpassing the best Stacking Regression architectures. Further study is planned to evaluate their performance. **Figure 4** demonstrates the training loss and mean absolute error for the SM-LSTM64 model, indicating its convergence and suitability for the task.

The promising results from our LSTM models, with an average error distance of 12.08 meters, suggest substantial improvements in predicting VRU trajectories in controlled simulations. These models can be integrated into real-time traffic management systems, potentially reducing the likelihood of

Model	t = 1 ϵ (m)	t = 2 ϵ (m)	t = 3 ϵ (m)	t = 4 ϵ (m)	t = 5 ϵ (m)	ET(s)	ECO2(g)
SM-GRU32	2.92	4.64	7.11	9.30	12.94	3,501	14.62
SM-GRU64	2.05	3.79	6.27	9.09	12.09	6,317	44.18
SM-GRU128	1.80	3.57	5.90	8.57	11.46	17,364	131.5
SM-LSTM32	3.13	4.62	7.04	9.95	13.18	3,738	22.21
SM-LSTM64	2.39	4.11	6.71	9.48	12.46	8,314	58.14
SM-LSTM128	1.64	3.43	5.82	8.58	11.63	38,124	142.88
SaM-GRU32_32	2.93	3.84	6.12	9.06	12.22	6,212	17.82
SaM-GRU64_32	2.60	3.89	5.99	9.27	12.23	11,221	42.1
SaM-GRU64_64	2.16	3.55	5.92	8.72	11.90	26,117	74.9
SaM-LSTM32_32	3.14	4.02	6.28	9.13	12.22	14,785	55.41
SaM-LSTM64_32	2.55	3.76	5.97	8.59	11.41	18,445	203.27
SaM-LSTM64_64	2.73	3.65	5.70	8.28	11.28	38,310	143.57
BM-LSTM32	2.52	4.16	6.6	9.35	12.5	4,785	8.72
BM-LSTM64	1.83	3.56	6.01	8.87	12.01	16,920	30.82
EDM-LSTM32	3.04	4.19	6.76	9.36	12.19	5,412	32.16
EDM-LSTM64	2.2	3.78	6.01	8.66	11.55	11,865	54.39
SMwAM-LSTM64_32	1.91	3.53	6.00	8.83	11.86	10,525	19.17
SMwAM-LSTM64_64	1.95	3.63	5.98	8.87	11.95	18,745	34.14
SMwAM-LSTM32_32	2.55	4.09	6.53	9.38	12.51	10,284	38.54
SMwAM-LSTM32_64	2.10	3.72	6.12	8.94	11.95	5,076	9.25

Table 4.
Error distance and execution time for deep learning models.

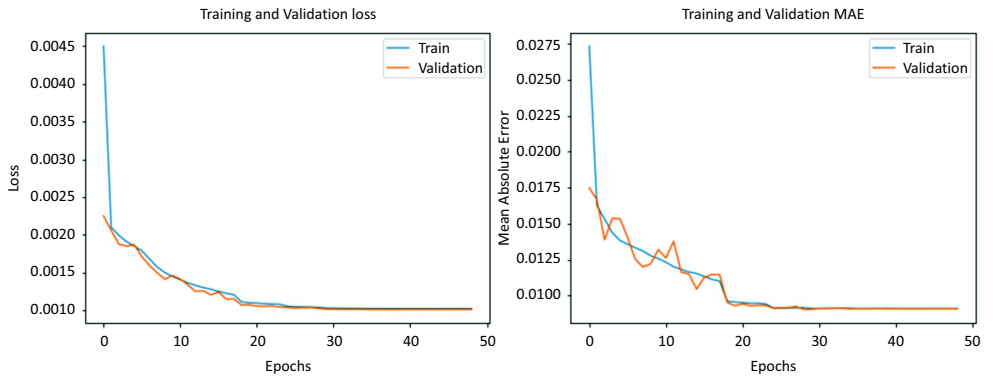


Figure 4.
Loss and mean absolute error plots from SM-LSTM64 model.

VRU accidents in urban environments. Future work will focus on validating these models in live traffic environments with unpredictable pedestrian and cyclist behavior.

4.4 Model evaluation

The metrics of the collision detection with the previously trained models are shown in **Table 5**, as well as the collisions and no collisions that were well predicted. The metrics calculated are Accuracy, Precision, Recall, Specificity and F1-score:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}, \tag{1}$$

$$\text{Precision} = \frac{TP}{TP + FP}, \tag{2}$$

$$\text{Recall} = \frac{TP}{TP + FN}, \tag{3}$$

$$\text{Specificity} = \frac{TN}{TN + FP}, \tag{4}$$

$$\text{F1} - \text{score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{5}$$

Where *TP*, *TN*, *FP*, and *FN* represent true positives, true negatives, false positives, and false negatives, respectively.

Some conclusions can be inferred from **Table 5**. Models that combined Linear Regression (LR), Decision Tree Regressor (DTR), XGBoost Regressor (XR), KNeighbors Regressor (KNR), and Elastic Net Regressor (ENR) tended to yield better results in terms of accuracy, precision, and recall. On the other hand, models that incorporated Multilayer Perceptron Regressor (MPR), Gaussian Process Regressor (GPR), and Supported Vector Regressor (SVR) showed lower performance and are unrecommended for further training, as mentioned in the previous subsection. It is worth noting that the number of base models did not necessarily correlate with improved accuracy, and some models exhibited longer execution times and severer environmental impact in terms of CO2 emissions.

All of them contain Linear Regression in the base-layer or as meta-regressor, a fact that could be predicted by the results obtained in individual ML metrics (as LR only got 15.91 m. error in t = 5s). Based on the provided information, it is evident that the F1-Score for all models are relatively low, indicating a limited number of detected collisions. This observation is consistent with the average prediction errors for the fifth second, which are at best around 18 meters. For precise collision detection between vehicles, the prediction errors should ideally be less than a meter. Additionally, it is explicit that LSTM models perform better in this scenario, with prediction errors of 12 meters, demonstrating a closer fit to the problem at hand. However, it must be mentioned also that Stacking Regression models have higher specificity in the vehicles that do not collide. Considering that none of the models developed within Stacking Regression perform well in solving the problem, the ENR-RR/LR model is chosen as the final model. This decision is based on its superior robustness and better overall metrics compared to the other models. Although it may not yield optimal results, it exhibits the most promising performance among the available options. In the next section, both Stacking

Model	Acc.	Prec.	Recall	Spe.	F1-S.
Stacking Regression					
LR–RR/DTR	0.509	0.850	0.017	0.997	0.033
LR-SVR/RiR	0.501	1.000	0.001	1.000	0.002
LR-DTR/LR	0.504	0.706	0.012	0.995	0.024
LR-MPR/LR	0.501	0.750	0.003	0.999	0.006
LR–XR/RiR	0.503	0.857	0.006	0.999	0.012
XR-GPR/RiR	0.501	0.571	0.004	0.997	0.008
LR-GPR/LR	0.505	1.000	0.010	1.000	0.020
KNR-XR/LR	0.505	1.000	0.010	1.000	0.020
KNR-DTR/LR	0.503	1.000	0.006	1.000	0.012
KNR-XR/DTR	0.501	1.000	0.001	1.000	0.002
LR-KNR/XR	0.501	1.000	0.001	1.000	0.002
LR–XR/KNR	0.501	1.000	0.001	1.000	0.002
KNR-LR/KNR	0.501	1.000	0.002	1.000	0.004
XR-GPR/LR	0.504	1.000	0.008	1.000	0.016
ENR-RR/LR	0.508	0.944	0.017	0.999	0.033
LaR-LR/DTR	0.501	1.000	0.001	1.000	0.002
LR-DTR-KNR/LR	0.505	1.000	0.011	1.000	0.022
LR-DTR-KNR/DTR	0.506	1.000	0.012	1.000	0.024
LR-DTR-KNR/KNR	0.503	1.000	0.006	1.000	0.012
XR-DTR-LaR/LR	0.505	1.000	0.010	1.000	0.020
LaR-KNR-ENR/DTR	0.501	1.000	0.001	1.000	0.002
LR–XR-KNR-DTR/LR	0.504	1.000	0.008	1.000	0.016
LR–XR-KNR-DTR/KNR	0.504	1.000	0.007	1.000	0.014
LR–XR-KNR-DTR/DTR	0.504	1.000	0.007	1.000	0.014
LR–XR-KNR-DTR/XR	0.502	1.000	0.004	1.000	0.008
LR-GPR/XR–LR	0.506	1.000	0.012	0.995	0.024
Deep Learning					
SM-GRU32	0.502	0.537	0.029	0.975	0.055
SM-GRU64	0.500	0.500	0.034	0.966	0.064
SM-GRU128	0.513	0.662	0.051	0.974	0.095
SM-LSTM32	0.505	0.605	0.026	0.983	0.050
SM-LSTM64	0.507	0.588	0.005	0.967	0.087
SM-LSTM128	0.510	0.643	0.045	0.975	0.084
SaM-GRU32_32	0.506	0.570	0.045	0.966	0.083
SaM-GRU64_32	0.506	0.597	0.037	0.975	0.070
SaM-GRU64_64	0.501	0.509	0.029	0.972	0.055
SaM-LSTM32_32	0.500	0.492	0.029	0.970	0.055
SaM-LSTM64_32	0.503	0.556	0.025	0.980	0.048

Model	Acc.	Prec.	Recall	Spe.	F1-S.
SaM-LSTM64_64	0.497	0.435	0.020	0.974	0.038
BM-LSTM32	0.507	0.600	0.039	0.974	0.073
BM-LSTM64	0.506	0.581	0.043	0.969	0.080
EDM-LSTM32	0.502	0.527	0.029	0.974	0.055
EDM-LSTM64	0.503	0.558	0.029	0.977	0.055
SMwAM-LSTM64_32	0.507	0.623	0.033	0.980	0.063
SMwAM-LSTM64_64	0.506	0.600	0.033	0.978	0.063
SMwAM-LSTM32_32	0.499	0.472	0.025	0.972	0.047
SMwAM-LSTM32_64	0.506	0.588	0.040	0.972	0.075

Table 5.
Model metrics.

Regression and Deep Learning the best model will be adopted to calculate the collision probability implementing the Monte Carlo method detailed in Sect. 3.5, to compare the models. Summarizing the above sections, **Figure 5** represents the process of choosing the two final algorithms. The initial techniques are the known AI techniques composed of traditional ML techniques and DL models combining LSTM and GRU architectures and using a diverse number of cells. The resulting techniques are compared until obtaining selected techniques for a further comparison. Finally, the compared techniques are the ones used in the following sections.

Figure 6 summarizes the section by comparing the performance of stacking regression models and deep learning models across the above evaluation metrics. Deep learning models generally show better performance in terms of accuracy, recall, and F1-score, indicating their ability to handle complex data and provide better overall predictions. However, this comes at a significant cost. Execution time, training time, and energy consumption are notably higher for deep learning models compared to stacking regression models. Stacking regression models, on the other hand, display more consistency in precision and specificity, with shorter training and execution times and lower energy consumption. This study emphasizes the trade-offs between performance and efficiency, suggesting that while deep learning models outperform in predictive accuracy, they are more resource-intensive, making stacking regression a more viable option in scenarios with limited computational resources or environmental concerns.

4.5 Collision probability estimation

In this subsection, our objective is to calculate the collision probability for a set of vehicle pairs using the algorithm we have described earlier. To achieve this, we will first evaluate the algorithm's performance by using the actual trajectories of the vehicles and establishing a decision threshold based on its output. Subsequently, the chosen model will be employed to predict the trajectories and apply the algorithm to

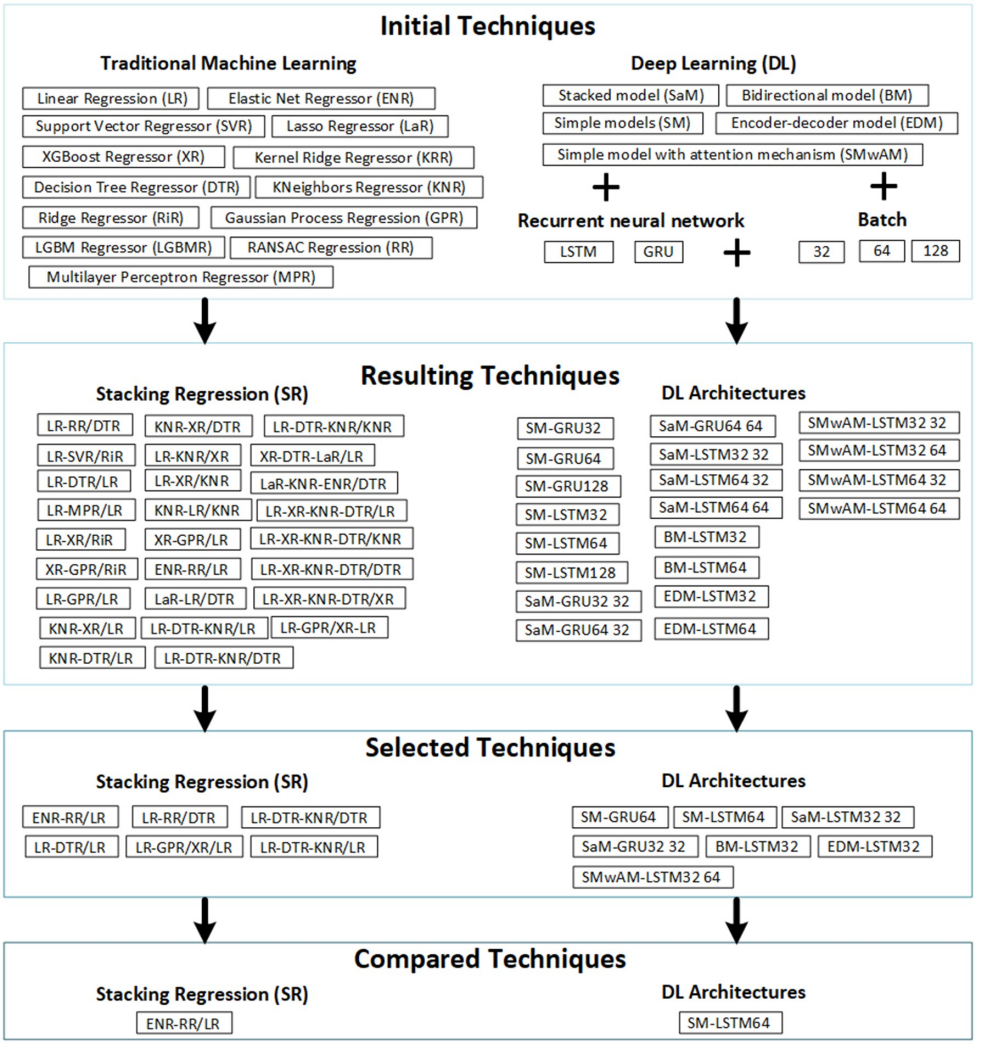


Figure 5.
Process on choosing the algorithms for comparison.

calculate collision probabilities for the same vehicle pairs. However, before executing the algorithms, the optimal number of random samples (N) to be used must be determined. Note that the variable N within the algorithm is customizable by the user. The rationale behind this variable is that as its value increases, the accuracy of the probability estimation improves; however, this also results in an increase in computational time. Given that our system must furnish collision predictions within a reasonable timeframe to be of practical use, it is not feasible to anticipate a vehicular position five seconds in the future when the computation time already takes four seconds. This circumstance leaves us with a mere one-second window to react and apply brakes in the event of a plausible real-world driving scenario. To accomplish this, a more in-depth study has been carried out for different values of N and an average collision probability has been obtained as well as the computation

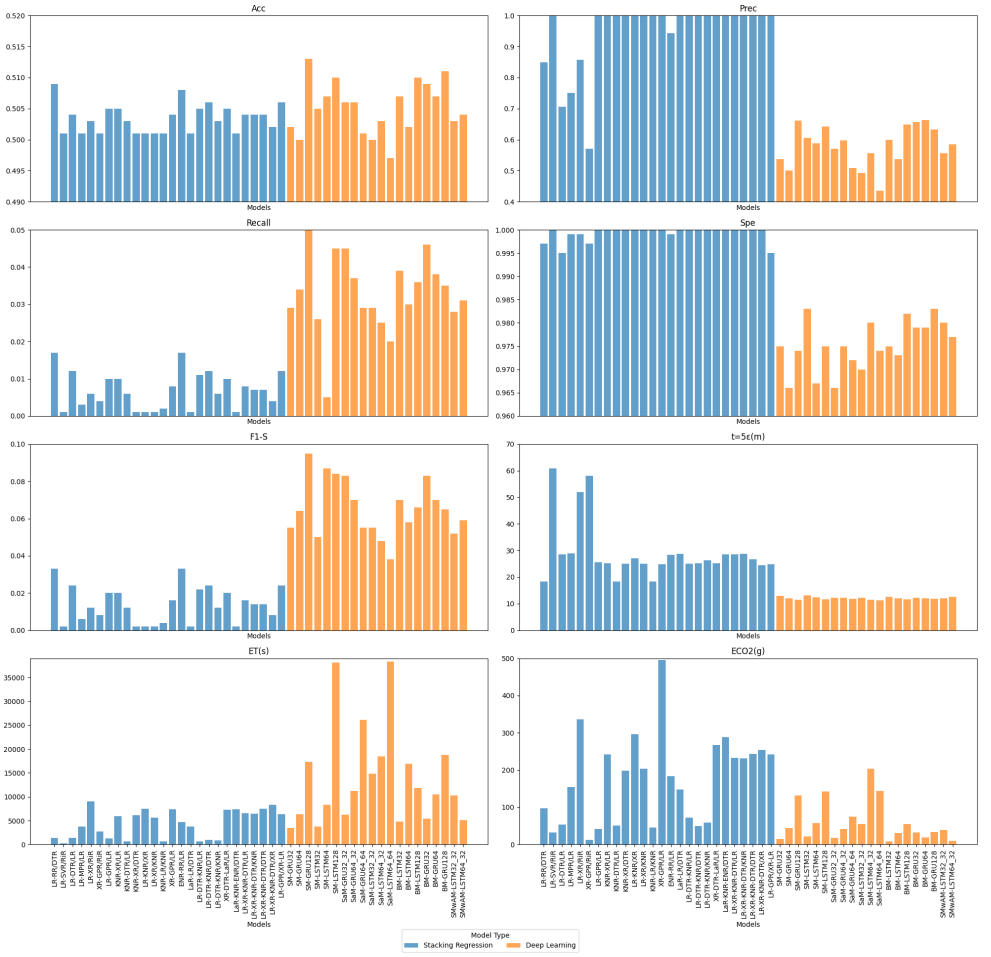


Figure 6.
Process on choosing the algorithms for comparison.

N	SR [ENR-RR/LR]			DL [SM-LSTM64]		
	ACT(s)	ECO (g)	CP (%)	ACT(s)	ECO (g)	CP (%)
100	0.243	0.0055	9.30	0.344	0.0038	13
250	*0.854*	*0.0145*	*9.39*	0.811	0.0089	21.6
300	1.017	0.0170	9.38	*0.930*	*0.0103*	*17*
350	1.200	0.0351	9.42	1.150	0.0127	16.6

Table 6.
Time and emissions analysis of the calculation of the probability of collision as a function of the number of samples.

time and emissions generated. The obtained results are presented in **Table 6** where ACT refers to the average computation time, ECO represents CO2 emissions, and CP denotes collision probability. We report CO2 emissions (ECO) measured with CodeCarbon as a sustainability/efficiency metric to complement prediction accuracy

and runtime. CO2 here quantifies the computational energy consumption associated with training/execution and is not an accuracy indicator. We use ECO to illustrate trade-offs between predictive performance and environmental cost (e.g., some high-accuracy DL models require substantially more compute and thus higher ECO), and to support discussion on model selection in resource-constrained or sustainability-sensitive deployments.

After comparing the N values from both Stacking Regression and Deep Learning approach, we can observe how while SR requires an N value of 250, Deep Learning uses 300 random samples to execute the Monte Carlo algorithm below 1 second. Finally, we statistically analyze the results. **Table 7** shows the average execution time (in seconds) and the statistical values of the collision probability calculated for the vehicles that collide and those that do not collide.

In order to determine at what probability a warning should be issued to vehicles indicating a risk of collision, it is needed to establish a decision threshold. This threshold will be used to determine whether an alert should be generated based on the calculated collision probability. Several considerations were taken into account when choosing the decision threshold:

- **An alert should be generated for all cases that are going to experience a collision:** When the collision probability reaches a certain level, it is crucial to issue an alert to vehicles involved in the potential collision. This ensures that appropriate actions can be taken to prevent the collision from occurring.

- **No alert should be generated for vehicles that are not going to collide in any way:** It is equally important to avoid generating unnecessary alerts for vehicle pairs that are not at risk of colliding. This prevents false alarms and minimizes distractions for drivers who do not face an actual collision threat.

- **An alert should be generated if two vehicles are going to pass very close to each other and could potentially collide for some reason:** Even if the probability of a collision is not high, there are situations where two vehicles may come very close to each other and pose a potential risk of collision. In such cases, it is prudent to issue an alert to inform the drivers about the proximity and potential danger.

Collision	2*AET (s)	Calculated collision probability						
		Mean	SD	Min	25%	50%	75%	Max
Stacking Regression								
Yes	0.5930	0.0177	0.0937	0.0000	0.0000	0.0000	0.0000	1.0000
No	0.59087	0.0030	0.0457	0.0000	0.0000	0.0000	0.0000	0.9760
Deep Learning								
Yes	1.213	0.0790	0.1168	0.0000	0.0167	0.0400	0.0967	0.9833
No	1.206	0.0294	0.0910	0.0000	0.0000	0.0000	0.0000	0.7200

Table 7.
Average running time and statistical values of the calculated collision probability for the real trajectories with stacking regression and deep learning.

Therefore, a threshold that maximizes the probabilities above the threshold and minimizes the probabilities below the threshold has been chosen. **Figure** 7 displays two boxplots belonging from the collision probability of the chosen model by both Stacking Regression (left image) and Deep Learning (right image) approach, respectively. The Y-axis represents the calculated collision probability, with values indicating the likelihood of a collision based on the model's predictions. The boxplot of the Stacking Regression shows that the calculated collision probabilities for the colliding vehicles are not very accurate, with an average probability of 1.772%. These results were expected since the used model has a very low precision in predicting trajectories, and the algorithm cannot perform reliable calculations. LSTM model (see right image from **Figure** 7) got an average probability of 1.997% with the alarms being generated for 15.2% of the colliding vehicles and for 8.7% of the non-colliding vehicles. This suggests that the LSTM model performed better in estimating collision probabilities compared to the model from SR, but it is also worth mentioning that in the stacking regressions, the model predicts better the non-collisions, and this is reflected in the fact that only 7 of the occasions of non-collision the alarms would be triggered, against the 87 triggered by LSTM. It is evident that LSTM models exhibit superior performance. They demonstrate a more accurate prediction, with an error rate of 12 meters, thereby indicating a stronger alignment with the problem under consideration. Nevertheless, it is important to note that Stacking Regression models exhibit higher specificity when it comes to vehicles that do not collide. Specificity refers to the ability of a model to correctly identify true negatives. In this regard, Stacking Regression models outperform LSTM models by achieving a higher level of accuracy in recognizing instances where collisions do not occur. As mentioned in [33], the SUMO environment does not simulate collisions by default. Hence, some expected collisions might not be real. As a consequence, the number of simulated collisions ends up being much lower than programmed.

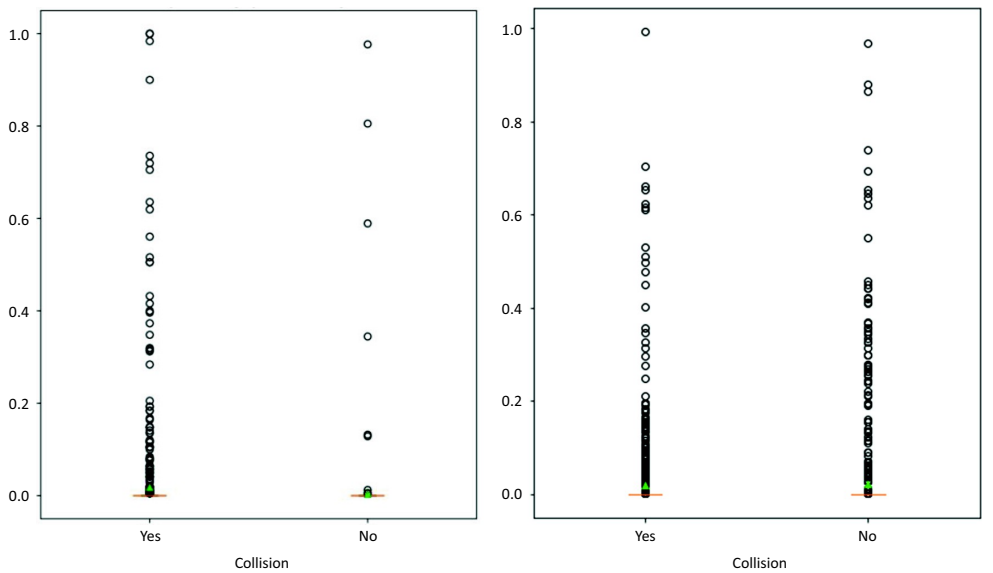


Figure 7.
Boxplot of the collision probability calculated on predicted trajectories – stacking regression (left) and deep learning (right).

As a conclusion, Deep Learning techniques outperformed Stacking Regression models in terms of position error with a difference of at least 6 meters, and as a consequence, the estimation of collision probability. Considering all metrics—prediction precision, execution time, and CO2 emissions—the Simple Model LSTM with 64 cells offers the best balance, achieving an error of 11.28 meters with reasonable execution time and CO2 emissions. This model performs consistently across different time intervals, making it ideal for real-time applications.

5. Conclusions and future work

This study explores advanced machine learning techniques for trajectory prediction and collision detection, building on previous research [2] and aligning with CCAM objectives of improving road safety and cooperative perception. Due to suboptimal results in initial trials, the focus shifted to Stacking Regression and widely used Deep Learning models. The objectives included gathering and cleaning data on crash-contributing factors, developing a methodology to predict crash probabilities, and training/validation on historical crash data—tasks relevant to several CCAM operational domains, particularly Urban Driving and Vulnerable Road User (VRU) protection.

Evaluation metrics (accuracy, precision, recall, F1-Score) were used to compare Stacking Regression with Deep Learning. Thirteen traditional ML models and twenty Deep Learning architectures were studied, with further improvement favoring Deep Learning models over the custom-designed ones. Despite a 12-meter error, Deep Learning outperformed Stacking Regression (average 18-meter error). A collision detection approach based on polygon intersection of predicted trajectories was implemented. However, due to large prediction errors, the evaluation results—such as only 17 detections out of 1000 collisions for the best model (ENR-RR/LR)—were insufficient for real-world deployment within CCAM environments.

To estimate collision probability, a Monte Carlo-based algorithm was applied, triggering alarms at risk thresholds of 0.8% for Stacking Regression and 1.6% for Deep Learning models. Results suggest that Stacking Regression models are suboptimal for trajectory prediction in CCAM contexts, encouraging further exploration of Deep Learning methods such as LSTMs. While the proposed system shows potential for enhancing VRU safety in cooperative scenarios, it also introduces ethical considerations, especially regarding continuous geospatial data collection and potential privacy infringements.

Future work will focus on increasing the precision of collision probability estimates by incorporating larger and more diverse datasets, representative of real-world CCAM environments. Moreover, advanced algorithms—such as reinforcement learning and transformers—will be explored to enhance the system's adaptability to dynamic and heterogeneous traffic conditions. Ensuring real-time applicability across CCAM domains remains a key challenge. To address privacy concerns, we also aim to integrate privacy-preserving mechanisms that safeguard individual rights while maintaining system effectiveness.

Acknowledgment

We would like to thanks to Jokin Cuestas Arrillaga for running the experiments about Stacking Regression. This work was supported by 6GOASIS project which has been funded by the "Ministerio de Asuntos Económicos y Transformación Digital" and the European Union-NextGenerationEU in the frameworks of the "Plan de Recuperación, Transformación y Resiliencia" and of the "Mecanismo de Recuperación y Resiliencia" under references TSI-0,63000-2021-18/24/77.

Author details

Raúl Parada[1*] and Rafael Corvillo[2]

1 Centre Tecnològic de Telecomunicacions de Catalunya (CTTC/CERCA), Castelldefels, Barcelona, Spain

2 Universitat Oberta de Catalunya (UOC), Barcelona, Spain

*Address all correspondence to: raul.parada@cttc.es

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] W. H. Organization. Road Traffic Injuries. 2022. Available from: https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries [Accessed: 2024-June]

[2] Parada R, Corvillo R, Dini P. A dl-based estimation probability approach for vru collision avoidance. 2023 IEEE Conference on Artificial Intelligence (CAI). 2023;23–25. DOI: 10.1109/CAI54212.2023.00018

[3] Parada R, Aguilar A, Alonso-Zarate J, Vázquez-Gallego F. Machine Learning-based Trajectory Prediction for VRU Collision Avoidance in V2X Environments. In: 2021 IEEE Global Communications Conference (GLOBECOM). 2021, p. 1–6

[4] Breiman L. Stacked regressions. Machine Learning. 1996;**24**(1):49–64. DOI: 10.1007/BF00117832

[5] Sharma SU, Shah DJ. A practical animal detection and collision avoidance system using computer vision technique. IEEE Access. 2017;**5**:347–358

[6] Lefèvre S, Vasquez D, Laugier C. A survey on motion prediction and risk assessment for intelligent vehicles. ROBOMECH Journal. 2014; **1**: 347–358

[7] Ammoun S, Nashashibi F. Real time trajectory prediction for collision risk estimation between vehicles. 2009 IEEE 5th International Conference on Intelligent Computer Communication and Processing. 2009;417–422. DOI: 10.1109/ICCP.2009.5284727

[8] Kaempchen N, Weiss K, Schaefer M, Dietmayer K. IMM object tracking for high dynamic driving maneuvers. IEEE Intelligent Vehicles Symposium. 2004;**2004**:825–830

[9] Eidehall A, Petersson L. Statistical threat assessment for general road scenes using monte carlo sampling. IEEE Transactions on Intelligent Transportation Systems. 2008;**9**(1): 137–147

[10] Tran Q, Firl J. Online maneuver recognition and multimodal trajectory prediction for intersection assistance using non-parametric regression. 2014 IEEE Intelligent Vehicles Symposium Proceedings. 2014;918–923. DOI: 10.1109/IVS.2014.6856480

[11] Laugier C, Paromtchik IE, Perrollaz M, Yong M, Yoder J-D, Tay C, Mekhnacha K, Nègre A. Probabilistic analysis of dynamic scenes and collision risks assessment to improve driving safety. IEEE Intelligent Transportation Systems Magazine. 2011;**3**(4):4–19

[12] Wiest J, Höffken M, Kreßel U, Dietmayer K. Probabilistic trajectory prediction with Gaussian mixture models," In: 2012 IEEE Intelligent Vehicles Symposium. 2012, p. 141–146

[13] Grigorescu S, Trasnea B, Cocias T, Macesanu G. A survey of deep learning techniques for autonomous driving. Journal of Field Robotics. 2020;**37**(3):362–386. DOI: 10.1002/rob.21918

[14] Zhao B, Zhang X, Chen H, Zhu W. A novel prediction algorithm of pedestrian activity region for intelligent vehicle collision avoidance system. IEEE Transactions on Intelligent Vehicles. 2023;**8**(3):2173–2183. DOI: 10.1109/TIV.2022.3215199

[15] Lyu N, Wen J, Duan Z, Wu C. Vehicle trajectory prediction and cut-in collision warning model in a connected vehicle environment. IEEE Transactions on Intelligent Transportation Systems. 2022;**23**(2):966–981

[16] Meng Q, Guo H, Li J, Dai Q, Liu J. Vehicle trajectory prediction method driven by raw sensing data for intelligent vehicles. IEEE Transactions on Intelligent Vehicles. 2023;**8**: 3799–3812

[17] Hou L, Xin L, Li SE, Cheng B, Wang W. Interactive trajectory prediction of surrounding road users for autonomous driving using structural-lstm network. IEEE Transactions on Intelligent Transportation Systems. 2020;**21** (11):4615–4625

[18] Wang P, Yu H, Liu C, Wang Y, Ye R. Real-time trajectory prediction method for intelligent connected vehicles in urban intersection scenarios. Sensors. 2023;**23**(6). Available from: https://www .mdpi.com/1424-8220/23/6/2950

[19] Gao Y, Fu J, Feng W, Xu T, Yang K. Surrounding vehicle trajectory prediction under mixed traffic flow based on graph attention network. Physica A: Statistical Mechanics and Its Applications. 2024;**639**:129643. Available from: https://www .sciencedirect.com/science/article/pii/ S0378437124001511

[20] Guo Y, Liu Y, Wang B, Huang P, Xu H, Bai Z. Trajectory planning framework for autonomous vehicles based on collision injury prediction for vulnerable road users. Accident Analysis & Prevention. 2024;**203**:107610. Available from: https://www.sciencedirect.com/sci ence/article/pii/S0001457524001556

[21] Zhu D, Khan Q, Cremers D. Multi-vehicle trajectory prediction and control at intersections using state and intention information. Neurocomputing. 2024;**574**:127220. Available from: http s://www.sciencedirect.com/science/arti cle/pii/S0925231223013437

[22] Li A, Sun L, Zhan W, Tomizuka M, Chen M. Prediction-based reachability for collision avoidance in autonomous driving. In: 2021 IEEE International Conference on Robotics and Automation (ICRA), IEEE; 2021, p. 7908–7914

[23] Yu H, Huo S, Zhu M, Gong Y, Xiang Y. Machine learning-based vehicle intention trajectory recognition and prediction for autonomous driving. In: 2024 7th International Conference on Advanced Algorithms and Control Engineering (ICAACE). IEEE; 2024. p. 771–775

[24] Duan Y, Jia J, Jin Y, Zhang H, Huang J. Expressway vehicle trajectory prediction based on fusion data of trajectories and maps from vehicle perspective. Applied Sciences. 2024;**14** (10). Available from: https://www .mdpi.com/2076-3417/14/10/4181

[25] Gao Z, Bao M, Cui T, Shi F, Chen X, Wen W, Gao F, Zhao R. Collision risk assessment for intelligent vehicles considering multi-dimensional uncertainties. IEEE Access. 2024;**12**:57780–57795

[26] Cai J, Zhu H, Feng H, Wen L, Wang W, Lv M, Fang K. Vehicle trajectory prediction based on dynamic graph neural network. In: 2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD). 2024. p. 67–72

[27] Tang L, Yan F, Zou B, Li W, Lv C, Wang K. Trajectory prediction for autonomous driving based on multiscale spatial-temporal graph. IET Intelligent Transport Systems. 2023;**17**(2):386–399. DOI: 10.1049/itr2.12265

[28] Li G, Zhang X, Guo H, et al. Real-time optimal trajectory planning for autonomous driving with collision avoidance using convex optimization. Automotive Innovation. 2023;**6**(4):481–491. DOI: 10.1007/s42154-023-00222-7

[29] Alsanwy S, Chalak Qazani MR, Al-Ashwal W, Shajari A, Nahvandi S, Asadi H. Vehicle trajectory prediction using deep learning for advanced driver assistance systems and autonomous vehicles. In: 2024 IEEE International Systems Conference (Syscon). 2024. p. 1–8

[30] G. A. C. (DLR). SUMO - Wiki - TraCI Protocol [Online]. Available from: https://sumo.dlr.de/docs/TraCI/Protocol.html

[31] Schmidt V, Goyal K, Joshi A, Feld B, Conell L, Laskaris N, Blank D, Wilson J, Friedler S, Luccioni S. CodeCarbon: Estimate and Track Carbon Emissions from Machine Learning Computing. 2021

[32] Lambert A, Gruyer D, Saint Pierre G. A fast Monte Carlo algorithm for collision probability estimation. In: 2008 10th International Conference on Control, Automation, Robotics and Vision. 2008. p. 406–411

[33] Ribeiro B, Nicolau MJ, Santos A. Using machine learning on V2X communications data for VRU collision prediction. Sensors. 2023;**23**(3). https://www.mdpi.com/1424-8220/23/3/1260

Section 4

Applications and Operational Insights

Chapter 14

Enhanced Strategies for Wide-Area Traffic Control

Franco Filippi, Roberta Di Pace, Facundo Storani and Stefano de Luca

Abstract

This chapter presents a comprehensive state-of-the-art review of wide-area traffic control strategies aimed at mitigating congestion and improving urban traffic flow. Network-wide control, implemented via ramp metering, intersection gating, and wide-area gating, regulates vehicle entry into specific network regions to maintain optimal conditions. The chapter explores theoretical foundations, adaptive control mechanisms, and the integration of macroscopic fundamental diagram (MFD)-based models for real-time traffic management. Emerging approaches for coordinating traffic with dynamic demand are discussed. Benefits such as congestion reduction, enhanced safety, and environmental improvements are highlighted, alongside challenges in implementation, such as public acceptance and infrastructure constraints. This work contributes a holistic understanding of current methodologies and identifies future directions for smart urban mobility solutions.

Keywords: wide-area control, macroscopic fundamental diagram (MFD), gating control, urban traffic management, perimeter control

1. Introduction

Traffic congestion is a prevalent issue both in urban and extra-urban areas, leading to significant economic, environmental, and social impacts. Researchers have proposed various strategies to address this challenge, with a particular focus on traffic control techniques. This literature review explores the theoretical foundations, case studies and experimentations, and emerging trends in wide-area traffic control strategies.

Wide-area traffic control refers to the implementation of mechanisms that regulate the flow of vehicles entering a specific region or network, such as a congested urban zone or a critical roadway segment, with the aim of optimizing overall network performance. By controlling the rate at which traffic is allowed to enter, perimeter control helps prevent congestion, improve traffic flow, and enhance overall network efficiency. This approach differs from the traditional fixed-cycle traffic signal control, which can often lead to inefficient resource utilisation and suboptimal traffic flow.

In order to achieve the main goal, i.e. traffic management, a general case of network-wide strategies is composed of: (1) Sensors and data collection, where traffic sensors (inductive loops, cameras, or radar) collect real-time data on traffic volume, speed, and density; (2) Control algorithms, which calculate optimal traffic entry and release rates using the previously collected information; (3) Traffic signals or barriers, which are physical controls used to manage vehicle flows; (4) Dynamic adjustments, defining a perimeter technique as an adaptive strategy that responds dynamically to traffic conditions, optimizing the flow rates with real-time updates. This last item highlights the main difference from fixed signal control strategies and the reason for the use of different types of boundary flow control strategies, such as ramp metering (which controls the flow of vehicles from the ramp onto highways to prevent bottlenecks), intersection gating (which restricts vehicle entry into congested urban zones), and area-wide gating (which limits access to entire districts or regions to manage traffic load) for better traffic management.

The expected benefits of implementing wide-area control strategies are: congestion reduction, in which gating prevents the breakdown of flow and minimises delays by keeping traffic volumes below critical levels; improving safety by reducing the likelihood of accidents caused by fewer traffic jams and smoother flows; improving environmental impacts due to the reduction in stop-and -go phenomena, which generally lead to higher fuel consumption and emissions; and network performance optimisation, where travel times and reliability are expected to improve due to the efficient use of roadway capacity.

Although the above-mentioned strategy might present interesting advantages, there are minor challenges and considerations to take into account, such as public acceptance, infrastructure requirements, and social equity, which could be evident in access restrictions affecting certain user groups. Regarding public acceptance, it may lead to resistance from drivers to the idea of having signal control or gated areas, which might produce some delays at the entries. Additionally, given the enormous technological assessment that most cities possess, this management technique depends on advanced traffic management systems, sensors, and control devices.

2. Literature review

Even if numerous approaches have been developed for traffic signal control, implementing sophisticated and effective traffic control techniques in diverse large-scale networks remains a significant issue. This is especially true when it comes to dealing with traffic congestion and propagation phenomena. Popular techniques like SCATS and SCOOT are less effective in oversaturated traffic situations with prolonged delays and spillbacks, despite being suitable for large-scale networks [1, 2]. Moreover, in saturated conditions, intersections are already operating at or near capacity. Thus, this means there is minimal opportunity for the aforementioned strategies to adjust signal timings (splits, offsets, cycle lengths) to improve traffic flow. To address local spill-over issues, ad hoc perimeter schemes and engineering solutions have lately been added to these systems. For instance, see [3]. This paper presents a report that summarises experts' observations regarding balancing traffic density or distributing traffic in an even manner. In addition, it investigates whether

such techniques can be implemented systematically with the use of ATCS, also known as area traffic control systems.

Optimised policies for adaptive control (OPAC) is a distributed control approach that uses a dynamic optimisation method to determine the best timing for signals in order to minimise a performance function of stops and total intersection latency. Phase lengths, which are limited only by minimum and maximum green times, may be determined by the algorithm using both measured and modelled demand. Not only does this work introduce the virtual-fixed cycle OPAC (VFC-OPAC) within the real-time traffic adaptive control system (RT-TRACS) project and its preceding versions (OPAC-1 dynamic programming, OPAC-2 sequential optimisation, and OPAC-3 rolling horizon approach), but it also conducted a study at the Reston Parkway, Virginia (USA) RT-TRACS demonstration site. According to the initial results, OPAC has succeeded in lowering pauses and delays while facilitating vascular advancement [4]. If there had been enough time to calibrate and fine-tune the OPAC parameters, the performance could have been even better.

The newly created feedback control system of traffic urban control (TUC) was a workable solution to oversaturated traffic conditions. In [5], a generic mathematical model based on the store-and-forward modelling scheme is investigated, developing three modelling variations for alternative optimal signal control strategies. These have the aim of minimise and moderating link queues and reducing the queue spillback risks under saturated traffic states. Then, signal control plans might be addressed with a linear multivariable feedback regulator, an open-loop constrained quadratic optimal control (QPC), or an open-loop constrained nonlinear optimal control (NOC). Both approaches can be suitable for on – and off-line network optimisation given that the utilised traffic flow models and related constraints incorporate all required network characteristics. As a result, NOC and QPC demonstrated sufficient efficiency at managing the network in comparison to LQ, even though they require greater computational effort and complexity.

By means of microscopic simulations research for the transportation network of Chania, Greece, a hybrid approach was developed in which its strategy changes depending on the actual traffic conditions of the network (i.e., under – or over-saturated state) [6]. It works by controlling the signalised junctions using the real-time Webster-type demand-driven strategy, provided that the intersections are in undersaturated conditions; if this state is almost reached, TUC (a multivariable regulator derived from a linear-quadratic control problem) is set up. Three different demand scenarios were carried out, considering three signal methodologies that are compared to fixed-time control (FT): LQ (TUC), demand-based (DB) approach, and hybrid approach. It has been shown via simulation investigations and field results that the integration of DB and TUC's LQ control can address both under – and oversaturated traffic conditions without requiring a prespecified fixed signal plan. In [7] and [8], studies were conducted regarding traffic-responsive coordinated signalised control via a simulation-based approach in Scotland (Glasgow) and Israel (Jerusalem and Tel Aviv), respectively. Both case studies present benefits, such as a reduction in mean travel time and an increase in travelled distance. Moreover, in the first case, as TUC was integrated with ramp metering strategies (such as ALINEA), safety measures were enhanced in on-ramp areas.

In other words, TUC aims to balance and reduce the relative occupancies of the connections in order to reduce the risk of oversaturation and spillback of link queues.

Additionally, it might work as a local gating mechanism that limits link access when it is about to overload, protecting downstream links from oversaturation. However, for diverse networks with several congestion centres and highly directed demand flows, these strategies may be less-than-ideal or delayed in their reactivity.

Another option for real-time network-wide traffic signal control for urban networks is a hierarchical two-level approach, where more detailed control can be applied to smooth traffic movements within these regions (for example, the above-mentioned technique TUC, also known as UTC) at the second level, while at the first level, perimeter and boundary flow control between various network regions advances the aggregated performance (for instance, the macroscopic or network fundamental diagram – MFD or NFD). In [9], while perimeter control is applied for regulating inter-flows among protected networks (PN), at a lower level, the max pressure (MP) approach addresses the heterogeneity limitation within PN. By doing so, results have shown that the integration of both control strategies outperforms the use of them separately. Another study regarding the use of two-layer control can be found in reference [10], in which similar results were observed. Moreover, the scheme of mutually exclusive yet interactive layers allows the congestion level of the intersections to be identified. In this way, relevant and crucial joints can be defined in order to reduce the number of constraints to take into consideration.

In contrast to the two aforementioned works, hierarchical control has been investigated using MPC and feedback-based approaches at the lower level, demonstrating reductions in delay times and improvements in vehicle flows among the regions [11, 12]. Section 2.3 provides a more profound revision of these works.

The benefits of hierarchical control structures over many other disjointed regulator schemes are illustrated by various simulation studies. According to preliminary findings, incorporating a network-level strategy into a local adaptive framework can greatly enhance system performance in situations where spillback phenomena arise, which is a typical occurrence in city centres with short links. Traffic congestion can be continuously improved by an effective multi-layer control architecture, which reduces delays and increases system output. Large cities can offer higher-quality services to infrastructure users, and this has favourable effects on the economy and the environment.

2.1 MFD as a control framework

Management of aggregated traffic networks can also be achieved by using the above-mentioned concept of the macroscopic fundamental diagram (MFD). As illustrated in **Figure 1(a)**, the MFD provides, for network regions under specific regularity conditions (primarily homogeneity in the spatial distribution of congestion and the network topology), a unimodal, low-scatter relationship between network vehicle accumulation n (veh) and network outflow O(n) (veh/h). See Appendix A for a concise derivation of these relations.

After the proposal of the MFD concept, its presence with dynamic aspects has recently been empirically verified [13]. This investigation focused on the existence of MFDs for urban-scale networks using empirical data from Yokohama, Japan. It combined fixed traffic detectors with GPS-equipped taxis to estimate network-wide traffic flow, density, and speed. It was shown that while individual link speed–density relations were highly scattered, aggregated network data formed a smooth,

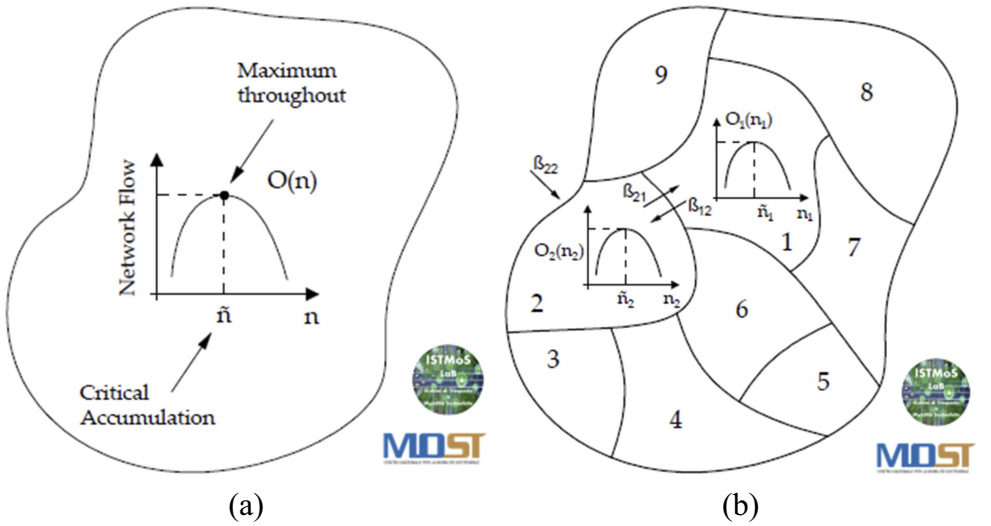


Figure 1.
A network modelled as (a) Single-reservoir system and (b) Multi-reservoir system.

consistent MFD curve, unaffected by variations in travel demand. Alternatively, MFD can be written as space-mean flow vs. accumulation because of the linear relationship between network outflow and circulating (or space-mean) flow (caused by time-invariant regional trip duration).

On the other hand, when link density heterogeneity is present, a well-defined MFD can be obtained by partitioning the heterogeneous network into smaller, homogeneous zones with low variability in link densities, as illustrated in **Figure 1(b)**. In [14], a three-step algorithm is used as a partitioning method for the urban transport network of downtown San Francisco. The steps are: normalised cut for initial segmentation, merging for cluster refinement, and boundary adjustment to reduce density variance while maintaining spatial compactness. It was observed that the proposed approach produced more compact and homogeneous regions than k-means clustering, resulting in low-scatter MFDs and improved traffic monitoring and control under heterogeneous congestion.

In order to enhance traffic conditions in an urban network that has been divided into two zones with clearly defined MFDs, an elegant perimeter control strategy was proposed in [15]. It developed an optimal perimeter control strategy for two-region urban traffic networks using MFDs and model predictive control (MPC). Each region is represented by an MFD, relating vehicle accumulation to trip completion flow, and perimeter controllers regulate transfer flows between the two regions to maximise total trip completions. For the combined urban and motorway network, these findings support the use of the MFD and the perimeter control strategy in reducing total delay, preventing gridlock, and enhancing total travel time in comparison to the greedy approach.

To increase mobility in homogeneous networks under saturated traffic conditions, a feedback-based gating strategy that takes advantage of MFD properties was applied to prevent oversaturation in urban networks [16]. The methodology identified an optimal accumulation level for a protected subnetwork and regulated

upstream inflow via gating at selected intersections. A simple proportional–integral (PI) feedback controller was designed using real-time measurements without requiring traffic prediction models. The case study of a district of Chania, Greece, has shown several improvements, such as reduced average delay and increased network speed.

2.1.1 MFD shape factors

While the MFD is a powerful tool for modelling network-level traffic dynamics, its reliability depends on specific assumptions regarding network homogeneity and demand stability. The study in [17] explored how numerous factors influence MFD shape through microscopic simulation of the Amsterdam ring road network. The findings show that road type, ramp metering, congestion dynamics, and demand variability significantly affect MFD form:

- Road type: Freeway sections exhibit more scatter in MFDs compared to urban networks due to more severe and variable congestion patterns.
- Ramp metering: Improves MFD performance by controlling inflow, reducing accumulation, and maintaining higher flow rates.
- Congestion onset and resolution: Introduces hysteresis and loop patterns, increasing MFD scatter and reducing interpretability.
- Traffic demand: Rapid changes in demand, particularly sharp drops, can cause the MFD to deviate from expected patterns, reflecting inefficient network usage despite available capacity.

At the same time, those key insights strengthen the regularity conditions for well-defined MFDs that have already been detailed above, which assume slow-varying demand, spatially even congestion, and redundant, homogeneous network structures [13].

2.1.2 MFD estimation methods

A variety of methods for estimating MFDs have been investigated in the literature. Reference [18] proposes a data fusion algorithm designed to improve MFD estimation for urban networks by combining loop detector data (LDD) with floating car data (FCD). In this approach, the network is divided into two parts (one monitored by loop detectors and one not), and flow and density estimates are then fused using a weighted method that accounts for probe vehicle penetration rates. The algorithm is evaluated through microscopic traffic simulations of both an abstract grid network and the city of Zurich under various levels of sensor coverage and probe penetration. The study shows that the fusion approach consistently reduces estimation errors compared to using either LDD or FCD alone, achieving accuracy close to an optimised reference method while requiring significantly lower computational cost.

Using microscopic simulations with an equilibrium traffic flow model (LWR), the study in [19] examined how detector position, distribution, and signal proximity

influence MFD accuracy. Furthermore, it compares three methods for estimating MFDs: (a) an analytical approach based on theoretical network properties, (b) a trajectory-based "production" method using vehicle path data, and (c) a loop detector-based method using aggregated flow, speed, and occupancy measurements. Overall, the results show that proper detector placement and adequate coverage are essential to avoid bias in MFD estimation.

Thus, it can be said that LDD and FCD are the two main data sources used to estimate empirical MFDs. In the first case, LDD is obtained through static sensors, which evaluate the traffic conditions at pre-defined locations; whereas, in the second case, vehicles driving in the network compose the FCD, and both can be collected through real-time measurements.

Furthermore, a recent study has also proposed two methods for estimating MFDs [20]. The first method relied on automated vehicle location (AVL) data from public transit vehicles, whereas the second combined AVL with FCD, even when the FCD was incomplete, to improve estimation accuracy without requiring knowledge of probe penetration rates. Both methods were tested on simulation grids and through field experiments on Zurich's real network. The results showed that AVL data can approximate car speeds with high accuracy, while the fusion approach further reduces estimation errors.

Efficient MFD estimation techniques are necessary and can be divided into analytical and experimental categories, as explored in reference [19]. According to [21], analytical techniques rely on a triangular local fundamental diagram (FD) together with the kinematic wave (KW) model, which provides an accurate local representation of traffic dynamics [22]. The resulting MFD can subsequently be derived using variational theory, which depends on the control parameters (mostly signal timings) and network architecture [23]. These approaches are particularly attractive because they offer a direct evaluation of the MFD for a given network without requiring measurements or simulations.

The current state of analytical approaches is restricted to homogeneous settings, meaning that all connections have the same or almost identical mean flow values. An example of this would be an urban corridor with evenly distributed inflows and outflows at crossings. The MFD derived from analytical methods is only an upper bound and may be significantly higher than the effective MFD when the required conditions are not fulfilled. Nevertheless, regularity conditions (in topology and signal settings) are no longer required to produce a precise estimation of the MFD, according to recent improvements [24]. This work investigates how route choice affects MFD estimation and network efficiency by implementing user equilibrium and system optimum conditions without requiring a regular network. Outcomes showed that user equilibria produce smoother but less efficient flow distributions, while system optimum maximises capacity but causes discontinuities and inequity.

On the other hand, observations are the foundation of experimental methodology. The most popular approach averages occupancy and flow from loop detectors in the region under study, e.g., see [13]. Although this approach is frequently used to extract MFD from measurements, its conformance to the notion of MFDs has received little consideration. In fact, MFD is intended to link spatially averaged traffic behaviour measurements. The impact of traffic lights in metropolitan networks is substantial. Then, it becomes clear that the complete picture of traffic dynamics within a connection cannot be captured by punctual Eulerian observations obtained from loop detectors. As mentioned above, depending

on the loop detector distribution across the networks, this approach may produce a sizable bias in the MFD. When traffic conditions inside the network are not uniform, scattered plots can also be seen, and they might contrast with the idea of a well-defined MFD, as investigated in reference [25].

In [26], a real-time estimation of aggregated traffic states (e.g., vehicle accumulations, demands, and model parameters) in multi-region urban networks using the Extended Kalman Filter (EKF) is investigated. The methodology integrates a stochastic traffic dynamics model with sparse sensor data (e.g., loop detectors, GPS) to estimate unobserved states in a partitioned urban network. Through simulations on a Barcelona case study, the EKF demonstrates robust performance in tracking traffic states and parameters under noise, even with limited measurements. In addition, results validate the estimator's ability to fuse model predictions and real-time data, enabling accurate state estimation for closed-loop traffic control systems like perimeter control. Furthermore, the approach is scalable to networks with arbitrary topology and measurement configurations.

Recently, the existence of MFDs has stimulated extensive research activity, primarily from a theoretical perspective. In practice, however, no MFD-based control schemes have yet been implemented in real cities. One of the main obstacles is that most cities cannot obtain the large amount of data required to construct an MFD due to limited monitoring resources. To address this, in reference [27], a method for comparing two aggregate flow–density relationships in terms of accuracy was proposed: an incomplete MFD (pMFD), derived from data on only p links, and a complete MFD constructed using data from all links in the network. The validity of a pMFD as a control mechanism is the main emphasis of this simple density ratio-based methodology, which assesses whether the imperfect MFD can adequately explain the growth of congestion. Researchers developed a quasi-optimal search algorithm using that methodology to determine the optimal choice of p links. In fact, one of the main highlights observed in this article is that a minimum network coverage of 25% is necessary to maintain an average error in density ratios below 15 percentage points, which is crucial for reliable traffic management. Numerous cities, apart from Zurich, Switzerland, such as Yokohama (Japan) and San Francisco (the United States), have demonstrated the existence of empirical MFDs [13, 28], respectively. Not only is the lack of data a major challenge for MFD estimation, but the definition of homogeneous and representative regions also poses significant difficulties. In [29], calibration and validation of an MFD simulation for the city of Lyon (France), partitioned into multiple reservoirs, is investigated. The validation process in the mentioned study used two main datasets for comparison: GPS taxi company trajectories (around 5,000 trips per day) and loop detectors operated by the Lyon authorities (330 loop detectors recording for several months). It was observed that the model accurately predicts regional traffic accumulation and mean speeds, demonstrating its potential for large-scale traffic monitoring and control applications.

2.2 Adapting control strategies

In Reference [16], the application of feedback-based gating control to urban road networks using the macroscopic or network fundamental diagram (MFD or NFD) for real-time traffic management has been introduced. The proposed strategy seeks to maintain traffic flow within optimal ranges to maximise throughput and reduce

delays in urban networks. Furthermore, recent work has explored integrating perimeter control with adaptive traffic signal strategies to improve the management of urban traffic networks [30]. Traditional urban traffic control relies heavily on traffic signals to minimise delays, yet these systems encounter difficulties under saturated conditions. Consequently, combining wide-area control with adaptive traffic signal strategies has been shown to improve network performance by reducing both delays and queue lengths at network boundaries. This integration helps maintain optimal vehicle accumulation within the protected network, ensuring higher throughput and shorter queues at entry points, especially during peak traffic periods.

In addition, the feedback approach was expanded to accommodate a large number of networks with separate individual NFDs [31]. According to research, this partitioning method might be helpful in situations involving large, congested networks with significant heterogeneity. The availability of real-time measurements from every network link was assumed by both feedback techniques. In [32], conducted research emphasises that effective traffic management through efficient feedback gating control can be achieved with limited real-time measurements, thereby reducing implementation costs while still maintaining traffic flow efficiency. A proportional–integral (PI) feedback regulator was used to maintain vehicle accumulation in a protected urban network region at levels maximizing throughput. It was tested on the network of Chania, Greece, via AIMSUN under different scenarios of measurement coverage (100%, 35%, 10%, and 5% of links). They found that reduced NFDs maintain critical traffic state detection equivalent to full measurements, enabling effective gating with far lower sensor requirements.

In [33], a performance assessment methodology grounded in the MFD is proposed. It introduces four core indicators (maximum throughput, critical accumulation, gridlock accumulation, and degree of homogeneity) to quantify traffic network efficiency under various signal control strategies. Unlike traditional segment-level metrics (e.g., travel time or delay), this MFD-based approach allows for a network-wide characterisation of control effectiveness, capturing both capacity and resilience under congestion. By means of a real-world case study in the Qingyang District in Chengdu, China, researchers compare fixed-time, actuated, adaptive, and adaptive coordinated control schemes. The study validates the MFD utility not only as a control reference but also as a robust, comprehensive tool for evaluating the systemic impact of signal control schemes, thus highlighting the potential of MFD-guided perimeter or network-wide controls in large-scale urban settings.

2.3 Model predictive control

Model predictive control (MPC) uses a moving horizon approach to optimise system control in real time, allowing decisions to be continuously adjusted to changing conditions and based on the latest information. This is especially useful in dynamic applications, such as traffic management. For example, a variety of traffic control concerns, such as ramp metering of freeway networks [34, 35], variable speed limits and route guidance for freeway networks [36], and signal control for large-scale urban networks [37], have all been optimised using a receding horizon framework.

As explained in Section 2.1, the MPC approach aims to maximise the number of trips reaching their destinations while managing congestion effectively [15]. Thus, it is observed that MPC is a viable and effective method for managing urban traffic, particularly in scenarios involving multiple regions and varying demand patterns. The findings support the use of MPC in real-time traffic management systems to enhance overall traffic flow and reduce congestion.

In the context of MFD-based models, MPC has recently gained attraction as a powerful tool for aggregated, network-level traffic control. This integration of model predictive control methods for traffic signal control, as is well explained in reference [38], allows for predictive perimeter control strategies, ensuring that vehicle entry into congested areas is regulated based on real-time system states.

Studies have demonstrated that using MPC with MFD enables more efficient, coordinated control in large-scale urban networks by balancing demand across network boundaries and maintaining optimal operating conditions with relatively low computational complexity. For instance, see [11, 12], where the authors propose similar ideas addressing the control problem by means of hierarchical traffic control strategies. In [12], the focus is on managing congestion heterogeneity using a two-level framework with a high-level MPC for network perimeter flow optimization and a low-level feedback homogeneity controller (FHC) to balance congestion among subregions. Its case study, based on a two-region network (periphery and city centre), demonstrates a 47.1% delay reduction and reduced MFD hysteresis. On the other hand, the study targets scalability and computational efficiency in large-scale networks, using MPC at both levels: an upper-level MFD-based controller for traffic demand balancing and a lower-level distributed multiagent MPC for signal coordination [11]. Tested on a three-subnetwork network, it achieved performance close to centralised MPC but with significantly lower computational times. In summary, the first emphasises heterogeneity mitigation and traffic flow stability, while the second focuses on efficient, scalable computation for network-wide optimisation.

2.4 Reinforcement learning

In the reinforcement learning (RL) context, an agent uses policy learning to maximise a long-term, goal-oriented reward. The RL agent engages with the environment at each stage, assessing the effectiveness of its actions by using input from the surroundings. Then, the agent attempts to enhance the performance of succeeding actions. In order to include uncertainties and changes in dynamics into the optimal control framework, the mentioned methodology assists optimal control in getting around the need for full knowledge of the system dynamics. In contrast to the traditional optimal control framework's online nature, RL can use data-driven mechanisms to discover the best solution online in real-time while still achieving robustness and adaptability.

Wide-area control may be a large and complex problem to which different algorithms, such as SARSA or Q-Learning, cannot scale. RL and deep learning have been integrated in great detail to address this problem. Signalised intersection control is one of the many traffic control applications of deep reinforcement learning that the transportation community has used. An early attempt to incorporate RL into perimeter control is presented in [39]. However, in this study, the RL approach was used merely to distribute metering rates along the cordon perimeters that were

generated by an MPC-based control architecture. A later study introduced a model-based RL method to replace the direct sequential approach used in [15], integrating the RL component into the MPC framework to address the open-loop optimisation problem [40]. Moreover, a model-free deep reinforcement learning method for perimeter control in two-region urban networks was introduced, eliminating the need for explicit MFD models [41]. Two agents are evaluated: one using discrete actions and one using continuous actions. Simulation results under varying demand and model uncertainty show that the continuous agent learns faster and performs as well as, or better than, MPC, while generalizing effectively to atypical demand patterns and limited traffic data.

In Reference [42], an integral reinforcement learning (IRL) approach is modified for continuous-time systems, although it assists the discrete nature of sensor data by allowing reinforcement intervals to vary with data resolution. Unlike traditional RL methods, this method enhances adaptability to real-world conditions.
A significant innovation is the use of the experience replay (ER) technique, which leverages historical data to improve learning efficiency and convergence speed. The methodology is built upon the MFD framework, which captures aggregated traffic behaviours in urban networks. Hence, the study introduces a data-driven policy iteration method that uses the IRL Bellman equation to compute optimal control without requiring a predefined system model. Some interesting contributions are a heterogeneous data application for varied real-time sensor data, a balanced computational complexity with performance, and the stability and convergence of the controlled traffic dynamics.

Reference [43] introduced two RL-based models, MFD-QL (using Q-learning) and MFD-DDPG (using deep deterministic policy gradient), which incorporate the MFD to regulate regional traffic without relying on detailed traffic forecasts. Simulations on a real Beijing network using SUMO showed that both models effectively avoided oversaturation and improved network performance. Between them, MFD–DDPG demonstrated better convergence and control accuracy, significantly reducing travel time, delay, and vehicle queues. These results highlight the potential of RL-based perimeter control for real-time, large-scale traffic optimisation.

3. Conclusions

This chapter has reviewed the evolution and current approaches to wide-area control strategies, with a focus on the usage of MFDs. From traditional perimeter control to data-driven adaptive methods, the literature highlights an increasing trend toward integrating network-level traffic modelling, real-time control, and optimisation techniques such as MPC and Reinforcement Learning. A key insight is the role of MFD as a foundation for regulating flow and managing congestion at different levels, providing a scalable and interpretable framework for gating decisions. However, recent studies show that MFD behaviour is sensitive to factors like network heterogeneity, ramp metering, dynamic demand, and congestion patterns, challenging the assumption of stable and universal MFD curves.

An important emerging perspective is the need to move beyond model-based gating and embrace learning-based control, which adapts to real-time, high-dimensional traffic environments. A variety of approaches, which were treated in

the present document, show promise in enhancing traffic flow under uncertainty, yet remain difficult to deploy due to their data requirements and lack of interpretability. In parallel, strategies such as network partitioning, loop detection integration, and multi-reservoir control continue to evolve to handle spatial heterogeneity more effectively.

Despite these advances, the implementation of network-wide control strategies in modern cities faces significant challenges: ensuring data availability and quality, achieving public acceptance, integrating with legacy infrastructure, and maintaining coordination across jurisdictions. The complexity of real-world urban environments (i.e., the presence of multimodal traffic, stochastic behaviours, and political constraints) denotes the need for robust, adaptive, and explainable control systems. Future research should focus on hybrid approaches that combine theoretical control models with empirical learning, and on developing MFD-based strategies that are resilient to irregular network conditions and responsive to equity, sustainability, and safety objectives.

Acknowledgments

This study was carried out within the MOST – Sustainable Mobility National Research Centre and received funding from the European Union Next-GenerationEU (PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR) – MISSIONE 4 COMPONENTE 2, INVESTIMENTO 1.4 – D.D. 1033 17/06/2022, CN00000023). This chapter reflects only the authors' views and opinions; neither the European Union nor the European Commission can be considered responsible for them. It was also partially funded by the project I CAN BE "Progetti di Rilevante Interesse Nazionale" (PRIN 2022 -MUR).

Conflict of Interest

The authors declare no conflict of interest.

Appendix A

This appendix provides a formal explanation of why accumulation, rather than density, is used in the MFD for wide-area traffic control. The derivation bridges the classical link-level fundamental diagram and its aggregated network-level counterpart, clarifying the modeling assumptions underlying **Figure 1** and Section 2.1.

Although classical fundamental diagrams describe the relationship between flow q (veh/h) and density k (veh/km), MFD-based control frameworks express this relationship in terms of accumulation n (veh). For a single link of fixed length L, density and accumulation are directly proportional:

$$k_i = \frac{n_i}{L} \tag{1}$$

Thus, the link FD retains the same shape whether the horizontal axis is expressed in k_i or n_i. At the network scale, however, defining a meaningful density is

challenging because links have heterogeneous lengths and detectors do not provide continuous spatial coverage. Accumulation, defined as the total number of vehicles within a region ($\mathcal{R}$), can instead be measured or estimated robustly and align naturally with the needs of wide-area control, where:

$$n = \sum_{i \in \mathcal{R}} n_i \tag{2}$$

Moreover, under mild homogeneity conditions, the network production P (veh-km/hs), also known as vehicle kilometre travelled (VKT) is the total trip completion rate across all links which can be approximated as a function of regional accumulation:

$$P = \sum_i P_i = \sum_i q_i(n_i) = \mathrm{q}\left(\sum_i n_i\right) \cong O(n) \tag{3}$$

which yields the characteristic MFD used to regulate system performance in real time.

Author details

Franco Filippi, Roberta Di Pace*, Facundo Storani and Stefano de Luca
University of Salerno, Salerno, Italy

*Address all correspondence to: rdipace@unisa.it

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] Sims AG, Dobinson KW. The Sydney Coordinated Adaptive Traffic (SCAT) System philosophy and benefits. IEEE Transactions on Vehicular Technology. 1980;**29**: 130–137

[2] Hunt PB, Robertson DI, Bretherton RD, et al. The SCOOT on-line traffic signal optimisation technique. Traffic Engineering & Control. 1982;**23**:190–192

[3] Wall A, Luk L, Green D. Balancing traffic density in a signalised network. AP-R369/10 Austroads Research Report

[4] Gartner NH, Pooran FJ, Andrews CM. Implementation of the OPAC adaptive control strategy in a traffic signal network. In: IEEE Conference on Intelligent Transportation Systems, Proceedings, ITSC; 2001; 195–200

[5] Aboudolas K, Papageorgiou M, Kosmatopoulos E. Store-and-forward based methods for the signal control problem in large-scale congested urban road networks. Transportation Research Part C: Emerging Technologies. 2009;**17**:163–174

[6] Kouvelas A, Aboudolas K, Papageorgiou M, et al. A hybrid strategy for real-time traffic signal control of urban road networks. IEEE Transactions on Intelligent Transportation Systems. 2011;**12**:884–894

[7] Diakaki C, Papageorgiou M, Aboudolas K. A multivariable regulator approach to traffic-responsive network-wide signal control. Control Engineering Practice. 2002;**10**:183–195

[8] Diakaki C, Dinopoulou V, Aboudolas K, et al. Extensions and new applications of the traffic-responsive urban control strategy: Coordinated signal control for urban networks. Transportation Research Record: Journal of the Transportation Research Board. 2003;**1856**:202–211. DOI: 103141/1856-22

[9] Tsitsokas D, Kouvelas A, Geroliminis N. Two-layer adaptive signal control framework for large-scale networks. In: 31st Mediterranean Conference on Control and Automation, MED 2023; 2023; **152**:452–457

[10] Kouvela A, Triantafyllos D, Geroliminis N. Two-layer hierarchical control for large-scale urban traffic networks. In: 2018 European Control Conference, ECC 2018; 2018; 1295–1300

[11] Zhou Z, De Schutter B, Lin S, et al. Two-level hierarchical model-based predictive control for large-scale urban traffic networks. IEEE Transactions on Control Systems Technology. 2017;**25**:496–508

[12] Ramezani M, Haddad J, Geroliminis N. Two-level hierarchical traffic control for heterogeneous urban networks. In: 2015 European Control Conference, ECC 2015; 2015; 3484–3489

[13] Geroliminis N, Daganzo CF. Existence of urban-scale macroscopic fundamental diagrams: Some experimental findings. Transportation Research Part B: Methodological. 2008;**42**:759–770

[14] Ji Y, Geroliminis N. On the spatial partitioning of urban transportation networks. Transportation Research Part B: Methodological. 2012;**46**:1639–1656

[15] Geroliminis N, Haddad J, Ramezani M. Optimal perimeter control for two urban regions with macroscopic fundamental diagrams: A model predictive approach. IEEE Transactions on Intelligent Transportation Systems. 2013;**14**: 348–359

[16] Keyvan-Ekbatani M, Kouvelas A, Papamichail I, et al. Exploiting the fundamental diagram of urban networks for feedback-based gating. Transportation Research Part B: Methodological. 2012;**46**: 1393–1403

[17] Ji Y, Daamen W, Hoogendoorn S, et al. Investigating the shape of the macroscopic fundamental diagram using simulation data. Transportation Research Record: Journal of the Transportation Research Board. 2010;2161:40–48

[18] Ambühl L, Menendez M. Data fusion algorithm for macroscopic fundamental diagram estimation. Transportation Research Part C: Emerging Technologies. 2016;**71**: 184–197

[19] Leclercq L, Chiabaut N, Trinquier B. Macroscopic fundamental diagrams: A cross-comparison of estimation methods. Transportation Research Part B: Methodological. 2014;**62**:1–12

[20] Dakic I, Menendez M. On the use of Lagrangian observations from public transport and probe vehicles to estimate car space-mean speeds in bi-modal urban networks. Transportation Research Part C: Emerging Technologies. 2018;**91**:317–334

[21] Daganzo CF, Geroliminis N. An analytical approximation for the macroscopic fundamental diagram of urban traffic. Transportation Research Part B: Methodological. 2008;**42**: 771–781

[22] Richards PI. Shock waves on the highway. Operations Research. 1956;**4**:42–51. DOI: 101287/opre4142

[23] Daganzo CF. A variational formulation of kinematic waves: Basic theory and complex boundary conditions. Transportation Research Part B: Methodological. 2005;**39**: 187–196

[24] Leclercq L, Geroliminis N. Estimating MFDs in simple networks with route choice. Transportation Research Part B: Methodological. 2013;**57**:468–484

[25] Geroliminis N, Sun J. Properties of a well-defined macroscopic fundamental diagram for urban traffic. Transportation Research Part B: Methodological. 2011;**45**:605–617

[26] Kouvelas A, Saeedmanesh M, Geroliminis N. Real-time estimation of aggregated traffic states of multi-region urban networks. IEEE Conference on Intelligent Transportation Systems, Proceedings, ITSC 2017; 2018, March. 1–6

[27] Ortigosa J, Menendez M, Tapia H. Study on the number and location of measurement points for an MFD perimeter control scheme: A case study of Zurich. EURO Journal on Transportation and Logistics. 2015;**3**:245–266

[28] Keyvan-Ekbatani M, Yildirimoglu M, Geroliminis N, et al. Multiple concentric gating traffic control in large-scale urban networks. IEEE Transactions on Intelligent Transportation Systems. 2015;**16**: 2141–2154

[29] Mariotte G, Leclercq L, Batista SFA, et al. Calibration and validation of multi-reservoir MFD models: A case study in Lyon. Transportation Research Part B: Methodological. 2020;**136**: 62–86

[30] Keyvan-Ekbatani M, Gao X, V. GV, et al. Examining perimeter gating control of urban traffic networks with locally adaptive traffic signals. Traffic and Granular Flow '15. 2016;579–586

[31] Aboudolas K, Geroliminis N. Feedback Perimeter Control for Multi-region and Heterogeneous Congested Cities. 2013. Available from: https://trid.trb.org/view.aspx?id=1241561 [Accessed: 2025-January-06]

[32] Keyvan-Ekbatani M, Papageorgiou M, Papamichail I. Urban congestion gating control based on reduced operational network fundamental diagrams. Transportation Research Part C: Emerging Technologies. 2013;**33**:74–87

[33] Lu W, Liu J, Mao J, et al. Macroscopic fundamental diagram approach to evaluating the performance of regional traffic controls. Transportation Research Record: Journal of the Transportation Research Board. 2020;**2674**:420–430

[34] Bellemans T, De Schutter B, De Moor B. Model predictive control for ramp metering of motorway traffic: A case study. Control Engineering Practice. 2006;**14**:757–767

[35] Papamichail I, Kotsialos A, Margonis I, et al. Coordinated ramp metering for freeway networks – A model-predictive hierarchical control approach. Transportation Research Part C: Emerging Technologies. 2010;**18**: 311–331

[36] Hegyi A, De Schutter B, Hellendoorn H. Model predictive control for optimal coordination of ramp metering and variable speed limits. Transportation Research Part C: Emerging Technologies. 2005;**13**: 185–209

[37] Lin S, De Schutter B, Xi Y, et al. Fast model predictive control for urban road networks via MILP. IEEE Transactions on Intelligent Transportation Systems. 2011;**12**: 846–856

[38] Ye B-L, Wu W, Ruan K, et al. A survey of model predictive control methods for traffic signal control. IEEE/CAA Journal of Automatica Sinica. 2019;**6**:623–640

[39] Ni W, Cassidy MJ. Cordon control with spatially-varying metering rates: A reinforcement learning approach. Transportation Research Part C: Emerging Technologies. 2019;**98**: 358–369

[40] Ni W, Cassidy M. City-wide traffic control: Modeling impacts of cordon queues. Transportation Research Part C: Emerging Technologies. 2020;**113**: 164–175

[41] Zhou D, Gayah VV. Model-free perimeter metering control for two-region urban networks using deep reinforcement learning. Transportation

Research Part C: Emerging Technologies. 2021;**124**:102949

[42] Chen C, Huang YP, Lam WHK, et al. Data efficient reinforcement learning and adaptive optimal perimeter control of network traffic dynamics. Transportation Research Part C: Emerging Technologies. 2022;**142**:103759

[43] Li Z, Zheng G, Liu Y, et al. Perimeter control method of road traffic regions based on MFD-DDPG. Sensors. 2023;**23**:7975

Chapter 15

A DRL-Based Control Strategy for Efficient Highway Entry in Congested Scenarios

Agostino Marcello Mangini, Gaetano Volpe, Antonio Salcuni and Maria Pia Fanti

Abstract

Efficient traffic management in high-density urban areas remains a critical challenge, particularly at highway entry ramps and merging points where congestion, sudden braking, and collision risks frequently occur. This chapter addresses the problem of coordinating vehicles entering ramps and intersections by formulating it as an optimization task aimed at minimizing delays, enhancing safety, and improving overall flow. To tackle this challenge, we propose a deep reinforcement learning approach based on the actor–critic framework, where intelligent traffic light agents are trained to dynamically manage vehicle entries. The design of the reward function plays a central role, as it balances safety and efficiency by penalizing excessive braking events while encouraging smooth traffic throughput. Simulations were conducted in a representative high-density traffic scenario located in Bologna, Italy. The results demonstrate that the proposed approach can significantly reduce congestion, lower waiting times, and increase safety margins compared with conventional management strategies. These findings highlight the potential of reinforcement learning techniques to support intelligent traffic control systems and provide a promising direction for future deployment in real-world urban and highway infrastructures.

Keywords: deep reinforcement learning, actor–critic framework, intelligent traffic light control, traffic flow efficiency, Simulation

1. Introduction

The continuous growth of vehicular traffic in urban and highway networks has made real-time traffic control increasingly complex. Traditional model-based or rule-based methods often fail to adapt to dynamic environments characterized by stochastic demand and the coexistence of human-driven and autonomous vehicles. In this context, deep reinforcement learning (DRL) has emerged as a powerful approach for adaptive traffic management and dynamic decision-making in uncertain and nonlinear systems [1, 2].

Unlike conventional optimization models, DRL enables agents to learn directly from interaction with the environment, adjusting their strategies through trial and error to maximize long-term rewards. This makes DRL particularly suitable for control problems where real-time adaptation and continuous decision-making are essential [3]. At the same time, swarm-based optimization methods, such as particle swarm optimization (PSO), have been widely explored for traffic control [4]. Although PSO achieves good convergence in static and low-dimensional optimization tasks, its reliance on global exploration reduces effectiveness in highly dynamic environments, where control policies must continuously adapt to rapid traffic fluctuations [5].

In recent years, the application of DRL to transportation systems has expanded significantly. Multi-agent and hierarchical DRL frameworks have been developed to coordinate intersections, regulate traffic flow, and optimize control fairness across multiple regions [6–9]. These approaches integrate distributed intelligence into the infrastructure, allowing cooperative decision-making among agents. Furthermore, techniques based on Reinforcement Learning (RL) have been incorporated into cyber–physical systems to enhance reliability, security, and adaptability under non-stationary conditions [10]. Multi-agent DRL has also been applied in mixed environments involving both autonomous and human-driven vehicles, addressing cooperation and collision avoidance in shared traffic contexts [11, 12].

In highway control, DRL has been integrated with Model Predictive Control (MPC) and Q-learning to improve coordination among ramp metering, variable speed limits, and lane control systems [13–16]. These techniques have demonstrated superior scalability and learning efficiency, offering a promising direction for intelligent traffic management.

A particularly critical scenario is the highway on-ramp merging problem, where vehicles must safely integrate into high-speed traffic streams. The optimization of merging operations requires balancing throughput, safety, and smoothness while minimizing congestion and sudden braking. Several DRL-based studies have addressed this problem, focusing on policy optimization through centralized or multi-agent architectures [17–19]. Other approaches have emphasized robustness against uncertain behaviors using constrained adversarial RL and hierarchical control strategies [20–24]. Safety-oriented frameworks, incorporating cooperative control barrier functions, have further enhanced the robustness of merging control [25].

Simulation tools, such as Simulation of Urban Mobility (SUMO), have proven essential for evaluating artificial intelligence (AI)-driven traffic control systems under realistic and reproducible conditions. SUMO supports the testing of adaptive control algorithms with microscopic precision, enabling validation of key metrics such as waiting time, safety indicators, and network throughput [26].

The contribution presented in this chapter builds upon the foundations of DRL-based merging optimization studies [17–19], which proposed communication-based or centralized actor–critic frameworks for highway entry coordination. While these works mainly focused on optimizing traffic throughput and acceleration smoothness, they generally neglected the joint impact of safety and braking stability under high-density conditions. The approach proposed here extends these studies by introducing a dual-agent actor–critic architecture designed to manage cooperative traffic light policies that regulate highway ramp entry. The method introduces a multi-objective reward function explicitly combining efficiency, safety, and comfort, penalizing excessive decelerations,

collisions, and prolonged waiting times. Moreover, the inclusion of bidirectional interaction between infrastructure agents enables adaptive coordination between entry and merging phases, improving flow regularity and safety margins compared to single-agent or purely vehicle-centric frameworks.

The proposed framework has been validated on a high-fidelity simulation of a real Italian highway scenario, characterized by dense traffic and limited merging space. Results demonstrate significant improvements in throughput, stability, and conflict avoidance compared with both traditional fixed-time control systems and standard DRL-based baselines [17–19].

This work advances the integration of DRL into intelligent transportation systems by addressing the interplay between connected vehicles and infrastructure-based control. The remainder of this chapter is organized as follows: Section 2 presents the problem formulation; Section 3 introduces the proposed actor–critic strategy; Section 4 discusses the simulation analysis and results; and finally, Section 5 concludes the chapter and outlines future research directions.

2. Problem formulation

The merging problem involves coordinating vehicle interactions on road segments where multiple traffic streams converge, such as highway ramps and intersections. Effective management strategies are needed to minimize congestion, reduce sudden braking, and enhance traffic flow. Traffic control mechanisms integrate predefined routes with intelligent signals to regulate merging operations.

Traffic routes define different vehicle interactions within the merging zone: vehicles entering the main traffic stream ($\mathcal{R}_{\text{in}}$), those changing direction and requiring lane transitions ($\mathcal{R}_{\text{turn}}$), and those traveling without lane changes ($\mathcal{R}_{\text{main}}$), which serve as a reference for evaluating interactions between merging and non-merging vehicles.

Intelligent traffic signals operate through multiple phases to ensure smooth merging. The $\mathcal{G}$ (Green) phase allows movement, while $\mathcal{R}$ (Red) forces vehicles to stop. Intermediate phases, such as $\mathcal{GR}$ and $\mathcal{RG}$ regulate merging by allowing traffic from one route while restricting the other.

The system coordinates vehicle entries and merging maneuvers: $\mathcal{S}_{\text{merge}}$ manages merging from a secondary road, alternating between $\mathcal{GR}$ and $\mathcal{RG}$ to prevent conflicts. $\mathcal{S}_{\text{entry}}$ controls vehicle entry at a regulated access point, alternating between $\mathcal{G}$ and $\mathcal{R}$ without stopping the main flow.

By integrating these mechanisms, traffic management dynamically adapts to varying conditions, optimizing throughput while maintaining safety in high-density road networks.

Figure 1 illustrates the considered environment: the left-side image (1) shows the merging route through which vehicles enter the second route; the right-side image (2) is the route that allows access to the highway.

2.1 Markov decision process

The merging problem is modeled as an MDP, defined by the tuple:

$$\mathcal{M} = (\mathcal{S}, \mathcal{A}, \mathcal{P}, \mathcal{R}, \gamma)$$

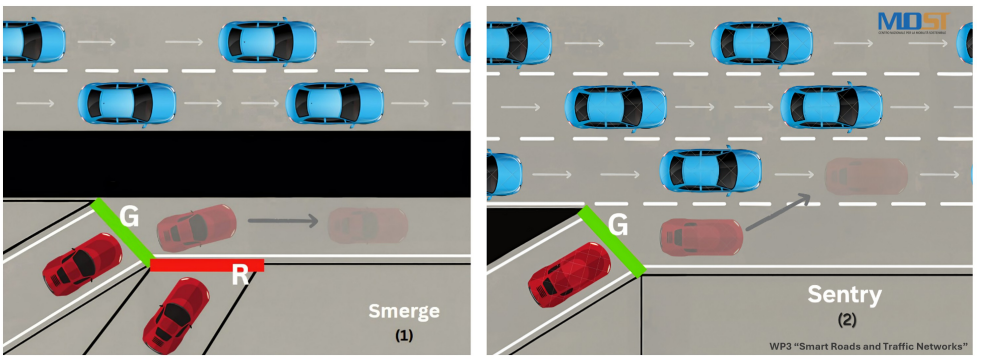


Figure 1.
The figure illustrates two different merging strategies in a highway scenario: S_{merge} (left) and S_{entry} (right). vehicles, after merging from two on-ramps regulated by the traffic light S_{merge}, continue along a single ramp toward the highway, which is controlled by the traffic light S_{entry}. The right-side image represents the natural continuation of the flow depicted on the left.

with

- $\mathcal{S}$ (State space): Represents traffic conditions;
- $\mathcal{A}$ (Action space): Represents the set of possible actions for controlling traffic signal phases.
- $\mathcal{P}$ (Transition probabilities): Defines the probabilistic evolution of the system's states given an action.
- $\mathcal{R}$ (Reward function): Balances safety and efficiency to optimize traffic flow.

γ (Discount factor): Determines the weight of future rewards in decision-making.

In our context, the class is model-free and, therefore, does not assume a probabilistic distribution $\mathcal{P}$.

2.2 State space and action space

At times t, the state s_t is defined as:

$$s_t = \{n_{\mathcal{R}_{\text{in}}}, n_{\mathcal{R}_{\text{turn}}}, n_{\mathcal{R}_{\text{main}}}, v_{\mathcal{R}_{\text{in}}}, v_{\mathcal{R}_{\text{turn}}}, v_{\mathcal{R}_{\text{main}}}\}$$

with

$n_{\mathcal{R}_{\text{in}}}$, $n_{\mathcal{R}_{\text{turn}}}$, $n_{\mathcal{R}_{\text{main}}}$ denote the vehicle counts in each route.

$v_{\mathcal{R}_{\text{in}}}$, $v_{\mathcal{R}_{\text{turn}}}$, $v_{\mathcal{R}_{\text{main}}}$ indicate the average speeds on the respective routes.

The action space is defined as a binary vector representing the state of the traffic signals:

$$S_t = \begin{bmatrix} S_{\text{merge}} \\ S_{\text{entry}} \end{bmatrix}$$

where:
$S_{\text{merge}} \in \{0,1\}$ controls the merging traffic light, with:

$$S_{\text{merge}} = \begin{cases} 0, & \text{if the signal is in phase } \mathcal{GR} \\ 1, & \text{if the signal is in phase } \mathcal{RG} \end{cases}$$

$S_{entry} \in \{0,1\}$ controls the entry traffic light, with:

$$S_{\text{entry}} = \begin{cases} 0, & \text{if the signal is in phase } \mathcal{R} \\ 1, & \text{if the signal is in phase } \mathcal{G} \end{cases}$$

Thus, the complete action space is:

$$\mathcal{S} = \{(0,0),(0,1),(1,0),(1,1)\}$$

where each action vector S_t defines the simultaneous state of both traffic lights at a given time t.

2.3 Reward function

The reward function is designed to balance traffic efficiency and safety, incorporating weighted penalties for collisions, sudden decelerations, and waiting times measured on key road segments:

$$\begin{aligned} R(s,a,t) = & -w_c \cdot n_c(s,a,t) - w_d \cdot d(s,a,t) \\ & - \Big(w_{\text{m}} \cdot t_{\text{m}}(s,a,t) + w_{\text{t}} \cdot t_{\text{t}}(s,a,t) + w_{\text{in}} \cdot t_{\text{in}}(s,a,t)\Big) \end{aligned} \tag{1}$$

where:
$n_c(s,a,t)$: Number of collisions at time t.
$d(s,a,t)$: Number of sudden deceleration events exceeding a threshold.
$t_{\text{m}}(s,a,t)$: Cumulative waiting time on the main road edge.
$t_{\text{t}}(s,a,t)$: Cumulative waiting time on the turning road edge.
$t_{\text{in}}(s,a,t)$: Cumulative waiting time on the highway ramp (entry) edge.
w_c: Weight associated with the severity of collisions.
w_d: Weight penalizing sudden decelerations, capturing traffic instability.
w_{m}, w_{t}, w_{in}: Weights penalizing waiting times on each edge correspond, respectively, to the main road, turning road, and highway ramp.

In addition, the cumulative sudden deceleration $d(s,a,t)$ is computed by summing the deceleration values of all vehicles that exceed a predefined threshold. For each vehicle$v$, the instantaneous deceleration is given by:

$$a_v(t) = \frac{v_v(t-1) - v_v(t)}{\Delta t} \tag{2}$$

where $v_v(t)$ is the velocity of the vehicle v at time t. If the deceleration exceeds the threshold a_{thr}, it contributes to the total penalty:

$$d(s,a,t) = \sum_{v \in V} \mathbf{1}_{\{a_v(t) > a_{\text{thr}}\}} \cdot a_v(t), \tag{3}$$

with $\mathbf{1}_{\{a_v(t) > a_{\text{thr}}\}}$ denoting the indicator function that equals 1 when the condition is satisfied and 0 otherwise.

This formulation ensures that only braking events above the threshold influence the reward function, penalizing unstable traffic conditions and promoting smoother traffic flow.

3. DRL approach

The DRL approach adopts the actor–critic framework, which integrates value-based and policy-based methods to optimize vehicle merging.

Traditional Q-learning relies on a tabular Q-function representation, where each state-action pair is stored explicitly. However, as the state space grows, the number of entries scales exponentially $\mathcal{O}(k^n)$, making this approach infeasible for traffic control scenarios with multiple variables. This necessitates function approximation techniques such as Deep Q-Learning (DQN).

While DQN addresses the limitations of tabular Q-learning using neural networks, it remains unsuitable for this problem due to:

- **Continuous action space:** DQN is designed for discrete actions, whereas traffic signal control often requires continuous adjustments.
- **Stability issues:** Traffic conditions evolve dynamically, making DQN harder to stabilize despite experience replay and target networks.
- **Inefficient policy optimization:** DQN indirectly learns a policy via value estimation, leading to suboptimal exploration and control in complex environments.

To overcome these issues, the actor–critic framework combines policy optimization with value estimation. The actor network maps states to actions, supporting continuous control, while the critic network stabilizes learning by estimating value functions. This synergy enhances adaptability and efficiency in dynamic traffic management.

3.1 Actor–critic framework

The DRL model utilizes two neural networks:

Actor network: That maps states to actions using a probabilistic policy $\pi(a|s)$. It outputs the probability of taking each possible action in a given state.

Critic network: That estimates the value of a state or the advantage of an action using a value function $V(s)$ or $Q(s,a)$.

The “actor” and “critic” work synergistically during the learning process. The actor selects an action based on the current policy, while the critic evaluates the chosen action by computing an estimate of the advantage or the error. The critic uses this error to update its parameters and provides feedback to the actor, which consequently updates its policy to favor actions that lead to higher rewards [27, 28].

The update of the critic parameters is based on the *Advantage Function* and the *TD-error* (temporal difference error). The TD-error measures how much the received reward deviates from the expected reward.

The advantage function $A(s,a)$ of a given action a in a state s is defined as the difference between the action-value function and the state-value function:

$$A(s,a) = Q(s,a) - V(s) \tag{4}$$

where:

$Q(s,a)$ is the action-value function, representing the expected return of taking action a in a state s and then following the current policy.

$V(s)$ is the state-value function, representing the expected return of a state s under the current policy.

The advantage function helps determine how much better an action is compared to the average value of the current state. Additionally, the advantage function is closely related to the TD error used in actor–critic algorithms to update the critic and, consequently, improve the actor's policy:

$$\delta = r + \gamma V(s') - V(s), \tag{5}$$

where r is the reward, γ is the discount factor, s is the current state, and s' is the next state. The architecture of the actor–critic framework is shown in **Figure 2**, while the agent parameters are reported in Appendix A.

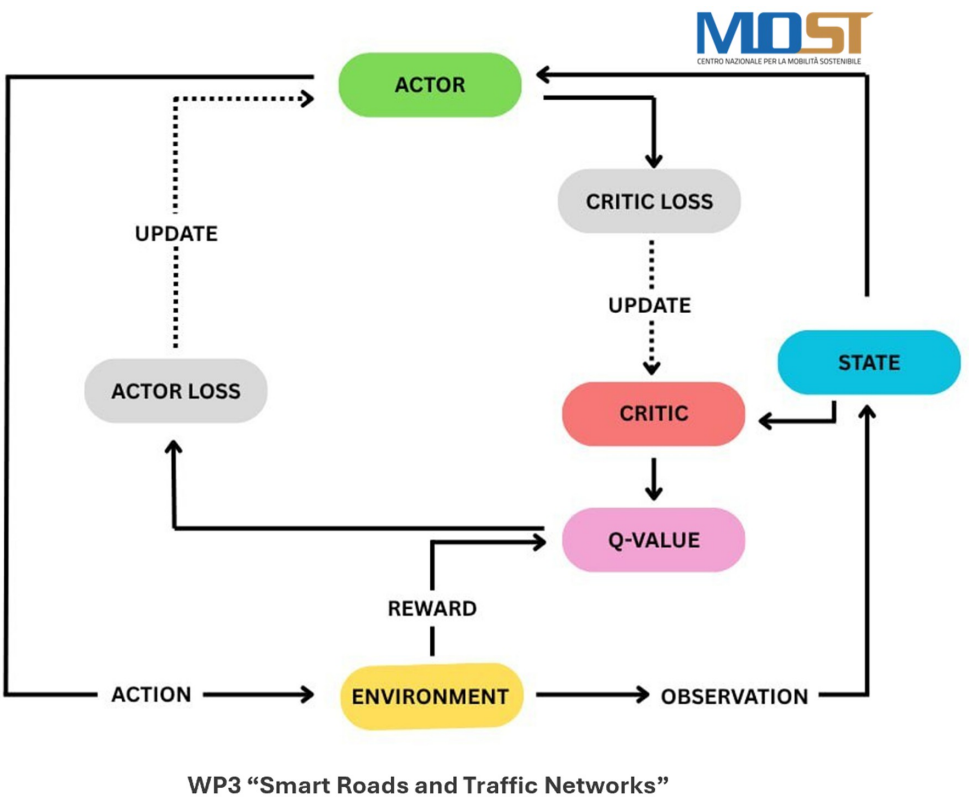


Figure 2.
Schematic of the actor–critic framework. The actor selects actions based on the current policy, while the critic evaluates them using the advantage function or temporal difference (TD) error. This feedback loop enables policy refinement and optimal decision-making in reinforcement learning.

3.2 Policy optimization

To train the actor–critic model, the proximal policy optimization (PPO) algorithm [29] is adopted, known for its robustness and stability. PPO updates the policy using a clipped surrogate objective, which prevents large and destructive updates. The loss function is defined as:

$$L_{PPO}(\theta) = \mathbb{E}_t\left[\min\left(r_t(\theta)A_t,\ \text{clip}(r_t(\theta), 1-\epsilon, 1+\epsilon)A_t\right)\right]$$

where:
$r_t(\theta) = \frac{\pi_\theta(a_t|s_t)}{\pi_{\theta_{old}}(a_t|s_t)}$ is the ratio between new and old policy probabilities.
ϵ is a hyperparameter limiting policy updates.
A_t is the advantage estimate.
This clipped objective ensures that policy updates remain within a conservative range, improving training stability – a critical feature in complex environments like urban traffic networks. PPO is particularly effective in problems where the decision space is sequential, dynamic, and must adapt to real-time conditions.

4. Case study

A case study was conducted at the intersection of the A13 Highway Bologna-Padova, Bologna's Tangenziale, and the A14 Highway. The location features high traffic volumes and complex ramp geometry, making it suitable for testing merging control strategies.

4.1 Simulation environment

The simulation presented in **Figure 3** was carried out using SUMO. The network topology was extracted from OpenStreetMap (OSM) and converted using `netconvert`. Key modeling choices:
Heterogeneous vehicle speeds and densities reproduce realistic interactions.
Two traffic lights $\mathcal{S}_{\text{merge}}$, $\mathcal{S}_{\text{entry}}$ alternate between green $\mathcal{G}$ and red $\mathcal{R}$;
Three main routes: $\mathcal{R}_{\text{in}}$, $\mathcal{R}_{\text{turn}}$, and $\mathcal{R}_{\text{main}}$.

4.2 Implementation steps

The scenario was prepared as follows:

1. Export the OSM map of the area and save it as `.osm`.
2. Convert to SUMO network with `netconvert`, producing `.net.xml`.
3. Define routes with `netedit` for $\mathcal{R}_{\text{in}}$, $\mathcal{R}_{\text{turn}}$, $\mathcal{R}_{\text{main}}$ as illustrated in **Figure 4.**
4. Configure traffic lights to alternate states (with initially static phases) and allow DRL-based control during learning and testing.

4.3 Performance indices

The effectiveness of the DRL control was evaluated using the following metrics (see **Table 1**).

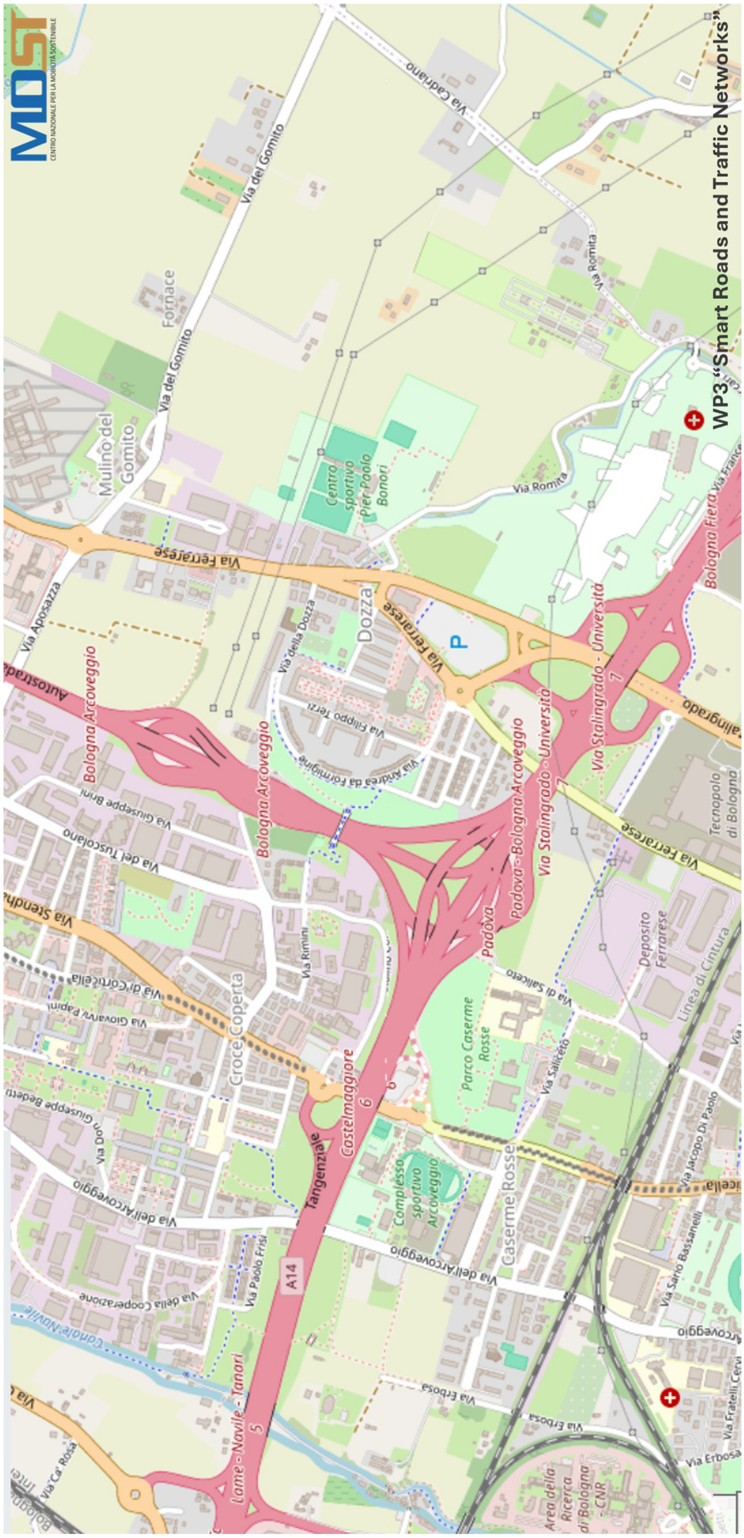


Figure 3.
Geometric layout of the A13–A14 intersection in the Bologna network. Merging zones, ramps, and flows are illustrated and used as a test environment for the DRL controller.

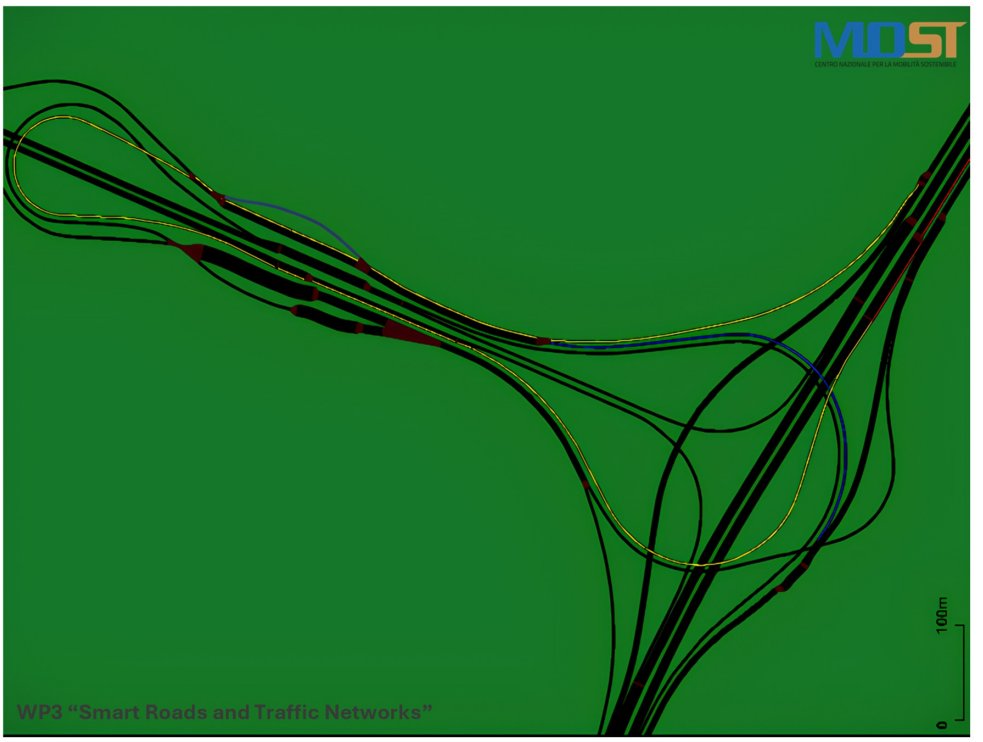


Figure 4.
Main routes: $\mathcal{R}_{\text{in}}$ (yellow) for merging vehicles, $\mathcal{R}_{\text{turn}}$ (blue) for U-turn maneuvers, and $\mathcal{R}_{\text{main}}$ (red) for through traffic.

Metric	Description
Collision frequency	Number of collisions recorded during the simulation.
Sudden braking events	Total deceleration events exceeding 4.5 m/s^2
Average waiting time	Average delay experienced by vehicles at merging zones.

Table 1.
Performance indices used for evaluation.

4.4 Training phase

The agent, representing an adaptive traffic light controller, was trained over 600 episodes, each consisting of 150 discrete simulation steps. The training environment was implemented in SUMO, designed to emulate realistic urban dynamics, including heterogeneous vehicle behaviors, stochastic inflow, and multi-lane interactions.

To assess the agent's ability to generalize across operational conditions, two distinct traffic regimes were constructed (in both cases, the cycle lasts 60 real seconds):

Low-medium traffic scenario: This scenario reproduces moderately congested conditions. In particular, this condition corresponds to typical weekday peak-hour traffic (12:00) recorded during less critical months, September–October 2025. Based on these empirical observations, vehicle flows were approximated through

randomized generation rules in SUMO: $\mathcal{R}_{\text{in}}$ and $\mathcal{R}_{\text{turn}}$ receive a low-to-moderate influx (3 to 8 vehicles per generation cycle), while $\mathcal{R}_{\text{main}}$ receives a slightly higher flow (15 to 20 vehicles per cycle). This stochastic generation preserves real-world variability while maintaining manageable interaction density.

Medium-high traffic scenario: This scenario reflects the congested conditions typically observed during the most critical part of the year, that is, weekday peak hours (12:00) in the highly trafficked summer period of July–August 2025. To replicate these conditions in SUMO, a higher and more variable randomized influx was adopted: $\mathcal{R}_{\text{main}}$ receives 30 to 45 vehicles, while $\mathcal{R}_{\text{in}}$ and $\mathcal{R}_{\text{turn}}$ receive between 6 and 15 vehicles per cycle. These values recreate the dense interaction patterns and congestion levels recorded in real traffic, while the stochasticity ensures robust training and generalization of the DRL agent.

Both scenarios shared an identical network topology and agent architecture, ensuring that observed differences in learning dynamics were attributable solely to traffic intensity. **Table 2** summarizes the key vehicle parameters that define driver behavior in the simulation.

All simulations were configured to include collision handling via the `<collision.action value = "teleport" />` directive in the SUMO configuration file. This setting ensures that vehicles involved in collisions are automatically removed from the network and repositioned, allowing the simulation to continue while still registering the event. Additional notes regarding the storage of simulation outputs are given in Appendix B.

The vehicle behavior was defined using the `<vType>` tag, with parameters chosen to reflect realistic urban driving dynamics. In particular, the `minGap` and `tau` parameters play a central role in shaping the overall prudence of the simulated drivers.

A low `minGap` value of 0.4 meters allows vehicles to follow each other more closely, increasing traffic density and interaction frequency. While this can improve throughput in low-congestion regimes, it also raises the risk of rear-end collisions and demands more precise control policies from the agent.

The `tau` parameter, set to 0.5 seconds, defines the driver's reaction time. A shorter `tau` implies quicker responsiveness to changes in traffic flow, enabling more agile maneuvers but also reducing the temporal buffer available to avoid conflicts. Together, low values of `minGap` and `tau` simulate a driving style that is assertive and potentially less cautious, requiring the agent to learn policies that balance efficiency with safety.

Parameter	Value and description
`vClass`	`Passenger`, `truck`–standard cars and heavy-duty freight vehicles.
`accel`	3.0 m/s^2 – maximum acceleration capability.
`decel`	6.0 m/s^2 – maximum comfortable braking deceleration.
`sigma`	0.5 – driver imperfection/noise factor.
`length`	5.0 m – physical length of the vehicle.
`maxSpeed`	30.33 m/s (≈109 km/h) – upper speed limit.
`minGap`	0.4 m – minimum bumper-to-bumper distance maintained.
`tau`	0.5 s – driver reaction time (headway).

Table 2.
Vehicle parameters used in the SUMO simulation.

Additionally, the `sigma` parameter introduces stochasticity in driver behavior, modeling imperfect human decision-making. The relatively high deceleration value ($6.0\ \mathrm{m/s^2}$) allows for aggressive braking when needed, while the moderate acceleration ($3.0\ \mathrm{m/s^2}$) ensures smooth recovery. These settings collectively define a driver profile that is reactive, moderately aggressive, and prone to dense interactions – ideal for testing the robustness of intelligent traffic control strategies under pressure. Given the simulated driver profile – characterized by reactive and moderately aggressive behavior – the agent's learning process was designed to mitigate emergent risks through a scalar reward signal composed of weighted penalties associated with undesirable traffic phenomena. The specific weights assigned to each penalized metric are detailed in **Table 3**, reflecting the relative importance of safety, flow efficiency, and strategic prioritization across road types.

These weights were empirically tuned to balance safety, throughput, and comfort, and they remained fixed across all training runs. During early training, the agent exhibited unstable behavior due to exploration-driven policy updates. As training progressed, convergence toward stable and effective control strategies was observed, with marked improvements in cumulative reward, collision avoidance, and traffic fluidity.

Figures 5–8, respectively, illustrate the evolution of the mean reward, collision count, cumulative deceleration events, and total waiting time across episodes for both traffic regimes.

To improve interpretability and reduce visual noise, all metrics are smoothed using a moving average computed over a 30-episode window. The original, unsmoothed values are retained in the plots for both traffic scenarios to allow direct comparison with the raw data.

4.5 Evaluation phase

To assess the operational impact of intelligent traffic light control, a comparative simulation was conducted under two distinct configurations:

- **Scenario 1: No traffic lights** – baseline configuration with uncontrolled intersections, relying solely on vehicle priority rules. The network topology was left unmodified, with no signalization elements present.

Component	Weight and rationale
Collision weight	$w_c = 100$ — This value enforces strict safety constraints by heavily penalizing any vehicular impact.
Waiting time (tangenziale road exit)	$w_{\mathrm{in}} = 10$ — reflects the strategic importance of ramp merging zones.
Waiting time (turning road)	$w_{\mathrm{t}} = 5$ — penalizes delays on turning roads.
Waiting time (Highway road)	$w_{\mathrm{m}} = 1$ — assigns minimal penalty to delays on main roads.
Sudden deceleration	$w_d = 1$ — penalizes abrupt braking events, which are indicative of discomfort and inefficient flow.

Table 3.
Reward weights used in the agent's learning process.

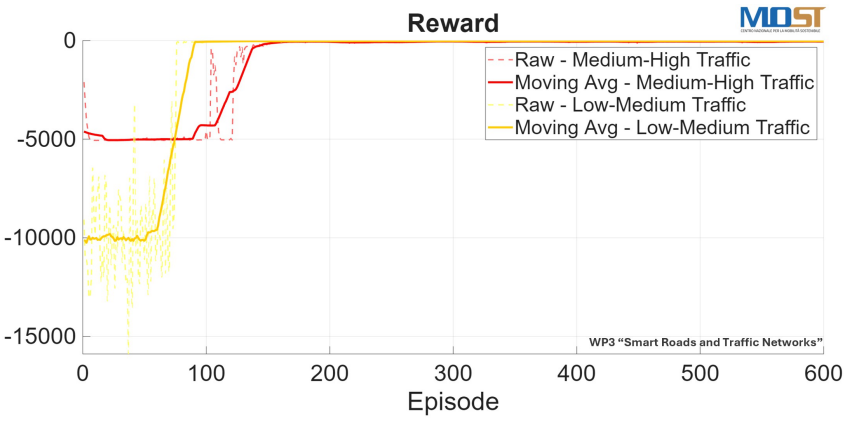


Figure 5.
Evolution of mean reward across training episodes under varying traffic conditions. The agent in low-to-medium traffic conditions reaches the correct behavior earlier due to the lower variability in the environment, whereas in scenarios with a higher number of vehicles, it converges more slowly. In both cases, however, the agent is ultimately able to find a policy that minimizes the cumulative reward to a similar extent.

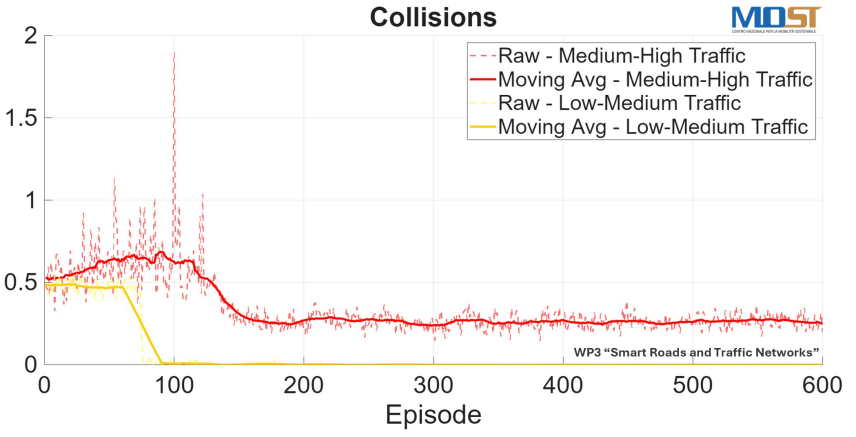


Figure 6.
Evolution of mean collisions across training episodes under varying traffic conditions. The agent exhibits a lower number of collisions following training in both scenarios, with near-zero convergence in low-density traffic. In higher-density scenarios, due to similarly aggressive driver parameters, complete elimination of collisions is harder to achieve; however, the presence of traffic lights still improves the overall network behavior.

- **Scenario 2: Intelligent DRL control** – adaptive intersection management using a DRL agent. The agent was previously trained over 600 episodes, and the evaluation was performed using one of the final episodes, representative of a converged policy.

Both scenarios were executed under identical traffic conditions, corresponding to a medium-density regime. Each simulation episode consisted of 400 discrete steps, allowing for consistent temporal comparison. The vehicle inflow, route distribution, and network geometry were held constant across both runs to isolate the effect of control logic. Performance metrics were computed by monitoring only the three

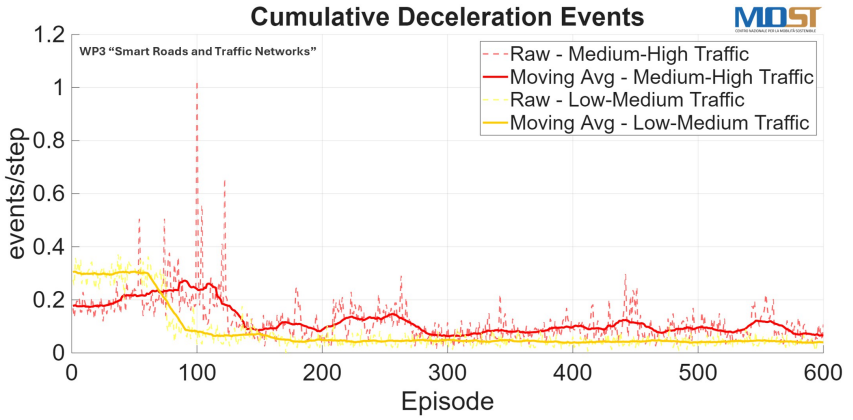


Figure 7.
Evolution of mean cumulative deceleration events across training episodes under varying traffic conditions. In low-density traffic, the agent quickly stabilizes with fewer deceleration events, indicating smoother driving behavior. Under higher-density conditions, convergence is slower due to increased interactions among vehicles, yet the presence of traffic lights still contributes to a more stable and coordinated overall flow.

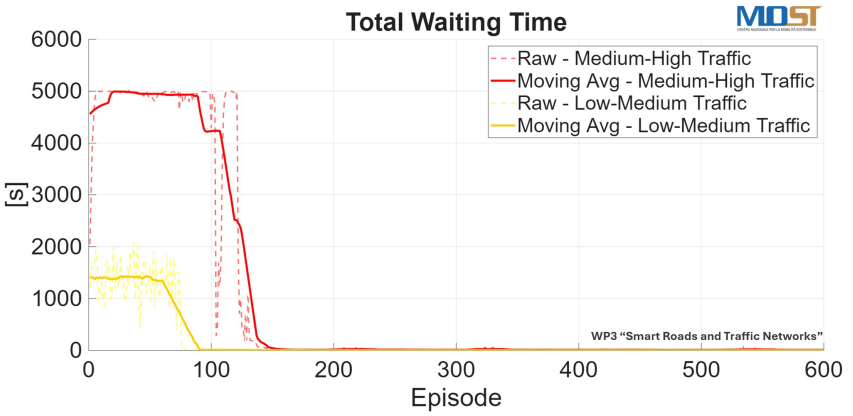


Figure 8.
Evolution of mean total waiting time across training episodes under varying traffic conditions. The high-density traffic scenario shows a delayed stabilization of the waiting time; however, convergence toward near-zero values is ultimately achieved in both cases.

edges directly connected to the intersections of the main routes: $\mathcal{R}_{\text{in}}$, $\mathcal{R}_{\text{turn}}$, and $\mathcal{R}_{\text{main}}$. This localized evaluation focuses on the most critical zones for traffic coordination and conflict resolution.

Figure 9 reports the evolution of average waiting times over the simulation horizon, restricted to vehicles present on the monitored edges. The DRL-controlled scenario exhibits significantly lower and more stable delays, indicating improved responsiveness and reduced queuing in key areas.

Figure 10 shows the number of vehicles present on the same three edges over time. The intelligent control scenario maintains a consistently lower vehicle count, suggesting enhanced throughput and reduced congestion relative to the unmanaged baseline.

Table 4 reports the comparison of averaged values extracted from MATLAB post-processing of the simulation data over 400 simulation steps. Unlike **Figures 9** and **10**,

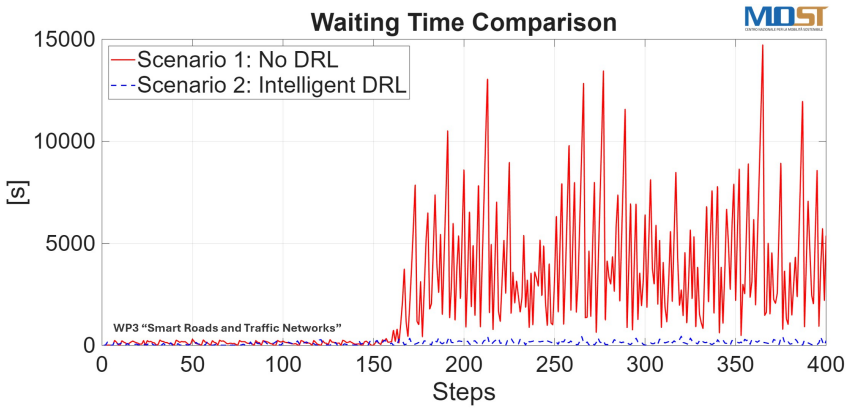


Figure 9.
Average waiting times over 400 simulation steps, computed on the three edges associated with the main intersections. The DRL-controlled scenario reduces delays compared to the baseline with no traffic lights.

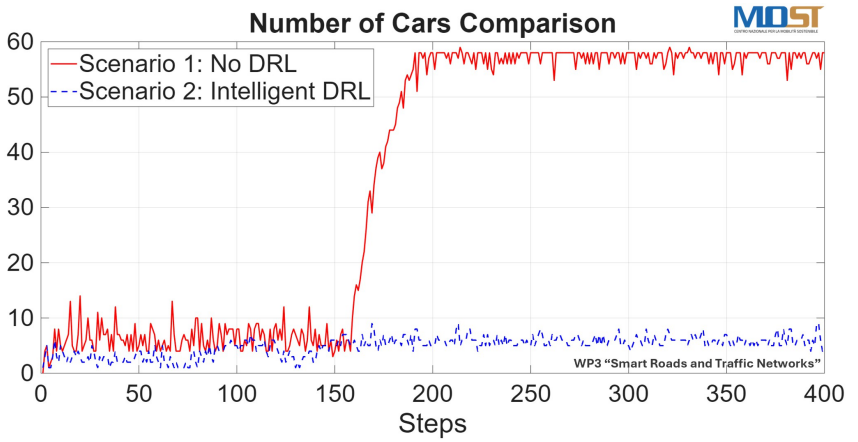


Figure 10.
Number of vehicles over time on the three monitored edges. Intelligent DRL control leads to lower vehicle accumulation and improved flow relative to the unmanaged baseline.

Metric	Baseline (No DRL)	Intelligent DRL
Waiting time R_{in} [s]	1,492.24	34.89
Waiting time R_{turn} [s]	892.17	6.50
Waiting time R_{main} [s]	115.98	83.61
Vehicles on Edge 1	19.73	1.09
Vehicles on Edge 2	11.85	0.75
Vehicles on Edge 3	3.91	3.09
Collision count	0.11	0.03

Table 4.
Comparison of average traffic metrics between the baseline (no control) and the DRL scenario.

which illustrate the temporal evolution of waiting times and vehicle counts, this table condenses the results into mean indicators. The comparison highlights the substantial reduction in average waiting times and vehicle presence achieved under the DRL-controlled scenario, together with a lower collision frequency, confirming the improved efficiency and safety relative to the unmanaged baseline. In this analysis, Edge1, Edge2, and Edge3 denote the incoming approaches to the signalized intersection, that is, the roadway segments immediately upstream of each traffic signal.

5. Conclusion

This chapter introduces a DRL-based actor–critic framework to optimize vehicle merging at highway ramps and intersections. Two intelligent traffic lights act as agents to regulate highway entry under congested conditions. Simulation results from the A13–A14 case study demonstrate: (1) the consistency of performance metrics across two different traffic scenarios; (2) improved performance of the DRL controller after training compared to the initial untrained (static SUMO phase) configuration; and (3) better overall results than a baseline scenario without traffic lights.

Future work will investigate scaling to larger networks, integrating IoT and V2X data for real-time operation, and exploring multi-agent RL to coordinate distributed controllers.

Nomenclature

$\mathcal{R}_{\text{in}}$	Merging route for vehicles coming from the ring road and entering the highway (first the A13 Bologna–Padova, then the A14). This section is prone to sudden braking due to competition for merging into the main traffic stream.
$\mathcal{R}_{\text{turn}}$	Route for vehicles already on the A14 highway that need to perform U-turns to travel in the opposite direction. The presence of ramps and interchanges introduces critical situations, as vehicles must cross multiple lanes to complete the maneuver.
$\mathcal{R}_{\text{main}}$	Main highway route on the A14, where vehicles travel straight without changing lanes. This route is essential for evaluating interactions between through traffic and merging or turning vehicles.
$\mathcal{S}_{\text{merge}}$	Traffic light controlling vehicles merging onto the secondary route.
$\mathcal{S}_{\text{entry}}$	Traffic light regulating highway entries.
$\mathcal{G}$, $\mathcal{R}$	Green and red signal phases, respectively.
s_t	State vector of the environment at time t.
S_t	Action vector defining the states of both traffic lights.
$n_{\mathcal{R}_i}$	Number of vehicles on route $\mathcal{R}_i$ at time t.
$v_{\mathcal{R}_i}$	Average speed of vehicles on route $\mathcal{R}_i$ (m/s).
$a_v(t)$	Deceleration of vehicle v at time t (m/s^2).
a_{thr}	Threshold deceleration value used for penalty computation (m/s^2).
$n_c(s,a,t)$	Number of collisions occurring at time t.
$d(s,a,t)$	Cumulative deceleration penalty at time t.

$w_c, w_d, w_t,$ w_m, w_{in}	Weights used in the reward function for collisions, decelerations, and waiting times.
$t_{\text{m}}, t_{\text{t}}, t_{\text{in}}$	Cumulative waiting time used in the reward function.
$R(s,a,t)$	Reward function balancing safety and efficiency.
$\pi(a\|s)$	Policy defining the probability of taking action a in state s.
$V(s)$	State-value function estimating the expected return from state s.
$Q(s,a)$	Action-value function estimating the expected return of action a in state s.
$A(s,a)$	Advantage function measuring the relative quality of action a in state s.
δ	Temporal difference (TD) error used for Critic updates.
γ	Discount factor for future rewards.

Acknowledgments

This study was carried out within the MOST – Sustainable Mobility National Research Centre and received funding from the European Union Next-GenerationEU (PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR) – MISSIONE 4 COMPONENTE 2, INVESTIMENTO 1.4 – D.D. 1033 17/06/2022, CN00000023). This chapter reflects only the authors' views and opinions; neither the European Union nor the European Commission can be considered responsible for them.

It is also part of the CHORUS (Coordination of Heterogeneous Actors in Mixed Traffic within CCAM) EU-project, which has received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement No. 101202981.

The authors acknowledge Overleaf (https://www.overleaf.com/) and its "Language Tool add-on" for help in checking potential grammar mistakes.

Appendix

Appendix A: DRL agent parameters

- **Framework:** Python 3.11 with TensorFlow 2.x and Ray RLlib, executed within a Conda-managed environment.
- **Learning algorithm:** On-policy Proximal Policy Optimization (PPO) using a custom actor–critic architecture with a clipped surrogate objective (Schulman et al., 2017).
- **Network architecture:**
  - Actor: Fully connected feedforward network with hidden layers, progressively reducing neurons (128 in the first, 64 in the second, 32 in the third), ReLU activations, and sigmoid output for binary control over each traffic signal.
  - Critic: Identical hidden structure with linear output for state-value estimation.
- **Action representation:** Binary vector $[a_1, a_2]$ indicating activation states of each traffic signal, obtained from thresholded actor output probabilities.

- **Optimization:**
  - Actor: Adam optimizer, learning rate $\alpha = 10^{-4}$.
  - Critic: Adam optimizer, learning rate $\alpha = 10^{-3}$.
- **Advantage estimation:** Generalized advantage estimation (GAE) with discount factor $\gamma = 0.99$ and $\lambda = 0.95$ normalization over each batch.
- **Policy update:** Clipped surrogate objective with ratio threshold $\epsilon = 0.2$, ensuring stable policy updates and bounded KL divergence.
- **Training loop:** Batch-based updates using sampled trajectories, with separate gradient computations for actor and critic losses.

Appendix B: Additional notes

The simulation outputs were stored in CSV files containing information on vehicle IDs, route identifiers, positions, velocities, emissions, and traffic light phases. The trained neural network weights for the actor and critic models were saved in `.h5` format. Data processing and visualization were performed using Python libraries such as `pandas` and `matplotlib`.

Author details

Agostino Marcello Mangini*, Gaetano Volpe, Antonio Salcuni and Maria Pia Fanti
Politecnico di Bari, Bari, Italy

*Address all correspondence to: agostinomarcello.mangini@poliba.it

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] Singh D. Deep reinforcement learning (DRL) for real-time traffic management in smart cities. In: 2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI); 2023; Greater Noida, India: IEEE; 2023. p. 1001–1004. DOI: 10.1109/ICCSAI59793.2023.10421359

[2] He Y, Kong Y. Traffic impact analysis of expressway accident in mixed traffic environment of connected and autonomous considering multi-factor coupling. In: IEEE Access. 2025;**13**:57342–57353. DOI: 10.1109/ACCESS.2025.3547236

[3] Burugadda VR, Jadhav N, Vyas N, Duggar R. Exploring the potential of deep reinforcement learning for autonomous navigation in complex environments. In: 2023 7th International Conference on Computing, Communication, Control and Automation (ICCUBEA); 17-19 August 2023; Pune, India: IEEE; 2023. p. 1–6. DOI: 10.1109/ICCUBEA58933.2023.10392109

[4] Tan MK, Ladillah MR, Chuo HSE, Lim KG, Chin RKY, Teo KTK. Optimization of signalized traffic network using swarm intelligence. In: 2021 IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET); 13-15 September 2021; Kota Kinabalu, Malaysia: IEEE; 2021. p. 1–6. DOI: 10.1109/IICAIET51634.2021.9573784

[5] Wu S. Research on county traffic optimization model based on spatio-temporal big data analysis. In: 2024 4th International Signal Processing, Communications and Engineering Management Conference (ISPCEM); 2024; China: IEEE; p. 563–567. DOI: 10.1109/ISPCEM64498.2024.00101

[6] Mao F, Li Z, Lin Y, Li L. Mastering arterial traffic signal control with multi-agent attention-based soft actor-critic model. IEEE Transactions on Intelligent Transportation Systems. 2023;**24**(3):3129–3144. DOI: 10.1109/TITS.2022.3229477

[7] Zhu Y, Lv Y, Lin S, Xu J. A stochastic traffic flow model-based reinforcement learning framework for advanced traffic signal control. IEEE Transactions on Intelligent Transportation Systems. 2025;**26**(1):714–723. DOI: 10.1109/TITS.2024.3494251

[8] Cai S, Fang J, Xu M. FairSignal: A multiagent reinforcement learning approach considering fairness for multi-intersection traffic signal control. IEEE Internet of Things Journal. 2025;**12**(13):23835–23851. DOI: 10.1109/JIOT.2025.3555822

[9] Wang Y, Cai W, Tu Y, Mao J. Reinforcement-learning-informed prescriptive analytics for air traffic flow management. IEEE Transactions on Automation Science and Engineering. 2024;**21**(3):4188–4202. DOI: 10.1109/TASE.2023.3292921

[10] Qiao Z, et al. Reinforcement learning-based security enhancement for controlled optimization of phases in intelligent traffic signal system. In: IEEE Transactions on Industrial Cyber-Physical Systems. 2024;**2**:575–587. DOI: 10.1109/TICPS.2024.3476455

[11] Zheng P, Chen Y, Kumar BVD. Regional intelligent traffic signal control system based on multi-agent deep reinforcement learning. In: 2023 8th International Conference on Computer and Communication Systems (ICCCS); 2023; Singapore: IEEE; p. 362–367. DOI: 10.1109/ICCCS57501.2023.10150595

[12] Huang M, Zheng F. Smart pedestrian-vehicle signal light: A policy gradient-based deep reinforcement learning model for single-intersection traffic signal control. In: 2025 5th International Conference on Neural Networks, Information and Communication Engineering (NNICE); Guangzhou, China: IEEE; 2025. p. 1224–1231. DOI: 10.1109/NNICE64954.2025.11064433

[13] Yuan T, Ioannou PA. Integrated freeway traffic control using Q-learning with adjacent arterial traffic considerations. IEEE Transactions on Intelligent Transportation Systems. 2025;**26**(6):7655–7666. DOI: 10.1109/TITS.2025.3559893

[14] Liu F, Tan Z, Chan HK, Zheng L. Ramp metering control on wireless charging lanes considering optimal traffic and charging efficiencies. IEEE Transactions on Intelligent Transportation Systems. 2024;**25**(9):11590–11601. DOI: 10.1109/TITS.2024.3381847

[15] He J, Yang J, Zhao J, Jia P, Li Y, Wang H. Simulation and evaluation of typical scenarios of smart expressway based on multi-level traffic cooperative control strategy. In: 2023 IEEE 8th International Conference on Intelligent Transportation Engineering (ICITE); Beijing, China: IEEE; 2023. p. 326–335. DOI: 10.1109/ICITE59717.2023.10733844

[16] Tyuplyaev N, Lukianchenko P. Stability analysis framework of traffic control algorithms. In: 2024 26th International Conference on Digital Signal Processing and its Applications (DSPA); Russia: IEEE; 2024. p. 1–6. DOI: 10.1109/DSPA60853.2024.10510125

[17] Kherroubi Z, Aknine S, Bacha R. Novel decision-making strategy for connected and autonomous vehicles in highway on-ramp merging. IEEE Transactions on Intelligent Transportation Systems. 2022;**23**(8):12490–12502. DOI: 10.1109/TITS.2021.3114983

[18] Li M, Li Z, Wang S, Zheng S. Enhancing cooperation of vehicle merging control in heavy traffic using communication-based soft Actor-Critic Algorithm. IEEE Transactions on Intelligent Transportation Systems. 2023;**24**(6):6491–6506. DOI: 10.1109/TITS.2022.3221450

[19] Chen D, et al. Deep Multi-Agent reinforcement learning for highway on-ramp merging in mixed traffic. IEEE Transactions on Intelligent Transportation Systems. 2023;**24**(11):11623–11638. DOI: 10.1109/TITS.2023.3285442

[20] He X, Lou B, Yang H, Lv C. Robust decision making for autonomous vehicles at highway on-ramps: A constrained adversarial reinforcement learning approach. IEEE Transactions on Intelligent Transportation Systems. 2023;**24**(4):4103–4113. DOI: 10.1109/TITS.2022.3229518

[21] Peng R, Yang M, Tao R, Zhang M, Zhang R. Hierarchical control strategy for cooperative on-ramp merging of connected and automated vehicles on multilane highways. IEEE Internet of

Things Journal. 2025;**12**(16):34513–34527. DOI: 10.1109/JIOT.2025.3578530

[22] Zhang X, Wu L, Liu H, Wang Y, Li H, Xu B. High-speed ramp merging behavior decision for autonomous vehicles based on multiagent reinforcement learning. IEEE Internet of Things Journal. 2023;**10**(24):22664–22672. DOI: 10.1109/JIOT.2023.3304890

[23] Gao K, Liu X, Hu H, Liu L, Ye L, Du R. Research on on-ramp merging decision-making for autonomous vehicles based on the dueling-DQN algorithm. In: 2024 IEEE International Conference on High Performance Computing and Communications (HPCC); China: IEEE; 2024. p. 1657–1664. DOI: 10.1109/HPCC64274.2024.00219

[24] Xu X, Lai M, Zhang H, Dong X, Li T, Wu J, Li Y, Peng T. Spatio-temporal cooperative control method of highway ramp merge based on vehicle–road coordination. In: 2024 12th International Conference on Traffic and Logistic Engineering (ICTLE); 2024; China: IEEE; p. 93–98. DOI: 10.1109/ICTLE62418.2024.10703891

[25] Chang PY, Bhatti SG, Javed NU, Ahmed Q. Enhancing safety at highway ramps and intersections using safe cooperative controls in automated vehicles. In: 2024 IEEE 27th International Conference on Intelligent Transportation Systems (ITSC); 2024; Spain. IEEE; p. 902–907. DOI: 10.1109/ITSC58415.2024.10920020

[26] Gonzalez-Delicado JJ, Gozalvez J, Mena-Oreja J, Sepulcre M, Coll-Perales B. Alicante-Murcia freeway scenario: A high-accuracy and large-scale traffic simulation scenario generated using a novel traffic demand calibration method in SUMO. In: IEEE Access; 2021;**9**:154423–154434. DOI: 10.1109/ACCESS.2021.3126269

[27] Sutton RS, Barto AG. Reinforcement Learning: An Introduction. 2nd ed. Cambridge, MA: MIT Press; 2018

[28] Dutta D, Upreti SR. A survey and comparative evaluation of actor-critic methods in process control. Canadian Journal of Chemical Engineering. 2022;**100**(9):2028–2056. DOI: 10.1002/cjce.24508

[29] Schulman J, Wolski F, Dhariwal P, Radford A, Klimov O. "Proximal Policy Optimization Algorithms. 2017

Chapter 16

Connected and Autonomous Vehicle Platoons and Traffic Bottlenecks: Effects on Recurrent and Non-Recurrent Congestion in Mixed Traffic Conditions

Caterina Malandri, Luca Mantecchini, Maria Nadia Postorino and Xuelian Wu

Abstract

Connected and autonomous vehicles (CAVs) are expected to play a transformative role in highway traffic, particularly through platooning strategies. Specifically, they are expected to enhance operational conditions at bottlenecks by reducing the propagation of congestion and the emergence of safety-critical conflicts. In these contexts, CAV platoons might increase flow capacity by operating with shorter headways, while they could enhance safety by adopting more coordinated maneuvers. While existing research has shown the potential of CAVs to enhance traffic performance, significant gaps remain regarding how platoons behave under bottleneck conditions, especially in mixed traffic with both CAVs and human-driven vehicles (HDVs). This chapter explores the impacts of CAV platoons on highway traffic performance under mixed traffic conditions, focusing on their role at bottlenecks. Two cases are considered: (i) a recurrent bottleneck in a highway merging area, where the interaction between entering and mainline flows typically generates congestion, and (ii) a non-recurrent bottleneck produced by a vehicle breakdown, causing temporary capacity reduction. Using microsimulation-based analyses, this study investigates how platoon size and CAV market penetration rate (MPR) influence traffic capacity, travel times, and environmental impacts. Results show that CAV platoons may reduce congestion in recurrent situations and improve resilience under non-recurrent disruptions: specifically, in highway merging areas, platooning increases flow capacity and reduces travel times, while in the case of vehicle breakdowns, platoons help mitigate capacity drops and limit delays, particularly at higher MPRs and moderate platoon sizes. These findings contribute to a deeper understanding of the opportunities and challenges of CAV platoon deployment.

Keywords: connected and autonomous vehicles (CAVs), platooning, mixed traffic, highway bottlenecks, on-ramp merging, vehicle breakdown

1. Introduction

In recent years, connected and autonomous vehicles (CAVs) have attracted growing attention for their potential to transform road transportation by improving safety, operational efficiency, and environmental performance. By integrating advanced sensing, control, and communication technologies and exchanging real-time information with other vehicles and the infrastructure, CAVs can coordinate their movements more effectively, leading to increased road capacity and optimized energy consumption [1–3]. At the same time, CAVs may enhance road safety by minimizing human errors, maintaining safer following distances, and responding more effectively to potential hazards [4, 5]. However, it is expected that, in the foreseeable future, CAVs and conventional human-driven vehicles (HDVs) will coexist in mixed traffic conditions [6, 7]. This mixed environment introduces additional complexity, as the effects of automated traffic depend not only on CAV performance but also on their interactions with conventional vehicles.

The potential of CAV could be relevant on highways, where relatively uniform traffic conditions and higher speeds amplify the benefits of coordinated vehicle behavior; particularly, CAV platooning has received significant attention [8]. Platooning refers to groups of vehicles traveling in a coordinated manner, maintaining short inter-vehicle distances and synchronized speeds enabled by vehicle-to-vehicle (V2V) communication. This coordinated behavior may increase road capacity, improve flow stability, and reduce fuel consumption due to lower aerodynamic drag [9, 10]. These features make platooning an effective strategy for enhancing the benefits associated with the gradual introduction of CAVs into highway systems. Beyond improving traffic flow under stable conditions, the potential of CAV platoons can be especially relevant when the highway network is subject to congestion. The highway system is often characterized by the presence of bottlenecks, that is, critical points in the network where traffic demand exceeds the available capacity, generating congestion, queues, delays, environmental impacts, and safety risks. These bottlenecks can be: (i) recurrent, such as those that form in on-ramp or off-ramp areas, where the interaction between entering flows and mainline traffic reduces overall capacity, or (ii) non-recurrent, associated with unexpected or temporary events such as accidents, vehicle breakdowns, or road works. In both cases, the occurrence of a bottleneck and the resulting reduction in effective capacity not only worsen local traffic conditions but can also trigger spillback along upstream segments, amplifying congestion. In these situations, CAV platoons might provide significant benefits in mitigating disturbances. In fact, by maintaining short and steady headways, adjusting speeds consistently, and reacting faster and more uniformly than human drivers, CAV platoons may help reduce disturbances, limit delays, and support a faster recovery of traffic flow, thereby improving the overall resilience of the highway system [11]. However, the actual potential of CAV platooning is not obvious: depending on factors such as platoon size and market penetration rate, they may either improve traffic performance or, in some cases, worsen local congestion at bottlenecks.

The literature has shown that CAVs can alleviate congestion both at recurrent bottlenecks and under non-recurrent disturbances. Most previous works have examined merging areas, where CAVs are generally found to improve capacity and flow efficiency [12]. However, the majority of studies analyze the behavior of individual CAVs rather than the dynamics of full platoons. Studies specifically

addressing platoons often concentrate on cooperative control strategies – such as gap opening, platoon splitting or coordinated merging – which assume that platooned vehicles actively adjust their configuration to facilitate ramp entries or respond to critical events [13, 14]. These approaches are useful for illustrating the maximum potential of platooning, but they rely on control capabilities that may not be available in the short to medium term, when CAV platoons are more likely to operate on the mainline without dedicated mechanisms for interacting with on-ramp traffic. Moreover, the literature is still limited in comparing platoon performance across different operational contexts. For example, a platoon configuration that proves effective at a recurrent bottleneck may perform very differently – and in some cases even worsen congestion – during a non-recurrent disturbance such as a vehicle breakdown. This context-dependence of platoon performance remains largely underexplored, despite being a key factor for assessing the feasibility of large-scale platoon deployment in real mixed-traffic conditions.

This chapter examines the effects of CAV platoons on highway traffic performance in the presence of bottlenecks under mixed traffic conditions. Two representative cases are considered:

1. A recurrent bottleneck, corresponding to a highway on-ramp merging area, where the interaction between entering vehicles and the mainline flow reduces capacity and generates congestion;

2. A non-recurrent bottleneck, generated by a vehicle breakdown, leads to a temporary capacity reduction and traffic disturbance.

For both scenarios, the analysis explores how market penetration rate (MPR) and platoon size affect traffic performance in the two bottleneck scenarios by assessing their effects in terms of capacity, travel times, and environmental impacts. The analysis relies on a microsimulation-based approach, which allows detailed modeling of vehicle interactions and the evaluation of different penetration levels and platoon configurations. The results provide a quantitative basis for evaluating the effects of CAV platoons and enable the identification of platoon configurations that are most effective for the different bottleneck scenarios, providing insight into how their performance evolves under varying disturbance conditions. This is particularly relevant in mixed traffic environments, as understanding how CAVs and HDVs interact at highway bottlenecks provides the basis for developing traffic management strategies that can fully exploit the benefits of platooning.

The chapter is structured as follows. Section 2 presents a review of the literature on platooning, with emphasis on bottleneck-related studies, while Sect. 3 outlines the methodological framework adopted in this study. Section 4 describes the simulation setup and reports the findings for the two case studies, and Sect. 5 discusses their implications. Finally, Sect. 6 summarizes the conclusions.

2. Literature review

A growing body of research has examined the potential of CAVs to improve the efficiency, safety, and stability of highway traffic flow. Studies consistently indicate that CAVs, thanks to real-time communication and coordinated

longitudinal control, can maintain more regular headways, react more smoothly to disturbances [15, 16], and reduce the formation and propagation of stop-and-go waves [17, 18]. These mechanisms are generally recognized as key enablers of both improved operational performance and enhanced safety in highway environments.

Within this context, vehicle platooning has attracted increased research interest, examining how groups of CAVs can travel cooperatively through communication and coordinated longitudinal control, enabling significantly shorter headways than those maintained by human drivers. The literature shows that platooning can significantly increase lane capacity [19] and improve flow stability [1, 20], while also enhancing safety [21]. Several studies on both truck and passenger-car platoons report higher throughput and lower emissions, the latter mainly resulting from lower aerodynamic drag and the mitigation of stop-and-go oscillations [22–24]. These advantages have been found to be particularly relevant in highway environments, where coordinated maneuvers and smoother trajectories can substantially enhance overall traffic performance [25, 26]. Although quantitative estimates vary across modeling approaches, the literature generally agrees that capacity gains become more substantial as cooperative automation increases [27, 28].

A growing number of modeling and simulation studies have also explored how CAV market penetration rates and platoon size influence mixed-traffic conditions [29]. Most work suggests that the benefits of CAVs emerge even at moderate penetration rates, although the magnitude of such benefits depends strongly on behavioral interactions with HDVs and on platoon configuration [30]. Behavioral heterogeneity between CAVs and HDVs is frequently identified as a central factor, especially in low-penetration scenarios where mixed-traffic instabilities may still occur [31, 32]. Using cellular automata models [33] demonstrates that fixed-length platoons can already enhance flow efficiency and reduce congestion [22]. This line of research is extended through a hybrid cellular automaton framework integrating both autonomous platoons and human-driven vehicles. Several simulation and analytical studies indicate that at low CAV penetration, very long platoons can even introduce additional disturbances if not properly managed, and improvements in capacity are limited. For instance, [8] reports that at 50% CAV penetration, platoons of around 20 vehicles increase capacity by only about 2% and tend to generate additional lane-changing interactions in predominantly human-driven traffic. Several studies indicate that moderate platoon sizes achieve higher capacity while keeping inter-vehicle dynamics stable [28, 34]. Beyond efficiency, several studies have investigated the safety and environmental implications of platooning. The main findings consistently point to fewer abrupt maneuvers, smoother speed adaptation, and potential reductions in collision risks [35], travel time [22], fuel consumption, and emissions [24].

In relation to freeway bottlenecks, most research has focused on on-ramp merging areas, where vehicles must negotiate right-of-way and where recurrent congestion typically arises. In these critical zones, CAV platooning has shown considerable potential to mitigate the capacity drop and delays usually associated with merges [36]. The literature on merging often centers on cooperative control strategies, such as adaptive gap policies or platoon reconfiguration, designed to facilitate smoother interactions with entering traffic [37]. Indeed, several cooperative merging algorithms have been proposed to improve lane-use efficiency during merging [38, 39]. For instance, [40] shows that employing cooperative merging control in on-ramp conditions enhances traffic flow stability and

throughput relative to conventional merging, and [14] proposes a platoon-split merging strategy for mixed traffic. Other works investigate cooperative lane-changing and trajectory-planning approaches, demonstrating that CAV coordination of lane and speed adjustments can increase merge capacity, smooth the flow, and reduce fuel consumption [41]. A second line of research quantifies the capacity gains achievable through platooning, generally considering CAVs operating on both the mainline and the on-ramp. The greatest benefits are consistently observed for the ramp flow: shorter inter-vehicle gaps reduce the effective length of merging vehicle strings, allowing a larger number of vehicles to clear the merge point within the same time interval [25]. A macroscopic model was developed showing that optimizing platoon length as a function of demand and CAV penetration can substantially increase the throughput of a freeway merge. However, it has been noted that, without adaptive gap management, tightly spaced platoons can restrict the gaps available to on-ramp vehicles, causing safety issues and degrading merge performance [42, 43]. It was observed that short intra-platoon gaps can form a "moving wall" that hinders merging, leading to late and risky lane changes, whereas slightly larger gaps increased merge success rates and reduced conflicts.

Beyond everyday bottlenecks, some studies have also examined the effects of non-recurring events such as accidents or vehicle breakdowns. Existing evidence suggests that CAV platooning can improve traffic performance during incidents by enabling faster recovery and reducing the severity of congestion [44, 45]. These benefits become more pronounced as penetration increases, with several studies reporting faster recovery and reduced secondary disturbances after an incident [46–48]. Reports indicate that under accident-induced bottlenecks, CACC-enabled platoons maintain higher throughput than human-driven traffic due to shorter safe gaps, with upstream congestion progressively diminishing as CAV penetration increases [49]. Researchers investigate platoon breakdowns and find that the sudden disablement of a platoon leader can temporarily reduce capacity, although higher CAV penetration considerably mitigates this effect. Their findings also show that very long platoons exacerbate delay and safety risks when forced to dissolve near an incident, leading the authors to recommend limiting operational platoon sizes to around four vehicles. Related research in lane-closure and work-zone contexts offers similar indications, reinforcing the idea that cooperative longitudinal control is particularly valuable under non-recurrent, capacity-reducing disturbances [50].

Overall, the literature strongly supports the capacity and safety advantages of CAV platooning under ideal or near-ideal conditions, such as high CAV adoption, tight coordination, and homogeneous traffic. In mixed traffic, however, existing findings also show that the magnitude of these benefits depends critically on factors such as market penetration and platoon size, indicating that platoon performance is highly sensitive to the operating conditions. Despite this, important gaps remain regarding how different platoon configurations perform across distinct bottleneck types. Most studies analyze platooning either in recurrent merging scenarios or in non-recurrent disruptions, but they rarely assess whether a given configuration performs consistently across both conditions. Consequently, there is limited evidence on whether configurations that prove beneficial in one type of bottleneck may become less effective when the congestion mechanism changes. Building on this gap, the present study examines how the effectiveness of CAV platoons varies across two fundamentally different types of freeway bottlenecks within a common modeling framework. In detail, this chapter investigates whether operational

characteristics such as market penetration or platoon size can lead to different outcomes depending on whether congestion originates from routine merging interactions or from an unexpected incident, thereby contributing to a clearer understanding of how platoons behave under heterogeneous traffic conditions and which configurations are more appropriate for each context.

3. Methodology

To address the research objectives, this study combines established microscopic traffic models with simulation experiments to analyses HDV and CAV behavior under bottleneck conditions. For longitudinal movement, different models are applied depending on the vehicle type. The car-following behavior of HDVs is simulated using the intelligent driver model (IDM) [51], which captures essential aspects such as acceleration, deceleration, and the management of safe distances typical of human drivers. For CAVs, the cooperative adaptive cruise control (CACC) and adaptive cruise control (ACC) models [52] are used to reflect their cooperative behavior and adaptive responses to surrounding traffic. For both CAVs and HDVs, lane-changing behavior is modeled using the LC2013 model [53], which effectively represents how vehicles decide to change lanes and execute these maneuvers in mixed traffic conditions. To model merging operations, it is assumed that shorter lane-changing gaps are accepted [54]. A highway segment is recreated in the simulation, incorporating realistic geometric and traffic flow characteristics. Two distinct scenarios are modeled: a non-recurrent bottleneck caused by a vehicle breakdown and a recurrent bottleneck generated by an on-ramp merging area. To assess the impact of these conditions, several key performance indicators are considered, focusing on traffic flow efficiency and environmental impacts. The overall architecture is depicted in **Figure 1**.

3.1 HDVs longitudinal movement model

HDVs' longitudinal navigation is modeled using the intelligent driver model (IDM), a standard car-following model widely adopted for representing human

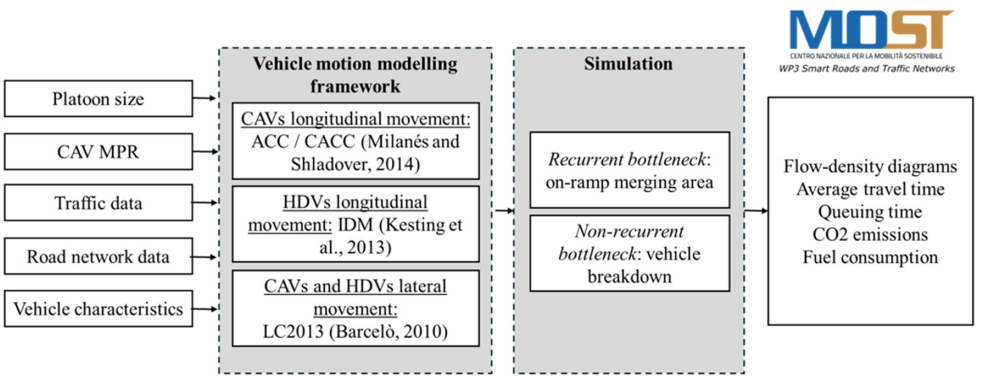


Figure 1.
Overview of the methodology.

driving behavior in microscopic simulations. IDM is used here because it captures typical acceleration, deceleration, and gap-keeping tendencies of human drivers, providing a reliable baseline for mixed-traffic conditions. Furthermore, it has been proven to be particularly suitable for microscopic simulations involving mixed traffic flows [55]. The IDM defines a vehicle's acceleration based on the current speed, the speed difference with the leading vehicle, and the space gap between them. The acceleration of a vehicle is given by:

$$a_{IDM} = a_m \left[1 - \left(\frac{v}{v_0} \right)^{\delta} - \left(\frac{s^*(v, \Delta v)}{s} \right)^2 \right] \tag{1}$$

$$s^*(v, \Delta v) = s_0 + \max\left(0, vT + \frac{v\Delta v}{2\sqrt{a_m b}} \right) \tag{2}$$

where a_m is the maximum HDV acceleration, v is the speed of the following vehicle, v_0 is the desired speed, s is the space gap between the leading and following vehicles, Δv is the speed difference between the leading and following vehicles, δ is a parameter characterizing how the acceleration decreases with the speed, $s^*(v, \Delta v)$ is the minimum desired space gap, s_0 is the minimum inter-vehicular distance at standstill, T is the safe time headway and b is the desired comfortable deceleration.

3.2 CAVs longitudinal movement model

CAVs are modeled as operating in platoons, each comprising a group of n vehicles. Within each platoon, the first vehicle is designated as the leader, while the others act as followers. This platoon-based structure reflects the coordinated behavior enabled by vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication technologies. The motion dynamics of CAV platoons are modeled by applying distinct control strategies to the leading and following vehicles. The longitudinal motion of the platoon leader is governed by an ACC model, which regulates the vehicle's behavior based on on-board perception systems (e.g., radar, LiDAR) to maintain a safe headway relative to the preceding traffic. In contrast, follower vehicles in the platoon are modeled using a CACC strategy, which integrates local sensor data with information received through V2V communication. The CACC framework enables the followers to access not only their immediate leader's state but also information from other platoon members, allowing for reduced time headways and improved responsiveness of the platoon.

For modeling the ACC and CACC behavior, a simplified version of the cooperative controller implemented in commercial CACC-equipped vehicles is employed, following the formulation proposed by [52]. The longitudinal control of the platoon leader under the ACC model is represented by a car-following scheme aiming to maintain a desired time headway t_{hw} with respect to the preceding vehicle. The acceleration a_i commanded by the ACC controller is given by:

$$a_i = k_1(x_{i-1} - x_i - t_{hw}v_i) + k_2(v_{i-1} - v_i) = k_1 e_i + k_2(v_{i-1} - v_i) \tag{3}$$

Where x_i, v_i and a_i are the current position, speed and acceleration of the i–th CAV vehicle; x_{i-1} and v_{i-1} are the current position and speed of the preceding vehicle; e_i is the gap error of the i–th vehicle, representing the difference between the desired gap and the actual gap between the vehicle and its preceding one. k_1 and k_2

are the gain coefficients on both the spacing and speed differences, respectively, acting as tuning parameters that determine the ACC controller's responsiveness to variations in traffic conditions.

For follower vehicles operating under the CACC model, a cooperative control law is applied and the desired speed v_i for a follower vehicle is computed based on information received from the platoon leader (or other upstream vehicles), according to [52]:

$$v_i = v_{i,\,prev} + k_p e_i + k_d \dot{e}_i \tag{4}$$

Where $v_{i,\,prev}$ is the speed of the i–th follower vehicle at previous time step; k_p and k_d are control gains associated to the time gap error.

3.3 CAVs and HDVs lateral movement model

For both HDVs and CAVs, lateral vehicle behavior is modeled using the LC2013 lane-changing framework [56]. The model distinguishes among three types of lane change motivations: strategic, cooperative and tactical. A strategic lane change is initiated to avoid reaching a dead-end or an unusable lane and is classified as a mandatory maneuver. A cooperative lane change occurs when a vehicle adjusts its speed or position to facilitate the lane change of another vehicle. A tactical lane change is performed voluntarily to optimize travel conditions, such as improving speed, following traffic rules (e.g., returning to the right lane after overtaking) or maintaining lane discipline. Once a lane change is deemed necessary or desirable, the vehicle evaluates the feasibility of the maneuver through a gap acceptance process, where it assesses the available gaps in the target lane relative to its own speed and position. If a suitable gap is identified, the vehicle may initiate the maneuver; otherwise, it may postpone the lane change and adapt its behavior to create favorable conditions. To model bottleneck conditions, it is assumed that vehicles temporarily accept shorter lane-changing gaps than under normal conditions, reflecting the increased urgency to complete the maneuver before the end of the lane [54]. Specifically, a reduction of approximately 20% in the acceptable gap size is considered, based on empirical observations [57]. Following the lane change, vehicles gradually restore their headways to typical values within a short recovery period, consistent with the relaxation phenomenon described by [58].

3.4 CAV platoon behavior at bottlenecks

In the presence of a bottleneck, whether recurrent or non-recurrent, the behavior of CAVs within platoons is modified based on the approach developed by [49]. A CAV detects a bottleneck when the speed of its preceding vehicle remains at zero for more than 2 seconds and the distance to that vehicle is less than 60 m. The 60 m threshold corresponds to the typical stopping distance at highway speeds and is consistent with values reported in the literature [59]. When these conditions occur, it is assumed that the CAV "recognizes" that it has entered the influence area of a bottleneck and triggers a dedicated control logic.

The platoon that includes the detecting CAV is dissolved by modifying the control logic described in Sect. 3.2, specifically through the activation and deactivation of ACC and CACC modes, consistent with the approach proposed in [60]. For all follower CAVs in the platoon, the CACC mode is deactivated, and their

control is switched to ACC. The platoon leader already operates under ACC and, therefore, remains in ACC mode. At this point, all CAVs behave as independent vehicles rather than as members of a coordinated platoon. The choice to model platoon dissolution near bottlenecks is driven by the need to ensure sufficient gaps to perform lane changes. In fact, if the platoon is kept intact, coordinated maneuvers would require gaps that could accommodate the entire formation. Such gaps grow rapidly with platoon size and may not be available in congested conditions, potentially leaving the platoon stuck in the tail for long periods. Platoon dissolution avoids this problem by allowing each CAV to act independently and use smaller, individually acceptable gaps, thus improving maneuverability. More advanced cooperative lane change or platoon-splitting strategies are not considered, as they require coordinated interactions that cannot be guaranteed in mixed traffic, especially in cases of low CAV penetration. For this reason, platoon dissolution has been adopted here as the most effective default behavior in bottleneck regions.

In ACC mode, each CAV adapts its speed to the vehicle ahead and, at the same time, monitors the neighboring lane. If the lane-changing criteria (safety gaps and incentive conditions) are satisfied, the CAV initiates a lane change to bypass the obstacle or the queue forming upstream of the bottleneck. The flowchart of the proposed platoon control algorithm in the presence of bottlenecks is shown in **Figure 2**. After passing the bottleneck and once local traffic conditions return to normal (i.e., no stopped vehicles ahead within the detection distance and speeds compatible with free-flow or near free-flow), CAVs return to their lane. If other CAVs are available in the same lane and within the required distance, platoons are re-formed by reactivating CACC mode for follower vehicles, following the logic described in Sect. 3.2. In practice, platoons dynamically dissolve in the vicinity of bottlenecks and re-establish once the congested area has been cleared. HDVs are modeled using the IDM car-following model and perform lane changes to avoid the stopped vehicle according to the LC2013 lane-changing model described earlier.

3.5 Traffic performance indicators

The system's performance is assessed through a set of indicators, each addressing different dimensions, including operational efficiency and environmental impacts.

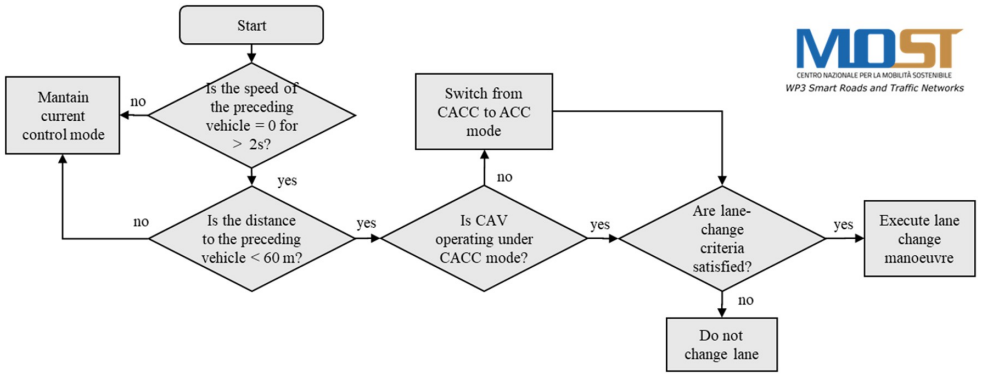


Figure 2.
Control logic in the presence of a bottleneck.

Specifically, the selected metrics include traffic capacity, vehicle travel time, CO_2 emissions, and queuing time. Traffic capacity is derived by calibrating the flow-density (q–k) relationship using experimental data, employing a triangular flow diagram [61]:

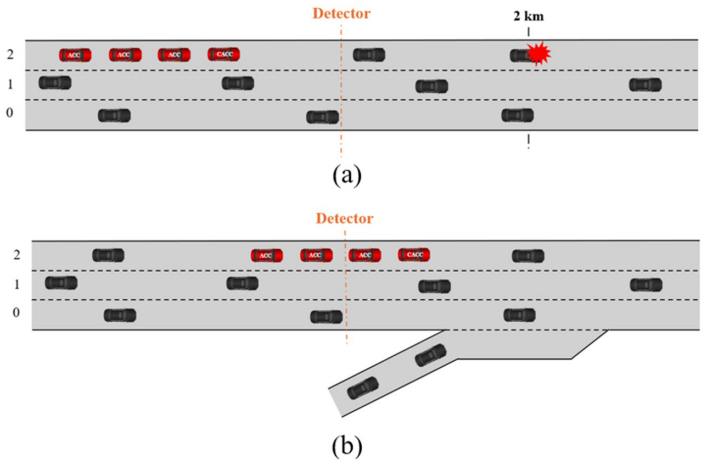
$$q(k) = \begin{cases} v_f k & for\, k < k_c \\ w(k_j - k) & for\, k > k_c \end{cases} \tag{5}$$

where q is the traffic flow; k is traffic density; v_f is the free-flow speed; w is the shockwave speed; k_j is the jam density; k_c is the density at capacity (critical density). The maximum flow q_{max} (capacity) occurs at k_c and is equal to $v_f k_c$. Average travel time is employed as a performance indicator of the overall efficiency of the network and it is computed by averaging the individual travel times of all vehicles in the network. Queuing time is used to quantify the delay experienced by vehicles during congested conditions. It is computed as the total time during which a vehicle speed falls below 0.1 m/s, which corresponds to stopped or near-stop motion. Two complementary indicators are considered: the average queuing time per vehicle, which reflects the typical delay experienced by individual users, and the total queuing time per 5-minute interval, used to capture the temporal evolution of congestion formation and dissipation along the network. Environmental impacts are evaluated in terms of CO_2 emissions (mg/vehicle). Emissions are estimated using the HBEFA4 emission model, which computes pollutant production for each vehicle based on its instantaneous kinematic state (speed and acceleration). For each scenario, the total CO_2 emitted along the highway segment is aggregated across all vehicles and the corresponding average emission per vehicle is used to compare environmental performance across different market penetration rates and platoon sizes. These indicators are calculated across various scenarios under varying levels of MPR and platoon size and compared to evaluate the impacts of CAV platooning on traffic efficiency and safety.

4. Simulation experiments

4.1 Simulation setup

The simulation is carried out using the Python-SUMO platform on a three-lane highway segment. The simulated section is 3 km long, with a lane width of 3.75 m and a speed limit of 130 km/h. Two scenarios are implemented to analyze both a non-recurrent bottleneck (vehicle breakdown) and a recurrent bottleneck (on-ramp merging area). The first scenario (**Figure 3a**) represents a freeway segment without ramps, reproducing undisturbed flow upstream of a non-recurrent event. The breakdown is modeled by stopping an HDV in the left lane at 2 km. The stopped vehicle remains in place for 15 minutes, during which approaching vehicles slow down and perform lane changes to bypass the lane blockage. CAV behavior follows the obstacle-avoidance logic described in Sect. 3.4: once the bottleneck is detected, platoons dissolve, follower vehicles switch from CACC to ACC mode, and all CAVs operate as independent units while executing lane changes based on safety and incentive rules. After removal of the obstacle, the resulting queue gradually dissipates until normal operating conditions are restored. The second scenario (**Figure 3b**) represents an on-ramp merging area. The acceleration lane is 200 m



CENTRO NAZIONALE PER LA MOBILITÀ SOSTENIBILE
WP3 Smart Roads and Traffic Networks

Figure 3.
Simulated highway segment and bottleneck configurations: (a) Non-recurrent incident scenario; (b) Recurrent on-ramp merging scenario.

long, and entering vehicles, composed exclusively of HDVs, merge into the mainline. The on-ramp flow is fixed at 600 veh/h. In both scenarios, the mainline flow consists of mixed traffic, with the proportion of CAVs determined by the market penetration rate; CAVs travel in platoons and may use all lanes.

Parameter values for car-following and lane-changing models follow established values in the literature [52, 62] and are summarized in **Table 1**. A set of experiments is conducted to evaluate how MPR and platoon size affect traffic performance. CAV market penetration is varied across 0%, 20%, and 40%, representing plausible medium-term adoption levels. For each penetration level, platoons of 2, 4, 6, and 8 vehicles are simulated. Total traffic demand is varied at several levels of congestion conditions, across 1,000, 1,350, 1,650, and 2,000 veh/h/lane, the latter representing highly congested conditions. Each simulation runs for 3,600 s, preceded by a 600 s warm-up period excluded from the analysis. To account for stochasticity, three random seeds are used for each configuration. Performance is evaluated in terms of flow capacity, operational efficiency, and environmental impacts, using the indicators described in Sect. 3.5.

Parameter	Value	Parameter	Value
k_j (maximum density)	160 veh/km/lane	Platoon inter-vehicle distance	5 m
δ (HDV free acceleration exponent)	4	t_{hw} (CACC desired time gap)	1.1 s
b (desired deceleration)	2 m/s^2	t_{hw} (ACC desired time gap)	0.6 s
a_m (max. acceleration)	1 m/s^2	k_1 (gains on positioning errors)	0.23 s^2
v_0 (desired speed)	33 m/s	k_2 (gains on speed errors)	0.07 s^2
T (safe time headway)	1.6 s	k_p (gains on time-gap)	0.45
s_0 (min. gap at standstill)	1 m	k_d (gains on time-gap)	0.25

Table 1.
Parameters used in the simulation.

4.2 Results

Figure 4 shows the results for the vehicle breakdown scenario: **Figure 4a-d** describe the effects of different market penetration rates (*MPR* = 0.20 and 0.40) and platoon sizes (n = 0, 2, 4, 6, 8) under high-demand conditions (2,000 veh/h/lane); **Figure 4e** presents the flow-density relationships observed upstream of the incident. Traffic data are collected at a simulated detector located 50 m upstream of the breakdown (see **Figure 3a**) and averaged across the three lanes for each MPR. For every condition, a triangular fundamental diagram is fitted to the aggregated data to estimate the free-flow speed (v_f), critical density (k_c), and maximum flow (q_{max}); calibration uses the Nelder–Mead optimization method [63], with the jam density fixed at 160 veh/km/lane.

Overall, the introduction of CAV platoons markedly improves traffic performance compared with the all-HDV baseline. Travel times (**Figure 4a**) decrease substantially even at moderate penetration levels, and their variability is significantly reduced. At *MPR* = 20%, travel times already show a notable reduction: for n = 2, the median decreases by roughly 25–30%, and for n = 4, by about 20–25%

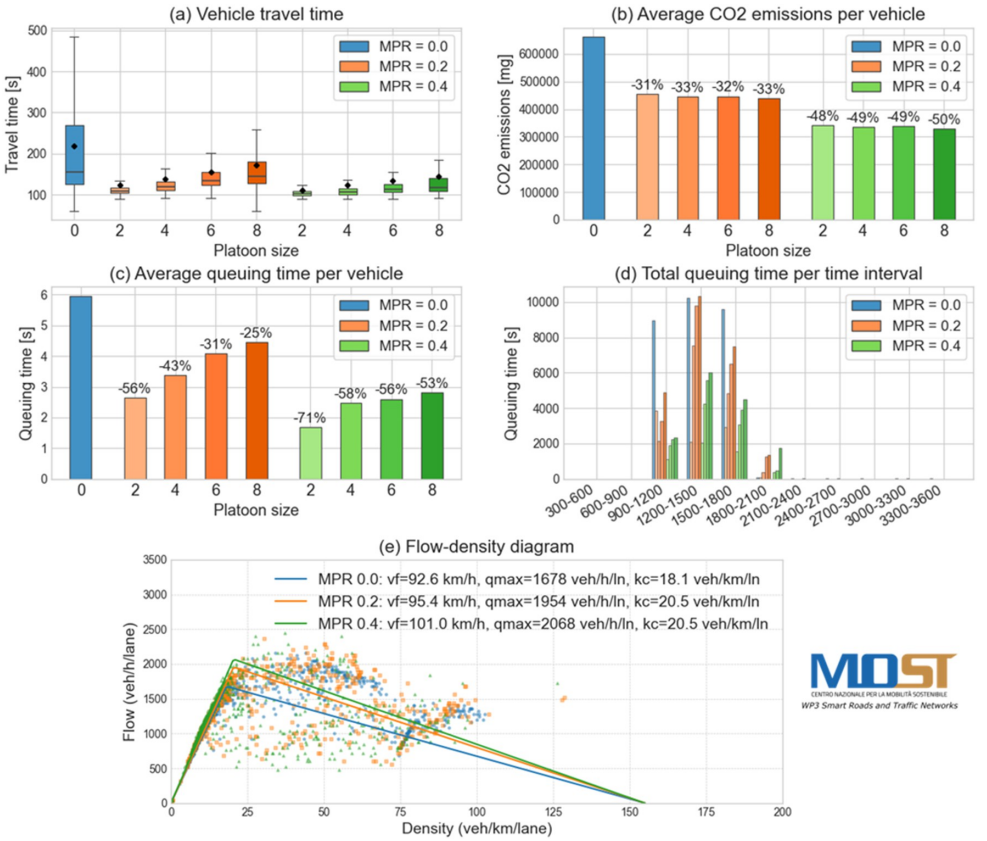


Figure 4.
Indicators under different market penetration rates (MPR) and platoon sizes for the breakdown scenario: (a) Vehicle travel-time; (b) Average CO_2 emissions per vehicle; (c) Average queuing time per vehicle; (d) Total queuing time per 5-minute interval; (e) Flow-density diagrams.

relative to the HDV case. The improvement becomes even more pronounced at *MPR* = 40%, where reductions of approximately 40–45% (n = 2) and 35–40% (n = 4) are observed, together with a marked contraction of the interquartile range. However, increasing platoon size does not continue to improve performance. For both penetration levels, larger platoons (n = 6 and n = 8) lead to increased travel times relative to smaller formations. The flow-density diagram in **Figure 4e** further quantifies the positive effects of CAV MPR on the macroscopic traffic characteristics. As MPR increases, the scatter of flow-density observations is reduced, and the estimated maximum flow shows a moderate but consistent improvement relative to the all-HDV case, indicating that CAVs can enhance overall throughput even when HDVs remain the majority of the fleet. In particular, maximum flow increases by approximately 16% at *MPR* = 20% and by about 23% at *MPR* = 40% compared with the HDV baseline. Although the gain between 20% and 40% penetration is moderate, the upward shift in both critical density and maximum flow indicates that CAVs improve the ability of the traffic stream to sustain higher densities before the onset of congestion. Queue-related indicators provide additional insight into the system's response to the breakdown (**Figure 4c, d**). Average queuing times decrease substantially with the introduction of CAVs. At *MPR* = 20%, reductions of approximately 56% (n = 2) and 43% (n = 4) are observed relative to the HDV case, while at *MPR* = 40%, the decrease reaches about 72% and 55% for the same platoon sizes. These improvements are also reflected in the temporal distribution of delays across the simulation horizon, which becomes smoother in the presence of CAVs: in the all-HDV scenario, queuing concentrates in sharp peaks associated with rapid queue formation, whereas with CAVs, the peaks are smaller and more evenly distributed. Therefore, queues build up more gradually and dissipate more quickly once the obstacle is removed. Emissions-related indicators show a similar pattern. Average CO_2 emissions per vehicle (**Figure 4b**) decrease markedly with the introduction of CAVs: reductions of about 31–33% are observed at *MPR* = 20% and approximately 45–50% at *MPR* = 40%. As with queuing times, the largest benefits occur for smaller platoon sizes (n = 2–4), while larger formations offer more limited improvements. **Table 2** summarizes the percentage improvements in average travel time, CO_2 emissions, and queuing time for the breakdown scenario.

The results for the merging scenario (**Figure 5**) reveal patterns that are broadly consistent with those observed in the incident case, but with differences in both

Platoon size		**n = 2**	**n = 4**	**n = 6**	**n = 8**
Average travel time [Δ%]	MPR = 0.2	−43.98	−37.15	−29.38	−21.29
	MPR = 0.4	−49.15	−43.73	−39.01	−33.42
Average CO_2 emissions [Δ%]	MPR = 0.2	−31.08	−32.86	−32.47	−33.49
	MPR = 0.4	−48.42	−49.09	−48.63	−50.24
Average queuing time [Δ%]	MPR = 0.2	−55.66	−43.26	−31.32	−25.36
	MPR = 0.4	−71.49	−58.24	−56.24	−52.51

Table 2.
Percentage reductions in travel time, CO_2 emissions, and queuing time relative to the all-HDV case for the breakdown scenario.

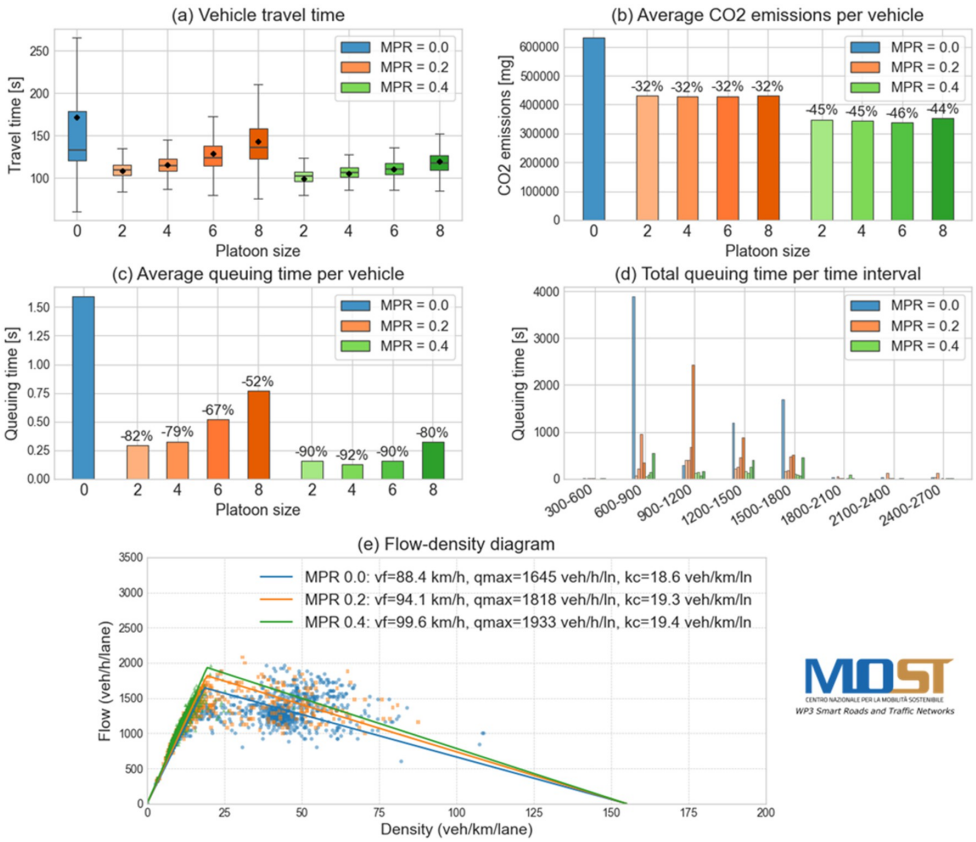


Figure 5.
Indicators under different market penetration rates (MPR) and platoon sizes for the merging scenario: (a) Vehicle travel-time; (b) Average CO_2 emissions per vehicle; (c) Average queuing time per vehicle; (d) Total queuing time per 5-minute interval; (e) Flow-density diagrams.

magnitude and pattern. As in the breakdown scenario, the introduction of CAVs reduces travel times (**Figure 5a**), queuing (**Figure 5c, d**) and emissions (**Figure 5b**) relative to the all-HDV baseline, and these improvements become more pronounced as MPR increases. However, in this case, reductions in travel and queuing times are smaller than those observed during the incident. For example, at *MPR* = 20%, median travel times decrease by roughly 10–15% for small platoons (n = 2–4), and at *MPR* = 40%, the reduction rises to approximately 20–25%. Platoon-size effects also differ. While small platoons (n = 2–4) again provide the best performance, the penalty associated with larger formations is less severe than in the breakdown scenario. For instance, moving from n = 4 to n = 8 at *MPR* = 40% increases median travel time by only 5–8%, whereas the same increase in platoon size during the incident caused travel-time penalties exceeding 15–20%.

Macroscopic flow patterns confirm these trends. The flow-density diagrams in **Figure 5e** – derived from data collected at the detector positioned 50 m upstream of the on-ramp (see **Figure 3b**) – show a moderate upward shift in both critical density and capacity with increasing MPR, similar in direction to the incident scenario but smaller in magnitude. Maximum flow increases from the HDV baseline to

Platoon size		***n*** **= 2**	***n*** **= 4**	***n*** **= 6**	***n*** **= 8**
Average travel time [Δ%]	MPR = 0.2	−36.78	−32.67	−25.04	−16.91
	MPR = 0.4	−42.30	−38.59	−35.62	−30.53
Average CO_2 emissions [Δ%]	MPR = 0.2	−31.73	−32.34	−31.98	−31.67
	MPR = 0.4	−44.76	−45.42	−46.46	−43.89
Average queuing time [Δ%]	MPR = 0.2	−81.58	−79.50	−67.43	−51.69
	MPR = 0.4	−90.22	−92.20	−89.99	−79.85

Table 3.
Percentage reductions in travel time, CO_2 emissions, and queuing time relative to the all-HDV case for the merging scenario.

approximately +10% at *MPR* = 20% and +17% at *MPR* = 40%. CO_2 emissions follow the same qualitative pattern as in the incident scenario, decreasing by roughly 30–33% at *MPR* = 20% and 45–47% at *MPR* = 40% for *n* = 2–4, but again with more modest gains relative to the incident case. **Table 3** provides percentage variations in average travel time, queuing time, and CO_2 emissions for the on-ramp merging scenario.

5. Discussion

The results obtained from the two bottleneck scenarios provide a comprehensive view of how CAV platoons influence traffic performance under bottleneck conditions. Overall, during an incident, CAV platoons act as "shock absorbers," mitigating the abrupt disturbance generated by the lane blockage. The coordinated behavior within platoons limits sharp decelerations, reduces lane-change pressure upstream, and accelerates the transition back to uncongested flow. The benefits of platooning materialize across a wide range of performance indicators (capacity, travel time, queuing time, emissions), but the extent and nature of these benefits depend strongly on the type of disturbance affecting the traffic stream. This context-dependence is critical for understanding the real-world applicability of CAV platoons, especially in mixed traffic, where interactions between automated and human-driven vehicles introduce additional variability.

In the incident scenario, where an unexpected lane blockage abruptly reduces available capacity, CAV platoons generate significant improvements. The substantial reductions in travel time and queuing time, together with lower emissions and fuel consumption, show that platoons help normalize traffic behavior during both the formation and the dissipation of the queue. The flow-density relationships reinforce this interpretation: compared with fully human-driven traffic, even moderate CAV penetration produces denser and more compact flow regimes that can sustain higher densities before congestion emerges. These improvements stem from the coordinated deceleration and acceleration inherent in platooned CAVs, which limit the propagation of abrupt speed changes and maintain smoother trajectories upstream of the obstruction. In this scenario, therefore, platooning acts primarily as a stabilizing mechanism, reducing the severity of the disturbance and enabling a more efficient recovery of the traffic stream.

In contrast, in the merging scenario, benefits are still present but less pronounced. This is consistent with the fundamentally different nature of the bottleneck: whereas an incident induces a sudden and sharply localized reduction in capacity, merging turbulence arises from continuous interactions between entering vehicles and the mainline flow. Since the CAV platoons in this study do not perform explicit cooperative maneuvers, such as gap-opening or platoon splitting to accommodate merging traffic, the residual conflicts at the merge persist even at higher penetration levels. The improvements observed – lower travel times, reduced emissions and more compact flow-density patterns – result primarily from the smoother longitudinal behavior of CAVs on the mainline rather than from an active facilitation of merging maneuvers. As a result, the gains are more incremental and do not eliminate the inherent competition for space at the merge.

The analysis also highlights the central role of the market penetration rate. Across both scenarios, performance improves consistently as CAV penetration increases from 0% to 40%. This is evident in all key indicators: travel time, fuel consumption, emissions, and delay. These improvements at moderate penetration levels confirm that the benefits of platooning are accessible even in the early phases of deployment, when fleets are far from full automation. Importantly, however, the magnitude of the benefits differs between scenarios, confirming that the penetration rate interacts with the specific congestion mechanism at play.

Perhaps more importantly, the study reveals that platoon size has a non-trivial and context-dependent impact on performance. Contrary to earlier findings suggesting that medium-sized platoons (e.g., four vehicles) offer an optimal balance between capacity and stability, our results show that when platoons occupy all lanes, larger platoons tend to hinder lane-changing flexibility. This is particularly evident in both scenarios: long platoons act as moving barriers, reducing the opportunities for human-driven vehicles to execute evasive or merging maneuvers. In the incident scenario, this manifests as delayed lane changes upstream of the blockage, while in the merging scenario, it exacerbates competition for gaps at the merge. In both cases, smaller platoons – typically two vehicles – lead to better performance. This finding underscores the importance of considering lane distribution when determining optimal platoon configurations: what is optimal when platoons are confined to one lane may be suboptimal when they are distributed across all lanes. It is worth noting, however, that our findings on platoon size are linked to the demand conditions considered in this study. The simulations focus on traffic levels close to congestion, a regime in which density is high and acceptable gaps tend to be limited. Under these circumstances, it is plausible that long platoons reduce maneuverability and therefore perform worse. This mechanism may not operate in the same way under different demand levels: under low-demand conditions, larger gaps may be available, which could reduce the disadvantages associated with longer formations or even make them preferable in some situations. These considerations suggest that the advantage of small platoons observed here refers to highly congested conditions.

Together, these insights highlight the complexity of deploying CAV platoons in real-world mixed traffic. The performance of a given platoon configuration cannot be generalized across bottleneck types or roadway contexts. Instead, effective deployment strategies will likely require adaptive or context-specific settings – adjusting platoon size, gap policy, and possibly even lane allocation according to the nature of the bottleneck and prevailing traffic conditions. In other words, platooning strategies may need to adapt dynamically to the operational environment and to the

type of bottleneck encountered. This observation has direct implications for future CAV control algorithms and traffic management policies, suggesting that "one-size-fits-all" platooning strategies may be insufficient to deliver consistent benefits across the highway network.

6. Conclusions

This study examined the impact of CAV platoons on highway traffic performance under mixed-traffic conditions, focusing on two representative bottlenecks: an incident-induced lane blockage and an on-ramp merging area. By evaluating identical platoon configurations across these two distinct operational environments, the analysis provides insights into the conditions under which CAV platooning yields measurable performance gains in mixed-traffic scenarios.

The findings show that CAV platoons can provide substantial benefits, leading to reductions in travel time, queueing times, and environmental emissions. However, the magnitude of these benefits varies with the nature of the bottleneck and therefore depends on the operational context. During an incident, platoons help absorb the sudden disturbance caused by the lane blockage: they reduce abrupt braking, limit the propagation of shockwaves, and allow traffic to recover more quickly. In contrast, in the merging scenario, the improvements are smaller because the bottleneck is created by continuous interactions between mainline and ramp vehicles, and platoons can only smooth these interactions rather than eliminate them.

A central result of the analysis is that the "optimal" platoon size is not a fixed property of the system but varies with the type of bottleneck. While prior studies often assume an optimal platoon size – typically around four vehicles – our results demonstrate that this assumption does not generalize to multi-lane, mixed-traffic environments. When platoons operate across all lanes, larger groups can restrict lane-changing maneuvers, particularly in zones where such maneuvers intensify (as in both incident avoidance and merging). In these conditions, smaller platoons consistently perform better. This highlights that the effectiveness of a given platoon size is inherently context-dependent, shaped by the interplay between platoon structure, lane-changing needs and the disturbance driving the congestion. Overall, the findings suggest that effective real-world deployment of CAV platoons will likely require adaptive and dynamic strategies – allowing platoon size, headways, or lane-use patterns to change according to the type of bottleneck encountered and the prevailing traffic conditions. Such context-aware approaches could help ensure that platooning delivers the expected improvements in efficiency, reliability, and environmental performance.

Although there are some encouraging results, this study has some limitations. First, no cooperative merging or lane-changing mechanisms were implemented for CAVs: vehicles do not generate gaps, coordinate trajectories, or perform platoon-splitting operations but rely on standard gap-acceptance rules. Second, platoon lane allocation is fully flexible, with no dedicated lanes or priority policies, whereas some studies advocate lane restrictions for platoons. Third, the analysis relies on ACC/CACC longitudinal controllers; more advanced approaches, such as RL– or MPC-based cooperative control, increasingly discussed in recent literature, are not considered. These assumptions should be taken into account when interpreting the

results and considered in future extensions of this work. Moreover, in this study, platoons are always dissolved near bottlenecks, which is suitable for high-demand levels, but future research should verify whether this strategy is appropriate in all demand conditions. The advantage of dissolution may, in fact, depend on travel demand: while it appears beneficial under congestion, in low-demand conditions, larger gaps may be available, and keeping the platoon intact could be more effective. This aspect should be explored in future work.

Acknowledgments

This study was carried out within the MOST – Sustainable Mobility National Research Centre and received funding from the European Union Next-GenerationEU (PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR) – MISSIONE 4 COMPONENTE 2, INVESTIMENTO 1.4 – D.D. 1033 17/06/2022, CN00000023). This manuscript reflects only the authors' views and opinions, neither the European Union nor the European Commission can be considered responsible for them.

Author details

Caterina Malandri[1], Luca Mantecchini[1], Maria Nadia Postorino[1*] and Xuelian Wu[2]

1 Department of Civil, Chemical, Environmental, and Materials Engineering (DICAM), University of Bologna, Bologna, Italy

2 School of Highway, Chang'an University, Xi'an, China

*Address all correspondence to: marianadia.postorino@unibo.it

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] Shladover SE. Connected and automated vehicle systems: Introduction and overview. Journal of Intelligent Transportation Systems. 2018;**22**:190–200

[2] Yu H, Jiang R, He Z, et al. Automated vehicle-involved traffic flow studies: A survey of assumptions, models, speculations, and perspectives. Transportation Research Part C: Emerging Technologies. 2021;**127**:103101

[3] Song H, Zhao F, Zhu G, et al. Impacts of connected and autonomous vehicles with level 2 automation on traffic efficiency and energy consumption. J Adv Transp 2023; 2023: 6348778

[4] Ngoduy D, Keyvan-Ekbatani M, Treiber M. Special issue on connected and automated traffic systems. Transportation Science. 2021;**17**:1–4

[5] Dong J, Wang J, Luo D. Impact of connected and autonomous vehicles on traffic safety of mixed traffic flow: From the perspective of connectivity and spatial distribution. Transportation Safety and Environment. 2022;**4**: tdac021

[6] Guo J, Cheng S, Liu Y. Merging and diverging impact on mixed traffic of regular and autonomous vehicles. IEEE Transactions on Intelligent Transportation Systems. 2021; **22**:1639–1649

[7] Ma L, Qu S, Ren J, et al. Mixed traffic flow of human-driven vehicles and connected autonomous vehicles: String stability and fundamental diagram. Mathematical Biosciences and Engineering. 2022;**20**:2280–2295

[8] Martínez-Díaz M, Al-Haddad C, Soriguera F, et al. Impacts of platooning of connected automated vehicles on highways. IEEE Transactions on Intelligent Transportation Systems. 2024;**25**:6366–6396

[9] Liang K-Y, Mårtensson J, Johansson KH. Heavy-duty vehicle platoon formation for fuel efficiency. IEEE Transactions on Intelligent Transportation Systems. 2016;**17**: 1051–1061

[10] Bhoopalam AK, Agatz N, Zuidwijk R. Planning of truck platoons: A literature review and directions for future research. Transportation Research Part B: Methodological. 2018;**107**:212–228

[11] Calvert SC, Schakel WJ, van Arem B. Evaluation and modelling of the traffic flow effects of truck platooning. Transportation Research Part C: Emerging Technologies. 2019;**105**:1–22

[12] Chen N, van Arem B, Alkim T, et al. A hierarchical model-based optimization control approach for cooperative merging by connected automated vehicles. IEEE Transactions on Intelligent Transportation Systems. 2021;**22**:7712–7725

[13] Li Q, Chen Z, Li X. A review of connected and automated vehicle platoon merging and splitting operations. IEEE Transactions on Intelligent Transportation Systems. 2022;**23**:22790–22806

[14] Gao H, Cen Y, Liu B, et al. A collaborative merging method for connected and automated vehicle platoons in a freeway merging area with considerations for safety and efficiency. Sensors. 2023; **23**:4401

[15] Talebpour A, Mahmassani HS. Influence of connected and autonomous vehicles on traffic flow stability and throughput. Transportation Research Part C: Emerging Technologies. 2016;**71**:143–163

[16] Zhu J, Wang L, Tasic I, Qu X, et al. Improving freeway merging efficiency via flow-level coordination of connected and autonomous vehicles. IEEE Transactions on Intelligent Transportation Systems. 2024;**25**: 6703–6715

[17] Zheng F, Liu C, Liu X, et al. Analyzing the impact of automated vehicles on uncertainty and stability of the mixed traffic flow. Transportation Research Part C: Emerging Technologies. 2020;**112**:203–219

[18] Hyun K, SK M, Jeong K, et al. Understanding the effects of vehicle platoons on crash type and severity. Accident Analysis and Prevention. 2021;**149**:105858

[19] Peng Y, Liu D, Wu S, et al. Enhancing mixed traffic flow with platoon control and lane management for connected and autonomous vehicles. Sensors. 2025;**25**:644

[20] Ruan T, Zhou L, Wang H. Stability of heterogeneous traffic considering impacts of platoon management with multiple time delays. Physica A: Statistical Mechanics and Its Applications. 2021;**583**:126294

[21] Zheng S-T, Jiang R, (Michael) Chen X, et al. Communicating with two vehicles immediately ahead boosts traffic capacity sixfold in connected autonomous vehicle platoons. Communications Engineering. 2025;**4**:160

[22] Zhou L, Ruan T, Ma K, et al. Impact of CAV platoon management on traffic flow considering degradation of control mode. Physica A: Statistical Mechanics and Its Applications. 2021;**581**:126193

[23] Jerath K, Vv G, SN B. Mitigating delay due to capacity drop near freeway bottlenecks: Zones of influence of connected vehicles. PloS One. 2024;**19**: e0301188

[24] Rebelo M, Rafael S, Bandeira JM. Vehicle platooning: A detailed literature review on environmental impacts and future research directions. Future Transportation. 2024;**4**:591–607

[25] Sala M, Soriguera F. Capacity of a freeway lane with platoons of autonomous vehicles mixed with regular traffic. Transportation Research Part B: Methodological. 2021;**147**: 116–131

[26] Jiang Y, Zhu F, Yao Z, et al. Platoon intensity of connected automated vehicles: Definition, formulas, examples, and applications. Journal of Advanced Transportation. 2023;**2023**: 1–17

[27] Chang Q, Chen H. Enhancing freeway traffic capacity: The impact of autonomous vehicle platooning intensity. Applied Sciences. 2024;**14**:1362

[28] Liu H, Kan X, Shladover SE, et al. Modeling impacts of cooperative adaptive cruise control on mixed traffic

flow in multi-lane freeway facilities. Transportation Research Part C: Emerging Technologies. 2018;**95**: 261–279

[29] Yao Z, Ma Y, Ren T, et al. Impact of the heterogeneity and platoon size of connected vehicles on the capacity of mixed traffic flow. Applied Mathematical Modelling. 2024;**125**: 367–389

[30] Oriol L, Martínez-Díaz M, Moode SN, et al. Platooning of connected automated vehicles on freeways: A microsimulation approach. Transport B: Transport Dynamics. 2024;**12**:2360543

[31] Cheng R, Lou H, Wei Q. Analysis of the impact for mixed traffic flow based on the time-varying model predictive control. Systems. 2025;**13**:481

[32] Zhou M, Qu X, Jin S. On the impact of cooperative autonomous vehicles in improving freeway merging: A modified intelligent driver model-based approach. IEEE Transactions on Intelligent Transportation Systems. 2016;**18**:1422–1428

[33] Jiang Y, Wang S, Yao Z, et al. A cellular automata model for mixed traffic flow considering the driving behavior of connected automated vehicle platoons. Physica A: Statistical Mechanics and Its Applications. 2021;**582**:126262

[34] Gao H, Ren X, You Z, et al. Determination of the optimal connected and automated vehicles platoon size based on the merging success rate. Transportation Letters. 2024;**16**:857–871

[35] Zhu J, Tasic I, Qu X. Flow-level coordination of connected and autonomous vehicles in multilane freeway ramp merging areas. Multimodal Transportation. 2022;**1**:100005

[36] Xie J, Chen J, Lv Z, et al. An optimal coordinated merging strategy for CAVs platoon at on-ramp area. Physica A: Statistical Mechanics and Its Applications. 2025;**676**:130892

[37] Yue S, Zong F, Dantsuji T, et al. A platoon-based cooperative merging ecological control framework under connected environment. In: Proceedings of the Australasian Transport Research Forum, Melbourne, Australia 2024 Nov. p. 27–29

[38] Irshayyid A, Chen J. Comparative study of cooperative platoon merging control based on reinforcement learning. Sensors. 2023;**23**:990

[39] Xie J, Chen J, Lv Z, et al. An optimal coordinated merging strategy for CAVs platoon at on-ramp area. Physica A: Statistical Mechanics and Its Applications. 2025;**676**:130892

[40] Schwab A, Lunze J. Vehicle platooning and cooperative merging. IFAC-Pap. 2019;**52**:353–358

[41] Sakaguchi Y, Bakibillah ASM, Kamal MAS, et al. A cyber-physical framework for optimal coordination of connected and automated vehicles on multi-lane freeways. Sensors. 2023;**23**:611

[42] van Maarseveen S. Impacts of Truck Platooning at Motorway On-ramps

[43] Li X, Zhang W, Li Q, et al. Analysis of driver Lane-Changing behavior under the influence of truck platoons at highway Exits: A driving simulation study. Transportation Research Part

F: Traffic Psychology and Behaviour. 2025;**113**:174–193

[44] Jeon H, Benekohal RF. Speed and lane change management strategies for CAV in mixed traffic for post-incident operation. Future Transportation. 2025;**5**:51

[45] Aiura R, Morino H. Mitigating traffic congestion due to an accident with area-dependent jam absorption driving. In: 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops). IEEE, p. 575–580

[46] Zhang W, Yi J, Zhou G, et al. Drivers' decelerating behaviors in expressway accident segments under different speed limit schemes. International Journal of Environmental Research and Public Health. 2022;**19**:1590

[47] Bajestani SM, Fries RN. Predicting the effect of connected vehicles on safety near traffic incidents on freeways. In: International Conference on Transportation and Development 2019. Alexandria, Virginia: American Society of Civil Engineers, p. 30–40

[48] Li W, Zeng J, Wei X. Characteristics of mixed traffic flow at accident bottlenecks with connected and automated vehicles platoons: A cellular automata simulation. Xu Charact Mix Traffic Flow Accid Bottlenecks Connect Autom Veh Platoons Cell Autom Simul, Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4919439 [Accessed: 2025-December-01]

[49] Wu X, Postorino MN, Mantecchini L. Impacts of connected autonomous vehicle platoon breakdown on highway. Physica A: Statistical Mechanics and Its Applications. 2024;**650**:130005

[50] Abdulsattar H, Mostafizi A, Mr S, Wang H. Measuring the impacts of connected vehicles on travel time reliability in a work zone environment: An agent-based approach. Journal of Intelligent Transportation Systems. 2020;**24**(5):421–436

[51] Kesting A, Treiber M, Helbing D. Enhanced intelligent driver model to access the impact of driving strategies on traffic capacity. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences. 2010;**368**:4585–4605

[52] Milanés V, Shladover SE. Modeling cooperative and autonomous adaptive cruise control dynamic responses using experimental data. Transportation Research Part C: Emerging Technologies. 2014;**48**:285–300

[53] Barceló J, editor. Fundamentals of Traffic Simulation. New York: Springer New York; 2010. DOI: 10.1007/978-1-4419-6142-6

[54] Cohen S. Application of relaxation procedure for lane changing in microscopic simulation models. Transportation Research Record: Journal of the Transportation Research Board. 2004;**1883**:50–58

[55] Treiber M, Hennecke A, Helbing D. Congested traffic states in empirical observations and microscopic simulations. Physical Review E. 2000;**62**:1805–1824

[56] Erdmann J. Lane-changing model in SUMO. Proceedings of SUMO2014: Modeling Mobility with Open Data. 2014;**24**:127

[57] Daamen W, Loot M, Hoogendoorn SP. Empirical analysis of merging behavior at freeway on-ramp. Transportation Research Record: Journal of the Transportation Research Board. 2010;**2188**:108–118

[58] Laval JA, Leclercq L. A mechanism to describe the formation and propagation of stop-and-go waves in congested freeway traffic. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences. 2010;**368**:4519–4541

[59] Li Z, Yu S. Design and research of a vehicle approaching reminder device based on zigbee wireless sensor network. Scientific Programming. 2022;**2022**:8797953

[60] Xiao L, Wang M, Schakel W, et al. Unravelling effects of cooperative adaptive cruise control deactivation on traffic flow characteristics at merging bottlenecks. Transportation Research Part C: Emerging Technologies. 2018;**96**:380–397

[61] Newell GF. A simplified car-following theory: A lower order model. Transportation Research Part B: Methodological. 2002;**36**:195–205

[62] Zhang H, Hou N, Zhang J, et al. Evaluating the safety impact of connected and autonomous vehicles with lane management on freeway crash hotspots using the surrogate safety assessment model. Journal of Advanced Transportation. 2021;**2021**:5565343

[63] Nelder JA, Mead R. A simplex method for function minimization. The Computer Journal. 1965;**7**:308–313

Chapter 17

Optimization of Highway On-Ramp Merging Maneuvers in Pure and Mixed CAV Environments: An Overview

Salvatore Viscio, Nadia Giuffrida, Mario Marinelli and Mario Binetti

Abstract

This study provides a comprehensive review of optimization strategies for highway on-ramp merging in the context of connected and automated vehicles (CAVs), addressing both fully automated (pure CAV) and mixed traffic environments involving human-driven vehicles (HDVs). In pure CAV environments, vehicle connectivity and real-time communication enable coordinated control, allowing precise trajectory and speed optimization. Advanced control frameworks, such as hierarchical, predictive, and cooperative models, focus on minimizing travel time, energy consumption, and congestion while ensuring safety. Key optimization variables include vehicle speed, acceleration, and position, which are adjusted dynamically through centralized or distributed control systems. In mixed traffic environments, where CAVs coexist with HDVs, merging becomes more complex due to heterogeneous driving behaviors. Optimization methods here combine automated control for CAVs with behavior models representing HDV dynamics. Such approaches integrate cooperative adaptive cruise control (ACC), rolling-horizon trajectory planning, and hierarchical control frameworks to ensure safe and efficient merging across varying traffic compositions. Findings consistently highlight that higher CAV market penetration improves traffic performance, reducing delays and enhancing flow stability. Overall, the literature demonstrates that optimization of on-ramp merging in both pure and mixed CAV environments relies on fine-tuning speed, position, and acceleration through predictive and cooperative control frameworks. Future research should focus on developing real-time, scalable optimization frameworks that can adapt to varying levels of CAV penetration, account for human behavioral uncertainty, and enhance both traffic efficiency and safety through seamless coordination between automated and human-driven vehicles in complex traffic environments.

Keywords: optimization strategies, on-ramp merging maneuvers, CAV environment, connected and automated vehicles (CAVs), human-driven vehicles

1. Introduction

The development of connected and automated vehicles (CAVs) has motivated extensive research into how vehicle coordination can improve safety and efficiency in highway operations. One of the most studied situations is on-ramp merging, a critical phase that strongly affects traffic flow stability and congestion. In a pure CAV environment, where every vehicle is capable of automated driving and communication, merging can be optimized through real-time coordination instead of relying on human driver behavior. Using vehicle-to-everything (V2X) communication, CAVs continuously exchange information with nearby vehicles and roadside infrastructure, enabling centralized or cooperative control strategies that manage merging sequences, speed adjustments, and inter-vehicle gaps. However, as CAVs initially coexist with human-driven vehicles (HDVs), understanding and optimizing merging in mixed traffic conditions, where automated and manual driving behaviors interact, has also become a major research focus.

Based on this premise, this chapter reviews the main optimization-based methods proposed to address on-ramp merging under fully connected and mixed-traffic conditions. The literature includes a range of approaches, from analytical optimal control formulations to numerical optimization and hierarchical coordination frameworks. Early studies formulated merging as an optimal control problem and derived closed-form analytical solutions based on Hamiltonian analysis. Later works introduced trajectory optimization models that use speed and acceleration as decision variables, solved through tools such as MATLAB or LINGO to minimize fuel use or travel time while maintaining safe gaps between vehicles. Other research focused on cooperative and hierarchical control, where higher-level algorithms determine merging order or lane-change timing, and lower-level controllers generate feasible acceleration profiles through model predictive control or discrete-time optimization. These models are typically validated through microsimulation environments such as CORSIM, VISSIM, or MATLAB-Simulink, comparing performance against conventional traffic scenarios.

The chapter is organized as follows: Section 2.1 presents a detailed overview of the optimization strategies proposed for pure CAV traffic, including analytical, model predictive, and hierarchical approaches, highlighting their mathematical formulations, control structures, and performance results. Section 2.2 extends the analysis to mixed traffic environments, where CAVs interact with HDVs and where additional complexities emerge due to behavioral uncertainty and communication limits. Section 2.3 provides a classification framework that categorizes the reviewed methods according to traffic composition, control architecture, and coordination level.

Finally, in Section 3, the review discusses research gaps and future directions. Despite significant progress, many studies rely on simplified settings (e.g., single-lane freeways, perfect communication, or single-vehicle merging), which limit their applicability to real conditions. There remains a need for models that integrate multiple control layers (from trajectory to sequencing), handle multilane and multivehicle interactions, and incorporate stochastic elements to represent human behavior and communication delays. Future research is expected to move toward integrated, multiobjective, and adaptive frameworks, combining analytical optimization with data-driven and learning-based methods to support real-time decision-making in increasingly complex and mixed-traffic environments.

2. Overview of existing methods

2.1 Optimization strategies in pure CAV environment

This section focuses on approaches tailored to address the problem of on-ramp merging optimization within a setting where CAVs constitute the entirety of the vehicular fleet. Unlike traditional traffic scenarios where HDVs dominate, a pure CAV environment presents opportunities and challenges for optimization, given the connectivity and controllability of the driving behavior of such vehicles. Through V2X communication, CAVs exchange real-time status information with neighboring vehicles and Roadside Units (RSUs), e.g., enriching data available to a traffic management center (TMC) for more precise control strategies. Concurrently, infrastructure-to-vehicle communication channels enable the transmission of control commands from the infrastructure to CAVs, facilitating dynamic control measures for improved efficiency and safety during on-ramp merging maneuvers.

Optimization can play a role in maximizing the efficiency of traffic flows and the utilization of road infrastructure when it comes to CAVs, e.g., determining the most effective strategies for merging CAVs onto highways/freeways from entrance ramps. Optimization techniques may include adjusting traffic signal timings, designing merge areas for smooth integration, and utilizing predictive analytics to anticipate merging maneuvers.

Literature on the topic of CAV-based merging strategies has been developed since the early 2000s, and in the last decade, several studies have started to deal with the optimization of merging in a CAV environment. In 2016, in their study, Rios-Torres and Malikopoulos [1] devised an optimization framework aimed at achieving optimal vehicle coordination during merging scenarios, focusing on minimizing fuel consumption while ensuring collision avoidance. Utilizing a polynomial metamodel, they established a relationship between vehicle fuel consumption, speed, and control inputs (such as acceleration and deceleration). The researchers proposed an analytical closed-form solution based on Hamiltonian analysis. To validate their approach, they conducted simulations using MATLAB, simulating a merging scenario involving CAVs under the control of a centralized controller. The results demonstrated that their proposed approach effectively coordinated vehicle movements, leading to significant reductions in both fuel consumption and travel time. Importantly, it facilitated smooth merging without causing congestion, all while adhering to stringent collision avoidance constraints.

More generally, speed and acceleration emerge as key decision variables in addressing the on-ramp merging optimization problem in various works. As an example, Letter and Elefteriadou [2] introduced a longitudinal freeway merging control algorithm aimed at maximizing the average travel speed of CAVs. Their objective involved devising trajectories that would optimize each vehicle's average travel speed within the communication zone while considering factors such as processing order and minimum time gaps, all while adhering to predefined safety and physical constraints. Communication between entities was facilitated via dedicated short range communications (DSRC) Service, with DSRC control updates occurring at regular time intervals. Their optimization problem aims to maximize the average travel speed of the subject vehicle along the communication zone. The decision variables are the discrete-time accelerations, from which the corresponding

positions and speeds are computed. The formulation enforces several types of constraints:

- A safe time-gap constraint, ensuring the temporal distance between the subject vehicle and the preceding vehicle remains above a specified threshold; this safety margin is calculated as the distance between the rear bumper of the leading vehicle and the front bumper of the subject vehicle, divided by the speed of the subject vehicle.
- Velocity limits, bounding speeds within both regulatory and operational ranges.
- Acceleration and deceleration limits, reflecting physical capabilities and comfort expectations.
- A jerk constraint, restricting abrupt changes in acceleration to preserve ride comfort.

The authors evaluated the performance of the merging algorithm and conducted sensitivity analyses to compare the impact of traffic demand and minimum time gap settings. CORSIM microsimulation was utilized to represent a conventional traffic stream consisting of nonautomated vehicles, serving as a benchmark for comparison. Then, a traffic stream comprised entirely of connected, fully automated vehicles was considered. To facilitate these simulations, a merging simulator utility was developed to interface with the optimization software LINGO. Vehicles were randomly generated in CORSIM and utilized as inputs into the merging simulator, with LINGO solving the optimization problems generated at each time step. By employing the same vehicle generation file, direct comparisons between CORSIM simulations and the merging simulator were made possible. The results indicated that the algorithm effectively managed automated vehicle traffic at a basic merging segment, demonstrating improvements during undersaturated conditions in terms of travel time, average travel speed, and travel time per vehicle.

A similar approach is the one by Hu and Sun [3], involving the development of an online system control algorithm tailored for multilane freeway merging areas within a CAV environment. Their algorithm optimized vehicles' lane changing and car-following trajectories to enhance efficiency while ensuring safety through the imposition of various constraints. The merging system was conceptualized as a time-discrete linear system, with optimization objectives focused on efficiency enhancement. To simplify the lane-changing control problem, the study proposed a rule-based lane-changing decision and a cooperative lane-changing control (CLCC) lane-changing execution process. Additionally, a cooperative merging control (CMC) optimization was conducted. The execution of lane-changing control was facilitated through the CLCC model, a discrete-time linear system control model designed to optimize longitudinal lane-changing acceleration and maximize the average velocity of all vehicles. Similarly to [2], the objective function is to maximize the average velocity of all input vehicles in the current lane-changing period. Constraints include, as in [2], permissible limits on acceleration, velocity, and jerk value, considering both the freeway speed limit and passenger comfort. Other constraints consider: a vehicle's minimum time gap in the same lane; safety constraints for the lane-changing platoon, including the lane-changing platoon's

minimum time gap and maximum velocity difference, and the requirement that the velocity of the vehicles changing lanes be greater than the vehicles following them; traffic flow consistency requirements; and dynamic equations of this linear discrete-time system. The CMC model is also based on [2]; the objective function of the CMC model is to maximize the subject vehicle's average velocity during the optimization process. Also, in this case, constraints include permissible limits on velocity, acceleration, and jerk value. Other constraints are related to the minimum time gap allowed, minimum distance regardless of the subject vehicle's velocity, and system dynamic equations. One of the main challenges of proposing two optimizations in sequence is to offer a seamless integration between the two CLCC and CMC models; in this respect, the authors propose a dynamic moving border point method. To test the approach, the authors created in VISSIM a typical two-lane freeway with one on-ramp lane network and used MATLAB to solve the problems. The study's findings, obtained across various demand levels and demand splits, revealed that the exclusive CMC algorithm significantly decreased delay times by as much as 92.5% compared to scenarios without any control measures. Moreover, when employing a coordinated approach integrating both CLCC and CMC algorithms, superior performance was observed compared to solely utilizing the CMC algorithm, while showcasing the capability to effectively balance lane flow distribution downstream of the merging area.

Later in 2018, Zhou et al. [4] presented a vehicle trajectory planning method tailored for automated on-ramp merging. This study advocates for an endogenous determination of the merge location and time by the optimal control problem of the facilitating vehicle. The trajectory planning problem is expressed through two interconnected optimal control problems: one governing the behavior of the mainline "facilitating" vehicle and the other describing the motion of the on-ramp merging vehicle. For the mainline vehicle, the central goal is to identify a trajectory that enables efficient and safe gap creation for the merging maneuver. The optimization seeks to minimize a composite performance measure that combines the duration of the maneuver with the vehicle's motion effort. The vehicle's longitudinal position, speed, and acceleration evolve continuously over time and constitute the system states and control inputs. A weighting parameter is included in the objective function to penalize unnecessarily long merging processes, encouraging timely coordination. For the on-ramp vehicle, the optimization aims to guide its state evolution (specifically its position, speed, and acceleration) so that it reaches the merging point with desirable terminal conditions. These target conditions represent the speed and position needed for a smooth and safe integration into the mainline traffic stream. The cost function therefore penalizes deviations from these ideal terminal values, with dedicated weighting factors balancing the relative importance of reaching the correct speed versus the correct location at the end of the maneuver. Both optimal control problems incorporate explicit constraints on acceleration, ensuring that vehicle dynamics remain within physically feasible limits. Because the merging location and merging time arise naturally from the solutions of these optimal control problems rather than being predetermined, the framework allows the vehicles to adapt their behavior dynamically to the surrounding traffic context. The Pontryagin Maximum Principle is employed to derive solutions for the optimal control problems. To address the dynamic nature of the external environment, the proposed optimal control method is integrated into a recursive planning framework. Numerical experiments are conducted to assess the performance of the proposed

methodology under varying conditions, including different leading vehicle trajectories and intervals for planning updates. An experiment utilizing a real-world leading vehicle trajectory and considering various traffic demand levels is presented. The results of these experiments indicate that the proposed methodology performs effectively and exhibits promising potential for real-time applications.

In 2020, Chen et al. [5] devised a hierarchical control approach for CAVs, wherein a tactical layer controller utilizes a second-order car-following model alongside a cooperative merging mode to depict the cooperative merging process. This tactical controller generates an optimal sequence of vehicle mergers and determines the instants at which on-ramp CAVs adjust their speeds and positions to merge into target gaps effectively. Furthermore, an operational layer controller is developed based on model predictive control, leveraging a third-order vehicle dynamics model. This controller optimizes desired accelerations for CAVs and determines the instants when on-ramp CAVs initiate lane-changing executions. Both controllers derive their control commands by minimizing an objective function over different time horizons. The objective function penalizes deviations of CAVs' inter-vehicle gaps from desired values, relative speeds concerning their direct predecessors, and actual or desired accelerations. These optimizations are subject to constraints on velocities, actual or desired accelerations, and intervehicle gaps; the state variables include location, speed, and actual acceleration of mainline CAVs and on-ramp CAVs.

In Min et al. [6], the on-ramp merging problem is approached as a bi-objective optimization problem, focusing on minimizing both total fuel consumption and total travel time. To address this, optimal control based on Pontryagin's Minimum Principle is employed to tackle the motion planning challenge. In order to determine suitable parameters for the bi-objective optimization problem, a varying-scale grid search method is introduced. This method aims to systematically explore potential solutions across different scales, facilitating the identification of optimal parameter settings for the optimization process. In this framework, the optimization selects the acceleration trajectory that yields the best trade-off between these competing goals while respecting limits on how quickly a vehicle may accelerate or decelerate. An additional safety condition ensures that only one vehicle is permitted within the merging area at any given moment, preventing the possibility of lateral conflicts.

Shi et al. [7] introduced a control approach aimed at striking a balance between solution optimality and computational efficiency for the real-time determination of optimal merging speed profiles. The study utilizes a pseudospectral method and a sequential convex programming approach to develop two algorithms, both of which are integrated into a model predictive control framework. These algorithms enable the real-time generation of optimal solutions suitable for potential on-vehicle applications. Once the merging sequence and arrival time are established, the approach computes a speed profile to guide vehicles through the control zone. The optimal speed control is formulated as a nonlinear optimal control problem, seeking to minimize cost functions associated with fulfilling multiple driving requirements. These requirements include maintaining a safe distance from the preceding vehicle, ensuring passenger comfort, and adhering to desired speed levels. Rather than imposing a terminal time constraint on the problem, Shi et al. [7] opt to convert the arrival time into a reference speed for the vehicle to track. This approach allows for the iterative generation of the speed profile over a short rolling time horizon. In their formulation, the vehicle's acceleration and deceleration are the control inputs, and

the cost function reflects several competing priorities. One component encourages the vehicle to maintain an appropriate separation from its leader, using a measure of how far the actual spacing deviates from a predefined safe distance. Another component guides the vehicle toward a preferred cruising speed that is consistent with the planned arrival time. A third element discourages abrupt acceleration or braking, promoting smoother driving behavior. Because sustaining motion requires energy, an additional term is included to better represent fuel expenditure under different driving conditions. Each objective is weighted so that the controller can balance comfort, safety, and efficiency. Operational constraints bound the control inputs and restrict the acceptable range of speeds. Overall, the model seeks to produce a speed trajectory that follows a reference velocity while preserving a comfortable and safe distance to the preceding vehicle. The reference velocity itself is obtained by dividing the remaining distance to the merging point by the intended arrival time. If no specific arrival time has been assigned, the vehicle adopts either a fuel-efficient cruising speed or simply aligns its speed with that of the vehicle ahead, depending on which is more appropriate. This design enables the controller to generate feasible and responsive speed plans in real time.

Tang et al. [8] introduced a multilayer merging framework in which decisions about how vehicles should merge and where the merge should occur are optimized jointly. The upper tier of their approach functions as a tactical planner and determines the merging order together with the key states that each vehicle should reach during the maneuver. These key states include, for example, the speed and position that an on-ramp vehicle should have at the moment it enters the mainline. Because the tactical planner must handle both discrete sequencing choices and nonlinear vehicle dynamics, the resulting optimization is formulated as a mixed-integer quadratically constrained problem. Its goal is to minimize the cumulative time required for all vehicles to traverse the control zone. To make this computationally manageable, the authors incorporated a decomposition strategy based on Monte Carlo Tree Search. This method systematically explores promising combinations of merge sequences and critical state assignments before committing to a particular solution. Once the upper level identifies the sequence and state targets, the lower level, referred to as the motion-planning component, generates continuous trajectories that connect these states smoothly. For each pair of consecutive states that a vehicle is expected to reach, an optimal control subproblem is solved to determine a trajectory with minimal variability in speed, which serves as a surrogate for fuel-efficient driving. Vehicle acceleration acts as the control input, and constraints ensure that both speed and acceleration remain within their feasible limits. Simulation experiments showed that allowing the merge location to vary within the optimization significantly improves the chances that ramp vehicles can merge without experiencing undue delay. This flexibility helps the system accommodate diverse traffic situations and enhances the overall efficiency of the merging process.

Recently, Chen et al. [9] proposed an integrated approach that jointly optimizes the merging sequence and vehicle trajectories for multiple CAVs entering a freeway. They formulated a mixed-integer nonlinear programming model to minimize disruption: rather than pairing each entering vehicle with a single mainline vehicle, their model can assign multiple facilitating mainline CAVs to create gaps for a merge. An efficient solution algorithm (combining iterative linear programming with a tailored search strategy) was designed to greatly reduce the computational search

space. Simulations with real traffic data showed this method outperforms first-in-first-out and other baseline strategies in both traffic efficiency and real-time feasibility.

The study by Zhou et al. [10] focuses on preventing congestion shockwaves during merging by leveraging CAV capabilities. They note that when a mainline vehicle slows to facilitate a merge, it can trigger a temporary bottleneck behind it. Zhou's team proposed a simple yet novel CAV-based strategy to actively resolve the "temporary congestion caused by a freeway mainline vehicle's facilitating manoeuvre of creating a gap" for a merging vehicle. In essence, CAVs on the mainline are coordinated to adjust their speeds or lanes so that creating a gap for the ramp vehicle does not induce a cascade of braking. This CAV-enabled approach improved mainline flow efficiency under merging conditions, demonstrating how automation can eliminate the usual capacity drop associated with human drivers' courtesy yielding. By smoothing the mainline traffic disturbances, the method maintained higher throughput and more stable speeds during on-ramp merges, especially under moderate traffic demand, where purely local or purely global controls alone would falter.

Finally, some researchers target platoon-level coordination in pure CAV scenarios. Xie et al. [11] developed an optimal coordinated merging strategy for CAV platoons merging at on-ramps. Traditional approaches mostly optimize one CAV at a time, but this strategy treats groups of vehicles on both the ramp and mainline as cooperating platoons. They determine a globally optimal platoon merging sequence and then apply optimal control (using Pontryagin's Minimum Principle and dynamic programming) to jointly guide multiple vehicles through the merge. The framework ensures constraints (like safe gaps and vehicle dynamics) are respected, and the authors prove asymptotic and string stability for the platoon control system. Simulation experiments showed that coordinating merges at the platoon level can significantly improve traffic efficiency and driver comfort relative to single-vehicle merging optimizations.

In summary, in a full-CAV environment, advanced optimization and control methods (from integrated sequence/trajectory planning to platoon-based coordination) have demonstrated substantial gains in merge throughput, safety, and smoothness by exploiting the predictability and cooperation of automated vehicles. The comparison of studies underscores the predominant focus on optimizing speed, position, and acceleration/deceleration as key decision variables across the reviewed methodologies. Tactical planning models emerge as pivotal in optimizing merging sequences and critical states to minimize total travel time within the system; motion planning models specialize in generating feasible trajectories tailored to individual vehicles, ensuring their seamless integration into the traffic flow. **Table 1** reports a summary of the analyzed key contributions from the literature on on-ramp merging optimization in pure CAV environments.

2.2 Optimization strategies in mixed traffic environment

This section focuses on approaches tailored to address the problem of on-ramp merging optimization in a mixed traffic environment where both CAVs and HDVs coexist; in such cases, the design and optimization of merge areas become more complex due to the interaction between different types of vehicles with varying behaviors and capabilities. Optimization techniques in this context need to account

Authors (Year)	Contribution summary	Tools/methods	Optimization focus
Rios-Torres and Malikopoulos [1]	Analytical optimization using Hamiltonian methods for fuel-efficient merging	MATLAB simulation	Fuel consumption, travel time
Letter and Elefteriadou [2]	Trajectory optimization via LINGO to maximize travel speed	CORSIM + custom merging simulator	Average travel speed, travel time
Hu and Sun [3]	CLCC and CMC-based sequential optimization in multilane merging	VISSIM + MATLAB	Velocity, delay reduction
Zhou et al. [4]	Recursive optimal trajectory planning with endogenous merge point	Numerical simulations	Merge time, real-time feasibility
Chen et al. [5]	Hierarchical model predictive control for cooperative merging	Simulation-based	Acceleration, inter-vehicle gap, speed
Min et al. [6]	Bi-objective optimization using Pontryagin's principle	Grid search simulations	Fuel consumption, travel time
Shi et al. [7]	Pseudospectral MPC with convex optimization for speed profiles	Simulations	Speed tracking, comfort, safety
Tang et al. [8]	Hierarchical MIQCP with MCTS-DA decomposition	Simulations	Total travel time, fuel usage
Chen et al. [9]	Joint optimization of merging sequence and trajectory via MINLP	Real traffic data	Merge efficiency, real-time viability
Zhou et al. [10]	Mainline CAV control to prevent congestion from merging.	Simulations	Mainline capacity, stability
Xie et al. [11]	Platoon-level coordinated merging with dynamic programming	Simulations	Platoon stability, driver comfort

Table 1.
Summary of key contributions in pure CAV environments.

for the heterogeneity of traffic and aim to ensure safe and efficient merging for all vehicles. In general, one can observe that the literature on this topic is more recent; nevertheless, some works have dealt with the topic in recent years. Examples are those of Gao et al. [12], who developed an optimal trajectory optimization strategy for CAVs to facilitate mainline platooning and on-ramp merging within mixed-traffic conditions. Their approach centers on adjusting the behavior of a CAV based on the distance to the vehicle ahead and on the general traffic situation. When the automated vehicle is far from its leader, it simply travels at a steady speed. As it gets closer, its behavior changes: if the gap becomes sufficiently small, the vehicle activates an adaptive cruise control mode that regulates its speed using information about both the spacing and the relative velocity. In this mode, the CAV continually adapts its acceleration to maintain an acceptable headway behind the HDV in front. Between these two extremes lies an intermediate "buffer" range in which the CAV holds its current behavior until it is clear whether a transition to cruising or gap regulation is appropriate. To evaluate how this strategy performs in mixed traffic, the authors coupled a microscopic simulation platform with an external control module. By testing different proportions of CAVs and various demand levels, they observed that higher CAV penetration generally leads to lower average delays, particularly when traffic demand is moderate. At low penetration levels, improvements are limited because opportunities for forming stable CAV platoons are sparse; at very high demand levels, congestion dominates regardless of control

strategy. However, for intermediate conditions, especially around a 30% CAV share, the cooperative behavior supported by their model enables more efficient gap creation and merging, resulting in noticeable reductions in delay and more consistent traffic flow. Mu et al. [13] introduced an event-triggered rolling horizon-based systematic trajectory planning approach aimed at facilitating the safe and seamless merging of two platoons, whether composed of purely CAVs or a mixture of CAVs and conventional vehicles. This method is specifically designed for application at mainline-ramp intersections within well-defined trajectory control zones. The trajectory control zones, situated on both the mainline and ramp, are subdivided into pre-merging, virtual-merging, and postmerging subzones. The RSTP is activated solely when a new CAV approaches the virtual merging subzone on either the mainline or ramp. At this point, it generates an optimal trajectory plan for the CAV platoons within the two pre-merging subzones using a mixed-integer nonlinear program. The RSTP, coupled with a real-time correction mechanism, ensures that the two platoons smoothly merge at the conclusion of the virtual merging subzone, even in the presence of disturbances. The overarching objective is to maximize traffic performance across the entire stream. To efficiently tackle the MINLPs inherent in this approach, a heuristic algorithm known as the MIA has been developed, capitalizing on the problem's unique characteristics. The scholars evaluated their rolling-horizon trajectory planning framework using FHWA traffic data and showed that it performs reliably in both fully automated and mixed-traffic environments. The method assumes that CAVs strictly follow the trajectories issued by the controller, while the HDVs behave according to conventional car-following rules, such as those described by the Newell model [14]. Within each planning cycle, the controller attempts to maximize traffic efficiency, which they measure by the average longitudinal distance that a CAV is expected to travel during that cycle. Safety and feasibility are enforced through constraints associated with vehicle dynamics, the geometry of the merging zone, and the interaction rules in each subarea of the control region. To extend the framework to mixed traffic, the authors introduced a representation in which groups of HDVs are bundled into blocks led by a CAV. In this arrangement, the leading CAV dictates the motion of the block, while the HDVs inside it maintain appropriate spacing using their own car-following behavior. This structure allows the planner to treat each block as if it were a single entity with an effective length, making it possible to integrate both CAVs and HDVs within one optimization scheme. If, however, the HDVs are in unconstrained free flow and no longer respond to the leading CAV's trajectory, the controller cannot operate effectively, and the RSTP approach is not applied in that instance. When used for coordinating the merging of two platoons, one on the mainline and the other on the ramp, the framework seeks to identify trajectories that enable all vehicles or blocks to advance smoothly to the merging point. The optimization goal reflects how far these entities are expected to move collectively within the planning window, normalized by the total number of units involved. Because of the mixed composition, the problem incorporates the combined contributions of both CAVs and HDVs. Constraints ensure that each entity adheres to feasible motion conditions, including speed limits and limits on acceleration and braking. In addition, safety margins must be maintained so that neither individual vehicles nor blocks violate collision-avoidance rules. Through numerical testing, the authors demonstrated that the RSTP can coordinate mixed platoons effectively, provided that the HDVs remain responsive to the lead CAV. Under these conditions, the method creates orderly

merging patterns, reduces the risk of conflicts, and supports efficient use of the merging zone. Han et al. [15] developed a two-level hierarchical traffic control framework tailored for multilane merging areas in mixed traffic environments. The framework operates under the assumption that the merging sequence is determined at the high control level, with a focus on the low control level, particularly concerning trajectory optimization strategies for both CAVs and HDVs. At the low control level, the framework incorporates several key strategies. Firstly, a lane-changing optimization method is proposed to facilitate early lane changes for designated mainline CAVs, thereby balancing downstream lane flow distribution and providing ample merging space for on-ramp vehicles. Secondly, a cooperative merging control method is introduced to optimize longitudinal trajectories for both mainline and on-ramp CAVs while considering HDV movements. This strategy, essentially a discrete-time nonlinear program, aims to maximize CAV speeds throughout the cooperative merging control zone. Each vehicle entering the zone is assigned a merging sequence, optimizing CAV speeds while avoiding potential conflicts with other vehicles. For the HDVs' merging, the authors developed a human-like merging strategy to prevent oscillation in the cooperative merging control zone. HDVs on the outer lane consider their preceding vehicle as the leader, controlling their movement based on the Gipps car-following model. Upon reaching the merging point, HDVs evaluate the presence of merging vehicles and adjust their leader accordingly. HDVs on the on-ramp lane consider their preceding vehicle as the leader until reaching the merging point, thereafter seeking opportunities to merge into the mainline. If unable to merge immediately, the vehicle waits at the end of the acceleration lane for the next available gap. Once merged, HDVs maintain safe distances from their new leaders using the Gipps car-following model [16].

Recently, Jing et al. [17] developed a hierarchical cooperative merging strategy for a mix of CAVs and HDVs. In their approach, an upper-layer merging sequencing algorithm computes the optimal merge order for vehicles approaching the on-ramp junction, considering efficiency, safety, and comfort. This sequencing is formulated as a shortest-path problem (via a 0–1 integer program) to find the optimal ordering with minimal conflict. A lower-layer consensus control then guides the CAV platoon to execute the merge order smoothly while accounting for communication delays and ensuring string stability. Jing et al. found that this two-layer control can significantly reduce merging conflicts and delays; notably, as the CAV proportion increases, the traffic flow becomes more stable and robust against disturbances in the merge zone. Similarly, Hou et al. [18] proposed a cooperative on-ramp merging control model for multilane freeways with mixed traffic. Their upper layer uses an anticipatory search to decide at which position each ramp vehicle should merge and assigns one or more cooperative vehicles (CAVs on the mainline) to create a gap for it. A collaborative utility model determines how those mainline CAVs should maneuver (e.g., slowing down or changing lanes) to accommodate the merge, factoring in a driver compliance rate to reflect that some human drivers may not yield as instructed. The lower layer then handles the vehicle-following and lane-changing control to carry out the merge safely. This hierarchical scheme showed that when even half of the drivers cooperate, traffic performance improves markedly; at high CAV penetration and good compliance, Hou et al. report over a 75% increase in combined mainline-ramp throughput and far fewer shockwaves compared to unmanaged merges. These studies highlight that in mixed traffic, a structured two-level control (optimizing merge logistics at the network level and

vehicle motions at the local level) is effective, especially as the automated vehicle fraction and human compliance grow.

Another line of research in mixed environments aims to balance safety and efficiency objectives using CAVs as intelligent mediators. Zhang et al. [19] tackled this by formulating a multiobjective control for CAVs in merging zones that optimizes both traffic throughput and safety risk simultaneously. They developed a nonlinear mixed-integer model to govern each CAV's decisions (such as whether to yield or go) using predicted trajectories of surrounding vehicles. Uniquely, they employed a Transformer neural network to forecast near-future traffic conditions under different control parameter weights, effectively learning how aggressive or cautious strategies might play out. An adaptive weighting mechanism then selects the best trade-off solution from the Pareto frontier of the multiobjective optimization. Through iterative coordination (CAVs share intentions and adjust in several rounds), the system finds a balance that avoids collisions without too much loss of efficiency. Even with a low CAV market share, this strategy had a profound impact: at only 20% CAV penetration, simulations showed nearly a 49% reduction in total stopping delay and a 72% reduction in a time-to-collision risk metric compared to no control. This demonstrates the potential for CAVs to simultaneously improve safety and traffic flow in a mixed setting by intelligently adapting their behavior based on real-time conditions.

Since HDVs introduce uncertainty, some researchers have incorporated game-theoretic and human-behavior models into the merge control logic. Jing et al. [20] proposed a decentralized human-like merging framework that allows CAVs to anticipate and respond to human drivers' actions. They model the interactions at a merge as a stochastic potential game, where each CAV chooses actions (accelerate, decelerate, etc.) to maximize a payoff that reflects smooth traffic flow, while considering that HDVs may behave unpredictably. A model predictive controller is used for each CAV to optimize its trajectory over a short horizon with respect to the game's potential function. A distributed solution algorithm then lets multiple CAVs solve this game in parallel, achieving a near-optimal joint strategy without heavy centralized computation. Crucially, the team calibrated the game model with real human driving data so that the CAVs' decisions would appear more "human-like" and not inadvertently provoke or confuse human drivers. In tests on a two-lane merge scenario, this human-centric approach enabled CAVs to blend more seamlessly with human traffic (CAVs merged smoothly with improved overall efficiency, and the algorithm converged quickly to a stable traffic pattern). Such results indicate that accounting for human behaviors and uncertainties via game theory can enhance CAV integration into mixed traffic.

Coordination among multiple CAVs is another tactic to manage mixed-traffic merges. Choi et al. [21] introduced an optimization-based strategy where CAVs actively influence HDV behavior to facilitate smoother merging. In their scenario, all CAVs in the merging control zone coordinate as a group. A key innovation is identifying a "strategic" CAV (typically the CAV directly ahead of one or more HDVs on the mainline) and having it intentionally slow down slightly. By doing so, this strategic CAV enlarges the gap behind it, effectively prompting the trailing HDV to also slow and creating space for another CAV (from the on-ramp or another lane) to merge in front of the HDV with less uncertainty. The authors evaluate various slowdown patterns and select the optimal one in real time whenever a new vehicle enters the control zone, using a dynamic programming approach to maximize CAV

Authors (Year)	Contribution summary	Tools/methods	Optimization focus
Gao et al. [12]	Trajectory optimization integrating ACC behavior in mixed traffic	VISSIM + MATLAB	Delay reduction, CAV platooning
Mu et al. [13]	Rolling horizon MINLP-based trajectory planning for platoon merging	FHWA data, heuristic algorithm	Traffic efficiency, merge coordination
Han et al. [15]	Two-level control with lane change and human-like HDV strategies	IET model-based simulation	Trajectory optimization, HDV accommodation
Jing et al. [17]	Hierarchical merging strategy with integer programming and consensus control	Simulation-based	Merge sequencing, string stability
Hou et al. [18]	CORMC with cooperative utility and lane-changing logic	Simulation-based	Throughput, conflict reduction
Zhang et al. [19]	Multiobjective control using Transformer-based prediction	Simulations	Safety–efficiency trade-off
Jing et al. [20]	Stochastic game-based decentralized merging strategy	MPC + distributed algorithm	Human-likeness, merging coordination
Choi et al. [21]	CAV coordination strategy influencing HDV behavior	Dynamic programming	Delay reduction, strategic gap creation

Table 2.
Summary of key contributions in mixed CAV–HDV environments.

throughput without compromising safety. Importantly, this proactive gap creation by CAVs was shown to reduce average merge delays: the mixed-traffic simulations saw up to 31% lower average travel time delay compared to a prior state-of-the-art merging control method. This outcome underscores that even in a mixed fleet, CAVs can strategically cooperate (influencing human drivers' behavior in subtle ways) to improve overall traffic performance.

In summary, the inclusion of HDV behavior modeling in studies conducted in mixed traffic environments adds complexity and realism to the analysis, allowing researchers to develop comprehensive traffic control strategies that cater to diverse vehicle types and enhance overall traffic efficiency and safety. From the analysis of various approaches, it is evident that in mixed-traffic environments, HDV contributions are often modeled using traditional car-following models like those by Newell or the Gipps model. The dynamics derived from such models are then integrated into optimizations for CAVs, ensuring compatibility and coherence within the mixed traffic context. This allows for a holistic understanding of traffic flow dynamics and facilitates the design of effective control strategies that account for the interactions between different vehicle types, given that mixed traffic environments are likely to persist for the foreseeable future. In **Table 2**, a summary of the analyzed key contributions from the literature on on-ramp merging optimization in mixed CAV–HDV environments is reported.

2.3 Classification framework of optimization approaches

In this section, we provide a classification framework to better organize and compare the above-described methods.

Optimization-based approaches can be broadly classified along three key dimensions: traffic composition, control architecture, and coordination level. The first dimension distinguishes between methods developed for pure CAV traffic and those adapted for mixed environments involving HDVs. The second dimension refers to the control architecture, which can be either centralized, where a central controller manages all vehicle trajectories; decentralized, where vehicles make decisions locally based on shared information; or hierarchical, where control is layered into tactical (planning) and operational (execution) levels. The third dimension considers the coordination level, reflecting whether the model governs individual vehicles, vehicle pairs, or vehicle platoons. These dimensions are illustrated in **Figure 1**, which presents a conceptual diagram of the reviewed approaches. Each method is positioned based on its traffic setting (pure vs. mixed), control strategy (centralized, decentralized/hierarchical), and coordination level (vehicle-based vs. platoon-based).

In detail, methods in the pure-CAV/centralized/vehicle-level block assume a fully connected and automated traffic environment, where all vehicles are CAVs. Control is managed by a centralized system, such as a TMC or RSU, which has full access to the state of each vehicle within the merging area. Models in this category typically use continuous-time optimal control or trajectory planning methods, often solving closed-form or real-time numerical optimization problems. Assumptions include perfect V2X communication, complete vehicle controllability, and the absence of behavioral uncertainty. This setting allows for precise coordination of speed, acceleration, and position for each individual vehicle entering or traversing the merge zone.

The pure-CAV/decentralized or hierarchical/platoon-level block is characterized by the cooperative control of CAV platoons using decentralized or hierarchical architectures. The traffic environment is homogeneous (pure CAV), but the control

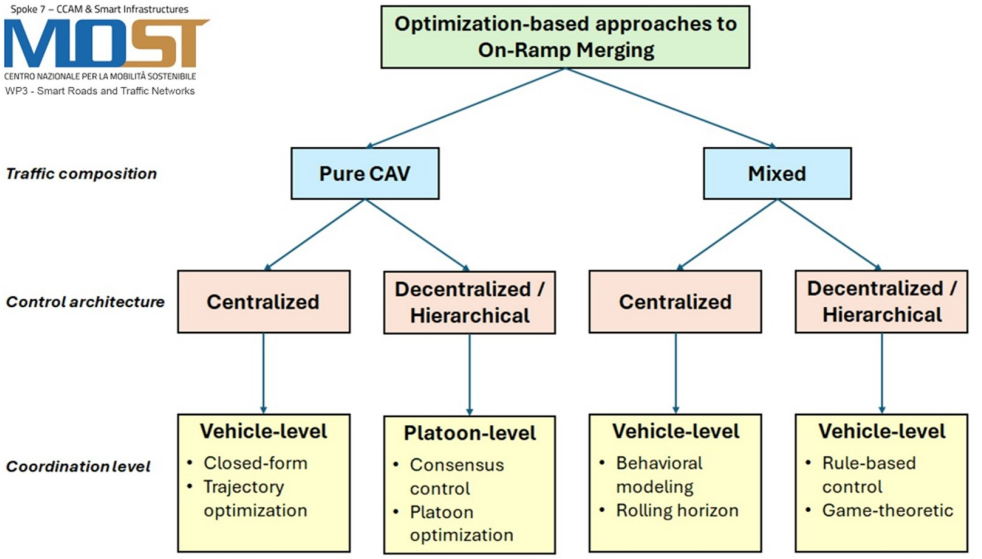


Figure 1.
Conceptual diagram of optimization-based approaches to on-ramp merging.

structure is distributed: each vehicle or cluster of vehicles operates semi-independently, often relying on consensus protocols, local V2V communication, or distributed model predictive control. Higher-level layers may plan merging sequences for platoons or groups, while lower layers ensure dynamic feasibility at the vehicle level. These strategies often aim to preserve string stability, minimize delay across multiple merging vehicles, or optimize the merging sequence for entire platoons.

The mixed-traffic/centralized/vehicle-level block represents centralized vehicle-level optimization strategies in heterogeneous traffic. It assumes that the infrastructure can exert some control over CAVs, while HDVs are modeled using behavior rules or car-following models (e.g., Newell or Gipps). The optimization problem becomes more complex due to partial observability and uncertain compliance of HDVs. Control inputs for CAVs are still generated by a centralized entity, but they often require robust or adaptive components to manage the unpredictable interactions with HDVs. Trajectory planning for individual CAVs is still the primary control mechanism, with safety margins adapted to reflect possible human deviations. Forecasting techniques and rolling-horizon algorithms are often used in this category to deal with prediction uncertainty.

Finally, the mixed-traffic/decentralized or hierarchical/vehicle-level block captures the most complex real-world setting, where CAVs must act autonomously (or semi-autonomously) in mixed traffic while anticipating or adapting to human driver behavior. Control is distributed among individual CAVs, often using predictive or game-theoretic reasoning to negotiate space and timing with HDVs. Models may use stochastic games, rule-based logic, or reinforcement learning to infer the intentions and responses of surrounding vehicles. Due to partial observability and limited control over HDVs, these systems rely on conservative safety margins and multiround decision updates. Coordination may involve influencing HDVs (strategic slowdown or lane occupation) to facilitate smoother merges for other vehicles. The hierarchy often spans from tactical decision-making (e.g., merge or yield) to operational control (e.g., trajectory generation).

This framework highlights several key insights. First, most pure CAV studies favor centralized control and precise trajectory optimization, leveraging the controllability of automated vehicles. Second, hierarchical and distributed control strategies dominate the mixed traffic domain, reflecting the need to accommodate behavioral uncertainty and partial observability of HDVs. Third, while some recent work addresses platoon-level merging, especially in the pure CAV setting, coordinated multivehicle control remains relatively underexplored in mixed environments, where scalability and robustness challenges are more pronounced. **Figure 1** thus serves as both a taxonomy and a roadmap for future research.

3. Discussion and conclusions

3.1 Research gaps

Despite significant progress, the research on optimization-based ramp merging reveals some gaps. Even in fully autonomous (pure CAV) scenarios, many models assume idealized conditions (e.g., single-lane freeways with 100% CAV penetration) and focus narrowly on lower-level trajectory control, with scant

attention to higher-level decisions like optimal merge sequencing or gap selection [22]. This ideal-case approach overlooks multilane interactions and broader traffic-flow effects, underscoring the need for integrated multilevel frameworks. In mixed traffic environments, a critical limitation is the simplified treatment of HDVs: most studies presume human drivers will strictly follow predefined rules without error or variation, which underestimates the uncertainty in human behavior and overestimates their willingness to cooperate. As a result, current strategies may not be robust to unpredictable driver responses. Moreover, existing models generally treat human-driven cars as passive obstacles, seldom exploring ways to influence or accommodate human behavior for smoother mergers. Another underexplored area is complex road geometry. Multilane mainlines and dual-lane on-ramps remain insufficiently addressed in the optimization literature [23]; even when tackled, many approaches rely on simplified, discrete maneuvers (e.g., binary lane-change decisions or fixed merge points), rather than continuous optimal control. Likewise, most frameworks handle one merging vehicle at a time, leaving open questions about scalability to multiple simultaneous mergers or high traffic volumes.
A further methodological gap is the lack of true multiobjective optimization: models typically optimize a single performance metric (efficiency, safety, or energy) in isolation, whereas real-world merging demands balancing these often-competing objectives. Overall, these limitations point to unresolved challenges in developing robust optimization models that can coordinate at both the vehicle and network levels, handle mixed traffic uncertainties, and manage multilane merging maneuvers in a unified way.

3.2 Future perspectives

Optimization modeling for on-ramp merging in both pure and mixed CAV environments is poised to become more holistic, robust, and adaptive. A major research direction is the development of integrated, multilevel control frameworks that unify lower-level trajectory optimization with higher-level decisions, such as merge sequencing and gap selection [22]. Most existing studies segregate these levels, focusing on either fine-grained vehicle trajectories or simplified merge-order rules. Thus, a comprehensive system that optimizes across operational and tactical layers is needed to fully capitalize on CAV capabilities. Such frameworks would likely be multiobjective, balancing efficiency, safety, and sustainability. Indeed, optimization-based approaches already target metrics from traffic throughput to fuel economy under various constraints. Future models will extend this by explicitly incorporating additional objectives (e.g., passenger comfort or emissions) and by leveraging hybrid methodologies. Emerging techniques like machine learning and game theory are being explored alongside classical optimal control, hinting at next-generation strategies where data-driven algorithms (e.g., reinforcement learning) and analytical models work in tandem. By combining these methods, researchers aim to produce merging maneuvers that are not only near-optimal but also adaptive to real-time conditions. Ensuring computational tractability for real-time deployment remains a parallel concern, prompting interest in decentralized or approximation algorithms that can deliver timely decisions without sacrificing much optimality.

Equally important are the conceptual challenges and underexplored settings that future studies must address. In mixed traffic scenarios, one fundamental challenge is

modeling and mitigating the unpredictability of human drivers. Many current approaches assume idealized human behavior (e.g., that HDVs will precisely follow recommended rules), which grossly underestimates the variability and error in real driver responses. To design robust merging strategies, future optimization models should incorporate stochastic driver behavior and uncertainty, using robust or probabilistic formulations to ensure solutions remain effective amid human variation. Researchers have begun to call for frameworks that systematically include human behavioral parameters, for example, developing extensible decision-making architectures that can be tuned to different CAV penetration rates and driver populations. Another promising direction is to move beyond treating HDVs as uncontrollable obstacles and instead explore ways to influence or coordinate with them. Recent literature highlights that current strategies rarely attempt to modify human behavior for mutual benefit. Addressing this gap could involve designing control strategies that provide incentives or advisory signals to encourage human drivers to cooperate (e.g., gently guiding them to adjust speed or yield), an approach that has been suggested to improve overall merging efficiency.

Furthermore, complex road settings and realistic constraints present rich avenues for future inquiry. Multilane freeway merges, for instance, remain relatively underexplored compared to one-lane scenarios due to their added complexity. Past studies often resort to simplified, discrete decision rules (such as fixed incremental speed changes or binary lane-change choices) to manage multilane merges. There is a clear need for more sophisticated coordination strategies in both longitudinal and lateral dimensions for multilane environments. Future work can focus on continuous or hybrid control approaches that allow CAVs to proactively change lanes and adjust speeds in concert, informed by thorough analyses of network-wide impacts. Similarly, merging situations beyond the canonical on-ramp (such as work zone merge areas, sudden lane drops, or weaving sections) deserve greater attention. Adapting CAV merging algorithms to these contexts (which introduce new traffic patterns and constraints) will extend the benefits of CAV coordination to a wider range of real-world scenarios. Importantly, as these advanced models grow more complex, extensive validation becomes crucial. Future research should rigorously evaluate the safety and adaptability of proposed merging strategies under diverse conditions (e.g., varying traffic densities, communication delays, sensor uncertainties) to ensure they are reliable in practice. By tackling these methodological advancements and conceptual challenges, future research will move highway on-ramp merging closer to its optimal form – one that seamlessly integrates automated and HDVs for maximal safety and efficiency in mixed traffic.

Acknowledgments

This study was carried out within the MOST – Sustainable Mobility National Research Centre and received funding from the European Union Next-GenerationEU (PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR) – MISSIONE 4 COMPONENTE 2, INVESTIMENTO 1.4 – D.D. 1033 17/06/2022, CN00000023). This manuscript reflects only the authors' views and opinions, neither the European Union nor the European Commission can be considered responsible for them.

The authors acknowledge the use of OpenAI tools for language editing and drafting support in portions of this chapter; all content was reviewed and validated by the authors, who retain full responsibility for the work.

Author details

Salvatore Viscio, Nadia Giuffrida, Mario Marinelli* and Mario Binetti
DICATECh, Polytechnic University of Bari, Bari, Italy

*Address all correspondence to: mario.marinelli@poliba.it

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] Rios-Torres J, Malikopoulos AA. Automated and cooperative vehicle merging at highway on-ramps. IEEE Transactions on Intelligent Transportation Systems. 2016;**18**(4):1–10. DOI: 10.1109/TITS.2016.2587582

[2] Letter C, Elefteriadou L. Efficient control of fully automated connected vehicles at freeway merge segments. Transportation Research Part C: Emerging Technologies. 2017;**80**: 190–205. DOI: 10.1016/j.trc.2017.04.015

[3] Hu X, Sun J. Trajectory optimization of connected and autonomous vehicles at a multilane freeway merging area. Transportation Research Part C: Emerging Technologies. 2019;**101**: 111–125. DOI: 10.1016/j.trc.2019.02.016

[4] Zhou Y, Cholette ME, Bhaskar A, Chung E. Optimal vehicle trajectory planning with control constraints and recursive implementation for automated on-ramp merging. IEEE Transactions on Intelligent Transportation Systems. 2018;**20** (9):3409–3420. DOI: 10.1109/TITS.2018.2874234

[5] Chen N, van Arem B, Alkim T, Wang M. A hierarchical model-based optimization control approach for cooperative merging by connected automated vehicles. IEEE Transactions on Intelligent Transportation Systems. 2020;**22**(12):7712–7725. DOI: 10.1109/TITS.2020.3007647

[6] Min H, Fang Y, Wu X, Wu G, Zhao X. On-ramp merging strategy for connected and automated vehicles based on complete information static game. Journal of Traffic and Transportation Engineering. 2021;**8** (4):582–595. DOI: 10.1016/j.jtte.2021.07.003

[7] Shi Y, Wang Z, LaClair TJ, Wang CR, Yuan J. Real-Time On-Ramp merging control of connected and automated vehicles using pseudospectral convex optimization. In: Proceedings of 2022 American Control Conference (ACC 2022); 8-10 June 2022; Atlanta, USA; p. 2000–2005. DOI: 10.23919/ACC53348.2022.9867422

[8] Tang Z, Zhu H, Zhang X, Iryo-Asano M, Nakamura H. A novel hierarchical cooperative merging control model of connected and automated vehicles featuring flexible merging positions in system optimization. Transportation Research Part C: Emerging Technologies. 2022;**138**:103650. DOI: 10.1016/j.trc.2022.103650

[9] Chen J, Zhou Y, Chung E. An integrated approach to optimal merging sequence generation and trajectory planning of connected automated vehicles for freeway On-Ramp Merging sections. IEEE Transactions on Intelligent Transportation Systems. 2024;**25**(2):1897–1912. DOI: 10.1109/TITS.2023.3315650

[10] Zhou Y, Chen J, Chung E, Ozbay K. CAV-enabled active resolving of temporary mainline congestion caused by gap creation for On-Ramp Merging vehicles. IEEE Transactions on Intelligent Transportation Systems. 2024;**25**(7):6873–6888. DOI: 10.1109/TITS.2023.3340170

[11] Xie J, Chen J, Lv Z, Xu Z. An optimal coordinated merging strategy for CAVs platoon at on-ramp area. Physica A: Statistical Mechanics and Its Applications. 2025;**676**:130892. DOI: 10.1016/j.physa.2025.130892

[12] Gao ZB, Wu ZZ, Hao W, Long K, Byon YJ, Long K. Optimal trajectory planning of connected and automated vehicles at on-ramp merging area. IEEE Transactions on Intelligent Transportation Systems. 2021;**23**(8):1–13. DOI: 10.1109/TITS.2021.3116666

[13] Mu C, Du L, Zhao X. Event triggered rolling horizon based systematical trajectory planning for merging platoons at mainline-ramp intersection. Transportation Research Part C: Emerging Technologies. 2021;**125**:103006. DOI: 10.1016/j.trc.2021.103006

[14] Newell GF. A simplified car-following theory: A lower order model. Transportation Research Part B: Methodological. 2002;**36**(3):195–205. DOI: 10.1016/S0191-2615(00)00044-8

[15] Han L, Zhang L, Guo W. Multilane freeway merging control via trajectory optimization in a mixed traffic environment. IET Intelligent Transport Systems. 2023;**17**(9):1891–1907. DOI: 10.1049/itr2.12382

[16] Gipps PG. Computer program MULTSIM for simulating output from vehicle detectors on a Multi-Lane Signal Controlled road. Transport Operations Research Group. Working Paper No. 20, University of Newcastle-Upon-Tyne, 1976

[17] Jing D, Chen R, Yao E, Menendez M. A hierarchical cooperative merging control strategy for the mixed traffic of CAVs and HDVs. Transportation Research Part C: Emerging Technologies. 2025;**179**:105230. DOI: 10.1016/j.trc.2025.105230

[18] Hou K, Zheng F, Liu X, Guo G. Cooperative On-Ramp Merging control model for mixed traffic on Multi-lane freeways. IEEE Transactions on Intelligent Transportation Systems. 2023;**24**(10):10774–10790. DOI: 10.1109/TITS.2023.3274586

[19] Zhang L, Ding H, Cheng Z, Zheng X, Zhang W. A traffic control strategy for freeway merging zones cooperating safety and efficiency in the intelligent connected environment of mixed vehicles. Transportation Research Part C: Emerging Technologies. 2025;**179**:105298. DOI: 10.1016/j.trc.2025.105298

[20] Jing D, Yao E, Chen R, Menéndez M. Decentralized human-Like Ramp Merging decision-Making and control based on a stochastic potential game. IEEE Transactions on Intelligent Transportation Systems. 2025;**26**(10):16724–16734. DOI: 10.1109/TITS.2025.3576347

[21] Choi K, Shin S, Seo M. Cooperative merging in mixed traffic based on strategic influence of connected automated vehicles on Human-Driven Vehicle Behavior. Advanced Intelligent Systems. 2025;**7**(7):2400797. DOI: 10.1002/aisy.202400797

[22] Zhu J, Easa S, Gao K. Merging control strategies of connected and autonomous vehicles at freeway on-ramps: A comprehensive review. Journal of Intelligent and Connected

Vehicles. 2022;**5**(2):99–111.
DOI: 10.1108/JICV-02-2022-0005

[23] Wang Y, Xiang J, Pan J, Wang J, Chen T, Wang H. Cooperative control of CAVs in the merging area of multi-lane mainline and dual-lane ramps on freeways. Transportation Safety and Environment. 2025;**7**(2). DOI: 10.1093/tse/tdaf030

Chapter 18

Route Guidance in ITS: Systems Classification, Enabling Technologies, and Methodological Approaches

Anna Laura Pala and Giuseppe Stecca

Abstract

This chapter provides a review of the evolution and classification of vehicle route guidance systems within the framework of intelligent transportation systems (ITS). The analysis highlights how the progressive integration of real-time technologies and data-driven modeling has transformed route guidance from static configurations into dynamic, predictive, and cooperative systems. The review connects route guidance methods to traffic assignment theory, examining the principles of user equilibrium (UE) and system optimum (SO) and discussing how guidance systems can mitigate the inefficiencies arising from self-interested routing behavior. The exploration of ITS-based rerouting strategies demonstrates how system architectures affect congestion detection, information dissemination, and alternative route computation. Finally, the authors discuss how the effectiveness of next-generation route guidance systems will depend on their ability to integrate predictive modeling with real-time adaptability, ensuring optimal route recommendations under changing traffic conditions.

Keywords: route guidance systems, traffic optimization, urban traffic management, intelligent transport systems (ITS) cooperative, connected and automated mobility (CCAM)

1. Introduction

Modern transportation systems are undergoing an important change, driven by the growing need for efficient, safe, and sustainable mobility solutions. Since traffic networks are affected by congestion and travel delays, the integration of decision-support tools and communication technologies has become central. In this context, route guidance systems play a crucial role in improving urban mobility. Specifically, route guidance systems operate at the operational level, providing drivers with real-time information and optimal route suggestions to reduce travel times. These systems can dynamically influence individual travel behavior, responding to changes in network conditions. To determine how such systems

should guide travelers, it is essential to refer to traffic assignment theory, which models how travelers distribute themselves in the network. It distinguishes between the user equilibrium (UE) Assignment, where each driver independently minimizes personal travel time, and the system optimum (SO), where total network efficiency is maximized [1]. By providing real-time traffic information, route guidance systems can influence drivers' decisions to guide the network toward a state closer to the SO condition. ITS and V2X communication technologies enable this through continuous interaction among vehicles, infrastructure, and traffic management centers (TMCs) [2]. Through data exchange, ITS architectures provide the informational backbone that supports dynamic traffic assignment and adaptive route guidance. V2X communications allow vehicles to share information about position, speed, and road conditions directly with one another and with the infrastructure. This feedback loop turns static route guidance into a cooperative and predictive process.

2. Route guidance systems

Vehicle route guidance systems represent a central component of intelligent transportation systems (ITS). Their specific aim is to reduce drivers' travel times, mitigate road segment congestion, and thus increase network efficiency. Over the last few decades, these systems have evolved from simple, rule-based frameworks to more sophisticated models that integrate real-time data and predictive analytics. The most important classifications of these systems fall into three main categories, which reflect different ways of managing uncertainty and information in traffic management: (i) *static* versus *dynamic*, (ii) *stochastic* versus *deterministic*, (iii) *predictive* versus *reactive*, and (iv) *centralized* versus *decentralized*. A comprehensive review and comparison of these classifications is provided by [3].

A static route guidance system relies exclusively on precollected or historical traffic data. In these systems, road conditions are assumed constant during a given analysis period, and no real-time data acquisition occurs. Consequently, optimal routes are calculated based on static maps or fixed travel time databases. In summary, static systems are computationally simple to tackle and infrastructure-independent but lack responsiveness to traffic changes or car crashes. In contrast, dynamic route guidance systems periodically extract real-time traffic information from sensors. These systems continuously update travel times and road conditions, enabling real-time route optimization. The integration of ITS and dynamic systems provides adaptability, higher accuracy, and resilience to traffic changes. However, despite their reactivity, dynamic systems are essentially descriptive: they respond to the current network situation but do not anticipate its future evolution. As a result, route recommendations based only on present conditions may become suboptimal even minutes after they are issued.

This limitation motivates the introduction of more reliable systems, that is, predictive systems. Specifically, they use historical data, machine learning models, or traffic simulations to estimate how road conditions will evolve in the near future. By anticipating congestion or delays, they can provide route suggestions expected to remain efficient even as traffic conditions change. On the other hand, reactive systems respond directly to current traffic data, for example,

accidents and weather conditions, offering immediate adjustments to drivers. Therefore, even though predictive models prove to be effective in stable conditions, reactive ones typically perform better when traffic behavior becomes unpredictable.

Regarding the distinction between stochastic and deterministic systems, it is about how uncertainty is managed. In a deterministic model, all inputs are assumed to be known and constant, for example, travel times, demand patterns, and road capacities. By contrast, stochastic models introduce randomness to reflect the actual uncertainty in human driving behavior, traffic flows, and random disruptions. This makes stochastic models more suitable to reflect realistic guidance conditions.

Path planning can also be classified as centralized or decentralized. Centralized systems use a central system to monitor the entire network and provide route guidance. The aim of these systems is to optimize the overall network performance, but achieving this requires significant infrastructure and user compliance. On the other hand, in decentralized systems, route decisions are made by individual users according to available traffic information. Despite being simpler to implement, decentralized routing may select user-optimal paths that are not optimal from a system-wide perspective.

Bringing these perspectives together, the aim should be to find the right trade-off and, therefore, systems that are predictive enough to anticipate change, reactive enough to adapt quickly, and computationally efficient enough to scale to large networks. **Table 1** provides a summary of the main features emerging from the classification of vehicle route guidance systems.

Classification	Type	Key features	Pros	Cons
Update	Static	Uses only historical data; road conditions are assumed constant.	Simple, low infrastructure	Not adaptive; routes may be suboptimal.
	Dynamic	Updates real-time traffic via sensors.	Adaptive, accurate	Reactive; may become suboptimal
Prediction	Predictive	Estimates future traffic using ML or simulations.	Anticipates congestion	Less effective in unpredictable traffic
	Reactive	Responds to current traffic (e.g., accidents, weather).	Fast reaction	Does not anticipate future issues
Uncertainty	Deterministic	Inputs are assumed to be known and constant.	Simple	Unrealistic for real traffic
	Stochastic	Includes randomness in traffic behavior.	Realistic	More complex
Control	Centralized	Central system guides all routes.	Optimizes network	Requires infrastructure
	Decentralized	Users choose routes individually.	Easy to implement	May not be network-optimal

Table 1.
Vehicle route guidance systems' classifications.

3. Traffic assignments

In transportation planning, the four-step model is a classic framework used to predict travel behavior. This model includes four steps: (i) trip generation, (ii) trip distribution, (iii) mode choice, and (iv) traffic assignment. Each stage builds on the previous one, turning travel demand into traffic flows that describe how many people move across the network in a specific timeframe. Specifically, the traffic assignment phase, which represents the core of our analysis, is particularly crucial because it assigns travel demand, represented by the OD matrix, to trips on a transportation network. Therefore, this phase uses the data collected in previous steps to determine the routes actually used by drivers and the travel time on each segment.

The first attempt to solve the traffic assignment problem is due to [4] who introduced *all-or-nothing assignment* (AoN). Under the AoN assignment, all flow of an OD pair is assigned to the shortest path, implicitly assuming that travel time does not depend on flow. However, this assumption was completely unrealistic because it ignored congestion effects. This led to the development of latency functions, in which the travel time of a road segment depends on the number of vehicles using it. Several formulations have been proposed in the literature, for example, the well-known Bureau of Public Roads (BPR) function, which models arc travel time (t_a) as an increasing and convex function of flow on the arc (f_a) relative to the segment's capacity (C_a):

$$t_a(f_a) = t_a^0 \left[1 + \alpha \left(\frac{f_a}{C_a} \right)^{\beta} \right]. \tag{1}$$

here, t_a^0 denotes the free-flow travel-time on arc a and typical values for the parameters are $\alpha = 0.15$ and $\beta = 4$. Formally, traffic assignment can be described as a constrained optimization problem, where variables represent flows on road segments and paths, constraints ensure demand satisfaction and non-negativity of flows, and the objective function depends on the type of equilibrium to be achieved. Two fundamental concepts, introduced by [1], govern flow distribution: UE and SO. In UE, every driver chooses the route that minimizes their own travel time, given the available paths and current network conditions. As a result, no driver can reduce their travel time by changing routes, and all used routes between an OD pair have the same average travel time. This equilibrium assumes drivers have complete network information and that flows are stable over time.

The SO, on the other hand, represents a condition in which the total travel time across the network is minimized. In this case, individual benefit is not the primary concern; rather, the aim is the collective optimal performance of the system. While, according to Lujak et al. [5], UE can be interpreted as a Nash equilibrium in a game with many players, SO corresponds to a socially optimal flow distribution, which often requires external interventions, such as traffic guidance, regulations, or incentives to direct drivers along routes they would not choose independently.

The difference between UE and SO highlights a key concept in both transportation theory and game theory: the *price of anarchy*. This metric quantifies the inefficiency resulting from individualistic behavior compared to the collective optimum, defined as the ratio between the total travel cost at UE and the total travel cost at SO [5, 6].

In addition to the deterministic formulation, a stochastic version of the User Equilibrium (SUE) was introduced by Sheffi [7], which accounts for drivers' incomplete information and bounded rationality. This assignment model introduces uncertainty in route choice decisions and considers factors such as perceived travel times, delay penalties, and individual preferences. This approach has led to more realistic and robust models capable of capturing the complexity of real-world behavior, including expected utility-based models [8], late arrival penalty models [9], and fuzzy decision models [10].

In summary, the traffic assignment is a key step in transportation planning. In particular, analyzing UE and SO, together with quantifying the price of anarchy, provides theoretical and practical tools to evaluate traffic management policies and design interventions aimed at improving overall system performance. In this regard, Morandi [11] provided an overview of state-of-the-art methodologies that integrate principles of user fairness with network efficiency to tackle traffic congestion.

Another crucial aspect relative to SO, or more generally to strategies aimed at improving network efficiency, is the concept of user compliance. This issue becomes particularly relevant when dealing with human-driven vehicles that might deviate from system-optimal recommendations. In this context, travelers can decide their own routes based on personal preferences, perceived conditions, and, importantly, how information is delivered to them [12, 13]. In fact, although full compliance may be assumed for self-driving vehicles, the coexistence with human-driven vehicles will keep traffic networks hybrid for the near future. Therefore, ensuring that the strategies proposed to users are perceived as fair and that information is provided in a reliable way will be essential to ensure users' trust and encourage cooperative behavior. In this context, it becomes essential to understand how to provide information effectively and through which channels, highlighting the role of ITS in supporting route guidance for travelers. A comprehensive overview of these systems and their integration to improve network efficiency is presented in Section 4.

4. Intelligent transport systems

4.1 Overview and classification of ITS

ITS are becoming essential tools in improving urban mobility and reducing congestion. Modern ITS use real-time data collected from vehicles, infrastructure, and travelers, integrating architectures to enable dynamic traffic management. The architecture of ITS is typically multilayered, including a facilities layer that provides applications and user services, a networking and transportation layer that manages data flow and communication protocols, and an access layer that ensures physical message transmission. ITS operate as integrated systems composed of three main components: data generation and processing, data recording and storage, and intelligent decision-support modules. Furthermore, ITS represents one of the main components of the Traffic Management System (TMS), primarily responsible for enhancing traffic mobility. In particular, TMS collects real-time data from various sources and integrates it within the TMC. ITS applications can be classified as follows:

- Advanced public transportation system (APTS): provides real-time information to public transport users, supporting better travel decisions.
- Advanced traveler information system (ATIS): provides route, travel time, and mode selection data directly to travelers.
- Advanced traffic management system (ATMS): manages traffic flow to optimize mobility.
- Automated highway system: enables the automatic control of vehicle steering, braking, and acceleration.
- Incident management system: issues alerts and warnings about accidents or other disruptions through variable message signs (VMS).
- Commercial vehicle control (CVC): manages, for instance, fleet management and safety monitoring.

Furthermore, ITS can also be classified according to their physical architecture, particularly with respect to the communication systems used among the physical entities, which may be centralized, distributed, and hybrid [2].

4.2 Technologies for ITS

ITS rely on a wide variety of technologies for data collection and dissemination. Specifically, traffic data can be collected and processed through several approaches: (i) infrastructure-based, (ii) vehicle-based, (iii) commuter-based, and (iv) geographical-area-based. Infrastructure-based methods employ vision-based, laser-based, and ultrasonic sensors, as well as microwave radars and CCTV cameras to monitor real-time traffic conditions without interrupting vehicle movement. These technologies offer wide coverage and structured data, although they are costly, require maintenance, and can be affected by environmental conditions. Vehicle-based approaches rely on GPS-equipped on-board units (OBUs) and wireless communication technologies such as DSRC-WAVE to enable V2X interactions. In this context, probe vehicles can provide real-time traffic information across wide areas, although the accuracy of GPS and dependency on onboard technology can pose limitations. Commuter-based systems, including mobile applications, for example, Waze, instead use travelers' locations to predict changes in traffic flow. However, their reliability is limited because their accuracy depends on the coverage and the number of users using these devices. Moreover, their precision in detecting locations is quite low, and the data they provide are semi-structured. Finally, geospatial methods, such as photogrammetry, enable large-scale traffic flow and speed monitoring, which proves to be particularly useful for incident management. For more details on the classification of ITS architectures, refer to the review by [2].

4.3 Rerouting strategies in ITS

Rerouting strategies are a core component of ITS, aimed at mitigating traffic congestion by redistributing vehicle flows in real time. The algorithms used for

congestion detection and alternative route computation depend on the architecture of the system. Specifically, the ITS architectures can be classified as centralized, distributed, or hybrid. According to this classification, various approaches are presented in detail in Sects. 4.3.1 and 4.3.2. Despite the variety of methods, most rerouting mechanisms share a common operational structure that includes four essential steps: traffic data collection, congestion detection, vehicle selection for rerouting, and alternative route computation. The first phase concerns the collection and representation of traffic information. Vehicles, roadside units (RSUs), or fixed sensors transmit real-time data such as position, speed, destination, and travel times. This information represents the input for congestion detection, which constitutes the next step. Depending on the system, congestion can be identified using different methods [14]: (i) machine learning classifiers, for example, K-nearest neighbors (KNN) or artificial neural networks (ANN), (ii) fuzzy logic, or (iii) methods based on speed and vehicle density analysis. Once congestion is detected, the system selects the vehicles to be rerouted, often prioritizing those whose rerouting would most effectively alleviate network congestion. Finally, alternative routes are computed using various algorithms, ranging from k-shortest paths to more sophisticated methods such as probabilistic algorithms or entropy-based heuristics. In the rerouting phase, several technologies and methods are employed to implement these strategies, including agent-based models, neural and fuzzy-neural networks, VANETs, cellular automata, rule-based reasoning, peer-to-peer communication, and wireless sensor networks [15]. Among these, vehicular ad hoc networks (VANETs) play a particularly important role. VANETs create short-range, ad-hoc communication networks among vehicles, enabling real-time data exchange for traffic management, route optimization, and safety applications [16]. They rely on vehicle-to-vehicle (V2V) communication for direct interactions between nearby vehicles, vehicle-to-infrastructure (V2I) communication to connect vehicles with RSUs or traffic control centers, and vehicle-to-everything (V2X) communication to extend coverage to vehicles outside the immediate range through multihop data forwarding. VANETs typically use dedicated short-range communications (DSRC) operating in the 5.85–5.925 GHz band with the IEEE 802.11p protocol (also known as wireless access for vehicular environments, WAVE) and are increasingly integrating technologies such as visible light communication (VLC). By providing low-latency and high-speed communication, VANETs support a wide range of applications, including collision avoidance, platooning, smart routing, and traffic optimization.

4.3.1 Centralized systems

In centralized systems, a central server or traffic management center monitors traffic conditions of the overall network and provides rerouting strategies. The most commonly used rerouting algorithms in this context are [17]: (i) the dynamic shortest path (DSP), (ii) random k-shortest paths (RkSP), and (iii) entropy-based k-shortest paths (EBkSP). In the DSP approach, each vehicle is assigned the current shortest path to its destination based on travel time or distance. However, it may accidentally shift congestion to other subnetworks, as it does not take into account the overall effect of rerouted vehicles. The RkSP method generates multiple candidate paths (k paths) for each vehicle and randomly assigns one. This reduces the likelihood of overcrowding a single route. However, the selected path may not be optimal in terms of travel time, introducing potential inefficiencies. Finally, EBkSP

improves the previous strategies by selecting the fewer flow routes based on an entropy metric, taking into account predicted future traffic loads. EBkSP generally achieves superior load balancing and reduces rerouting frequency. Simulation studies over urban road networks [17] have shown that all three strategies significantly reduce average travel time. DSP provides the fastest computation, while EBkSP has the best overall performance, improving travel times by up to 104% compared to a no-rerouting scenario and decreasing rerouting frequency by 34% relative to other methods. Very importantly, these strategies remain effective even with low driver compliance and low penetration rates.

Another approach, known as adaptive next road rerouting (a-NRR), was introduced by Wang et al. [18] for urban traffic congestion mitigation. This strategy takes the data collected by RSUs at intersections as input and, rather than providing a complete route to the destination, suggests the next optimal road segment for each vehicle. In addition, the RSUs communicate with a traffic operation center (TOC), which processes the data and sends relevant updates back to the RSUs near congested areas. These RSUs then deliver alerts to drivers, indicating whether a specific route should be avoided to prevent delays.

In the last decades, centralized systems started using machine learning techniques for congestion detection and rerouting. For instance, the SCORPION (a solution using cooperative rerouting to prevent congestion and improve traffic condition) system [19] employs a KNN classifier using average road speed as input to identify congested roads and reroutes vehicles through a cooperative greedy algorithm, which assigns them to the lowest-weighted roads while periodically updating the system to reflect current conditions. However, despite being effective in rapidly reducing local congestion, SCORPION may not ensure optimal global traffic flows. Congestion avoidance through a traffic classification mechanism and a rerouting algorithm (CHIMERA) system [20] extends this approach by implementing a probabilistic k-shortest path algorithm, distributing traffic more evenly across the network and reducing the likelihood of bottleneck buildup. Both approaches use V2I communications.

4.3.2 Distributed and hybrid systems

Many researchers have proposed rerouting methods based on distributed and hybrid architectures for ITS. These systems mainly rely on V2V and V2I communications.

Early distributed systems, such as SOTIS (a self-organizing traffic information system) [21], employ V2V communication to share local traffic flow and vehicle position data. SOTIS uses a store-carry-forward mechanism to deliver information in different areas. However, its effectiveness is limited by high message overhead, which can reduce system scalability. CoTEC (COperative Traffic congestion detECtion) [22] introduced a cooperative congestion detection framework using fuzzy logic. This system periodically broadcasts beacon or cooperative awareness (CAM) messages and evaluates congestion levels based on the level of service (LOS) from the highway capacity manual (HCM). When congestion is identified, vehicles can locally adjust their routes. It represents an early example of cooperative rerouting based on disseminated information. CARTIM (Cooperative vehiculAR Traffic congestion Identification and Minimization) [23] extends this concept by combining congestion detection and rerouting. Vehicles periodically transmit speed

and density data via beacon messages. Using fuzzy logic, the system identifies congested areas and suggests alternative routes to reduce travel time. To limit communication overhead, CARTIM reduces reliance on CAM messages, balancing information dissemination with rerouting effectiveness. Additionally, by optimizing traffic flow, CARTIM contributes to lowering carbon emissions. Several protocols specifically address efficient information dissemination, which is critical for rerouting. For example, DRIFT [24] uses V2V communication to broadcast accident warnings while mitigating broadcast storm issues. Vehicles receiving these alerts can reroute to avoid congested areas, reducing travel time and fuel consumption. More recent distributed systems are FASTER [25] and PANDORA (Preventing trAffic congestioN through a fully Distributed Rerouting Algorithm) [26]. FASTER divides the network into districts using the k-means clustering algorithm. Vehicles share local traffic information via beacon messages, and strategically selected nodes broadcast aggregated district knowledge to enable network-wide rerouting decisions using probabilistic shortest-path algorithms [27]. CRONOS introduced a protocol for data dissemination based on metrics of complex networks. It enhances dissemination efficiency by selecting relay nodes based on degree and betweenness centrality, providing high coverage while minimizing overhead.

Hybrid systems further integrate V2I communication to enable a collaborative and proactive rerouting. DIVERT (DIstributed VEhicular Re-rouTing system) [28] computes alternative paths for individual vehicles while ensuring user privacy and reducing server load. However, its performance is slightly worse than centralized ITS systems. FnS (Faster and Safer) [29] provides rerouting recommendations by combining V2V and V2I communication with information on congested and unsafe areas for pedestrians and drivers. ICARUS [30] is a hybrid ITS framework that integrates information from heterogeneous sources, for example, accident alerts, weather conditions, and congestion predictions, to support both proactive and reactive rerouting. When vehicles detect or receive warnings about unusual events via V2V communication, those affected request alternative routes from a central server through V2I communication. ECODE (Efficient road COngestion DEtection protocol) [31] is a geocast-based congestion detection and rerouting system that uses RSUs at intersections and multihop V2V communication to share traffic data. Vehicles aggregate local information about speed and flow and send it to the nearest RSU, which computes optimal routes. Additionally, RSUs provide a RecomReport with updated traffic and routing information.

4.3.3 Comparison between centralized, distributed, and hybrid ITS systems

As previously discussed, route guidance in transportation networks can be implemented through different architectural structures. In this subsection, we analyze the advantages and limitations of centralized, distributed, and hybrid systems, discussing when each architecture is most suitable depending on network scale, data load, latency requirements, and operational context. Centralized architectures are based on a central system that collects real-time traffic data, computes routes for the entire network, and delivers individual route instructions to vehicles [3]. By considering system-wide objectives, centralized systems achieve higher network throughput and more effective congestion control compared to distributed systems. However, centralized systems are constrained by limited scalability, since vehicles must constantly exchange data with the central system,

which in turn has to process a large volume of information [2]. Thus, centralized systems ensure global traffic optimization but require significant computational resources from the infrastructure [3]. As noted by Polydoros et al. [32], a centralized architecture also requires higher communication overhead than a decentralized or distributed one. Another concern is that a central entity may also become a single point of failure [33]. On the other hand, distributed architectures involve multiple local agents or vehicles communicating directly via V2V communication, enabling decentralized decision-making [2]. Moreover, these systems are scalable, exhibit lower latency, and are robust against failures or measurement errors [33, 34]. However, distributed ITS can suffer from limited coverage, broadcast storms, and challenges in handling complex road segments. Probabilistic or delay-based methods are often used to mitigate these issues, but global optimality cannot be guaranteed [2]. Hybrid architectures combine centralized global optimization with distributed local decision-making. A central controller provides high-level traffic strategies, while local agents or vehicles respond to real-time conditions [2]. This approach increases coverage through roadside infrastructure and multihop communication, reducing latency and improving robustness compared to purely centralized systems. Nevertheless, hybrid models face challenges in selecting vehicles for data dissemination in highly dynamic networks and cannot always guarantee globally optimal routing to avoid congestion. Hybrid systems are generally the most effective choice for large-scale heterogeneous networks where neither centralization nor distribution alone can meet scalability and optimization requirements. However, despite their differences and the specific ITS architecture in which they are implemented, all route guidance systems share a common problem, that is, user compliance. The effectiveness of any guidance system depends on how well drivers follow the suggested routes [3]. In centralized systems, low compliance may affect the optimization strategies defined by the central controller. In distributed systems, deviations by some users can disrupt local coordination and slow down the system's ability to reach optimal traffic patterns. Hybrid systems face a similar issue, as they need to balance global instructions with local decision-making. In short, regardless of the architecture, the compliance rate directly affects how well a route guidance system performs.

Table 2. Comparison between centralized, distributed, and hybrid architectures.

To conclude this comparison, **Figure 1** summarizes how information flows and which communication mechanisms are adopted in ITS systems according to their architecture.

Architecture	Pros	Cons	Best use-case
Centralized	Global optimization, coordinated routing	High computation and latency	Medium networks, strong infrastructure
Distributed	Scalable, low latency, low cost	Suboptimal globally	Large dynamic networks, fast decisions
Hybrid	Balanced performance, robust and scalable	Higher design complexity	Large heterogeneous systems, mixed conditions

Table 2
provides a brief summary of the main advantages, disadvantages, and best use cases of each architecture.

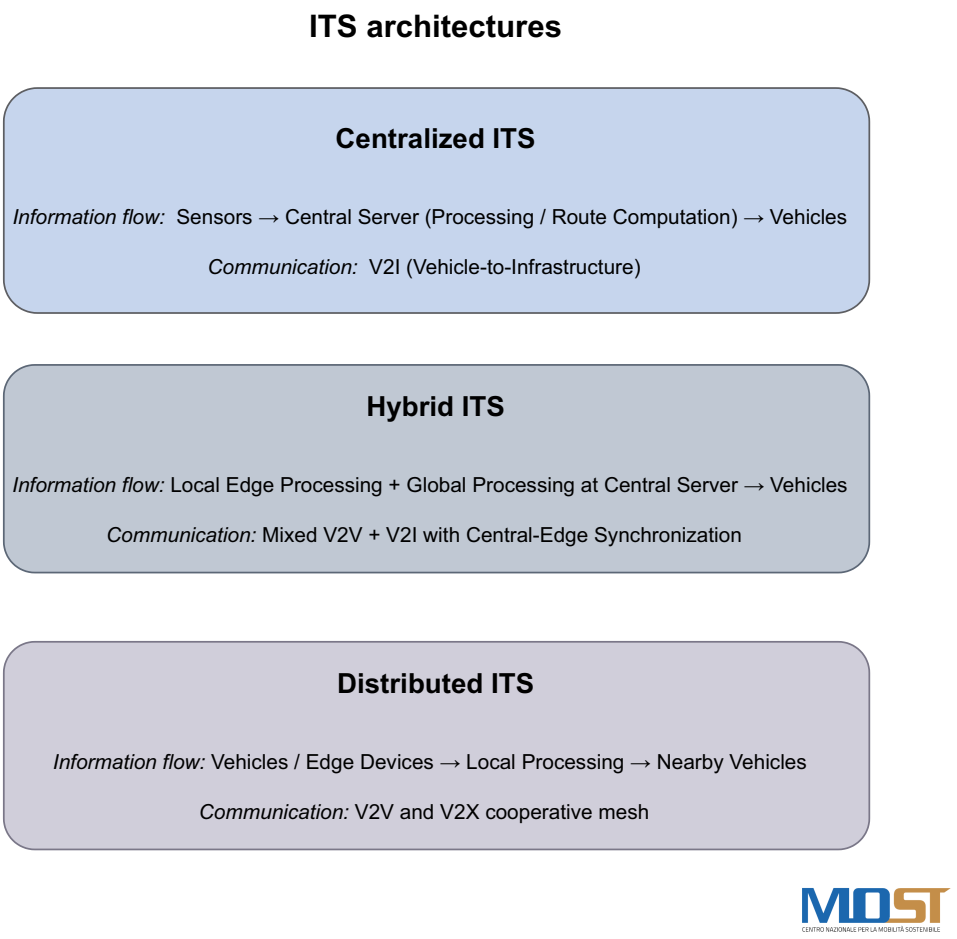


Figure 1.
Information flow and communication in centralized, distributed, and hybrid architectures.

5. Conclusions

This chapter has reviewed the evolution and classification of vehicle route guidance systems within the framework of ITS. The discussion concerned how the progressive integration of real-time technologies and data-driven modeling has transformed route guidance systems from static to adaptive, predictive, and cooperative.

From a methodological perspective, four main dimensions, that is, (i) temporal perspective (static vs. dynamic), (ii) uncertainty management (deterministic vs. stochastic), (iii) information response (predictive vs. reactive), and (iv) control structure (centralized vs. decentralized), provide a conceptual basis to compare system designs. While static and deterministic models offer computational tractability and minimal infrastructure requirements, they fail to capture the temporal and behavioral variability of real traffic. By contrast, dynamic and stochastic systems can better reflect user responsiveness at the cost of higher

complexity and data requirements. Achieving a functional trade-off among these properties remains an important challenge in modern route guidance systems.

The chapter also establishes the link between route guidance methods and traffic assignment theory, describing the theoretical aspects underlying the UE and SO principles. The aim is to balance these two principles, that is, individual rationality, represented by UE, and network efficiency, represented by SO, whose divergence can be quantified by the Price of Anarchy. In this context, route guidance systems act as mechanisms to reduce the inefficiencies caused by self-interested behavior. In addition, user compliance and fairness perception emerge as critical factors that affect the effectiveness of system-optimal strategies in hybrid networks combining human-driven and self-driven vehicles.

The review of ITS rerouting strategies demonstrated that system architectures (whether centralized, distributed, or hybrid) determine how congestion is detected, information is disseminated, and alternative routes are computed. For example, centralized approaches, such as DSP, RkSP, and EBkSP algorithms, use traffic information to achieve network-wide optimization but face scalability and latency limitations. Distributed methods, relying on V2V and V2I communications, enable local decision-making through cooperative data exchange, fuzzy logic, and probabilistic rerouting. As a result, they ensure greater adaptability and robustness. Hybrid systems, for example, DIVERT, ICARUS, and ECODE, combine the coordination of centralized control with the flexibility of decentralized communication, representing the most promising avenue toward scalable and resilient traffic management.

In conclusion, the effectiveness of next-generation route guidance systems will depend on their ability to combine predictive modeling with real-time adaptability, ensuring that route recommendations remain optimal under changes in traffic conditions. Furthermore, the integration of machine learning techniques is expected to evolve from reactive congestion mitigation to proactive and cooperative solutions. Looking ahead, several promising research avenues remain open. In particular, edge computing can enable low-latency decision-making directly at the network edge, while digital twins may allow real-time simulation and evaluation of traffic scenarios before deployment. Moreover, reinforcement learning-based cooperative routing represents a key opportunity for self-adaptive and scalable decision-making. Exploring how these tools can be combined into a unified framework is essential for designing ITS that can address the challenges of complex urban environments.

Acknowledgment

This study was carried out within the MOST – Sustainable Mobility National Research Centre and received funding from the European Union Next-GenerationEU (PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR) – MISSIONE 4 COMPONENTE 2, INVESTIMENTO 1.4 – D.D. 1033 17/06/2022, CN00000023). This manuscript reflects only the authors' views and opinions; neither the European Union nor the European Commission can be considered responsible for them.

Conflict of Interest

The authors declare no conflict of interest.

Author details

Anna Laura Pala[1,2*] and Giuseppe Stecca[2]

1 DIAG, Sapienza University of Rome, Rome, Italy

2 National Research Council, Institute of Systems Analysis and Computer Science "Antonio Ruberti," Rome, Italy

*Address all correspondence to: pala@diag.uniroma1.it

IntechOpen

© 2025 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] Wardrop JG. Road paper. some theoretical aspects of road traffic research. Proceedings of the Institution of Civil Engineers. 1952;**1**(3):325–362

[2] Sharma S, Awasthi SK. Introduction to intelligent transportation system: Overview, classification based on physical architecture, and challenges. International Journal of Sensor Networks. 2022;**38**(4):215–240

[3] Schmitt E. Vehicle route guidance systems: Classification and comparison. In: 2006 IEEE Intelligent Transportation Systems Conference. IEEE; 2006. p. 242–247

[4] Campbell ME. Route selection and traffic assignment: A compendium of correspondence relating to a suggested technique. Highway Research Board. 1950

[5] Lujak M, Giordani S, Ossowski S. Route guidance: Bridging system and user optimization in traffic assignment. Neurocomputing. 2015;**151**:449–460

[6] Jahn O, Möhring RH, Schulz AS, Stier-Moses NE. System-optimal routing of traffic flows with user constraints in networks with congestion. Operations Research. 2005;**53**(4):600–616

[7] Sheffi Y. Urban Transportation Networks. Vol. **6**. Englewood Cliffs, NJ: Prentice-Hall; 1985

[8] Mirchandani P, Soroush H. Generalized traffic equilibrium with probabilistic travel times and perceptions. Transportation Science. 1987;**21**(3):133–152

[9] Watling D. User equilibrium traffic network assignment with stochastic travel times and late arrival penalty. European Journal of Operational Research. 2006;**175**(3):1539–1556

[10] Miralinaghi M, Lou Y, Hsu Y-T, Shabanpour R, Shafahi Y. Multiclass fuzzy user equilibrium with endogenous membership functions and risk-taking behaviors. Journal of Advanced Transportation. 2016;**50**(8):1716–1734

[11] Morandi V. Bridging the user equilibrium and the system optimum in static traffic assignment: A review. 4or. 2024;**22**(1):89–119

[12] Ben-Elia E, Di Pace R, Bifulco GN, Shiftan Y. The impact of travel information's accuracy on route-choice. Transportation Research Part C: Emerging Technologies. 2013; **26**:146–159

[13] Di Pace R, Bruno F, Bifulco GN, De Luca S. Modelling travellers' behaviour in a route choice experiment with information under uncertainty: Calibration, validation, and further refinements. Transportation Letters. 2023;**15**(3):211–226

[14] Bhandari A, Patel V, Patel M. A survey on traffic congestion detection and rerouting strategies. In: 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI). IEEE; 2018. p. 42–44

[15] Khanjary M, Hashemi SM. Route guidance systems: Review and classification. In: Proceedings of the 6th Euro American Conference on Telematics and Information Systems; 2012. p. 269–275

[16] De Souza AM, Brennand CA, Yokoyama RS, Donato EA, Madeira ER, Villas LA. Traffic management systems: A classification, review, challenges, and future perspectives. International Journal of Distributed Sensor Networks. 2017;**13**(4):1550147716683612

[17] Pan J, Khan MA, Popa IS, Zeitouni K, Borcea C. Proactive vehicle re-routing strategies for congestion avoidance. In: 2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems. IEEE; 2012. p. 265–272

[18] Wang S, Djahel S, McManis J. An adaptive and VANETs-based Next Road Re-routing system for unexpected urban traffic congestion avoidance. In: 2015 IEEE vehicular networking conference (VNC). IEEE; 2015. p. 196–203

[19] de Souza AM, Yokoyama RS, Botega LC, Meneguette RI, LA V. Scorpion: A solution using cooperative rerouting to prevent congestion and improve traffic condition. In: 2015 IEEE international conference on computer and information technology; ubiquitous computing and communications; dependable, autonomic and secure computing; pervasive intelligence and computing. IEEE; 2015. p. 497–503

[20] De Souza AM, Yokoyama RS, Maia G, Loureiro A, Villas L. Real-time path planning to prevent traffic jam through an intelligent transportation system. In: 2016 IEEE symposium on computers and communication (ISCC). IEEE; 2016. p. 726–731

[21] Wischoff L, Ebner A, Rohling H, Lott M, Halfmann R. SOTIS - a self-organizing traffic information system. In: The 57th IEEE Semiannual Vehicular Technology Conference, 2003. VTC 2003-Spring. **4**; 2003. p. 2442–2446

[22] Bauza R, Gozálvez J. Traffic congestion detection in large-scale scenarios using vehicle-to-vehicle communications. Journal of Network and Computer Applications. 2013;**36**(5):1295–1307

[23] Araújo GB, Queiroz MM, Duarte-Figueiredo Fd LP, Tostes AIJ, Aaf L. CARTIM: A proposal toward identification and minimization of vehicular traffic congestion for VANET. In: 2014 IEEE Symposium on Computers and Communications (ISCC); 2014. p. 1–6

[24] Villas LA, de Andrade TP, da Fonseca NL. An efficient and robust protocol to disseminate data in highway environments with different traffic conditions. In: 2014 IEEE symposium on computers and communications (ISCC). IEEE; 2014. p. 1–6

[25] de Souza AM, Villas LA. A fully-distributed traffic management system to improve the overall traffic efficiency. In: Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems. MSWiM '16. New York, NY, USA: Association for Computing Machinery; 2016. p. 19–26. DOI: 10.1145/2988287.2989167

[26] de Souza AM, da Fonseca NLS, Villas L. A fully-distributed advanced traffic management system based on opportunistic content sharing. In: 2017 IEEE International Conference on Communications (ICC); 2017. p. 1–6

[27] Costa J, Rosário D, de Souza AM, Villas LA, Cerqueira E. Data dissemination based on complex networks' metrics for distributed traffic

management systems. In: 2018 IEEE Symposium on Computers and Communications (ISCC); 2018. p. 01062–7

[28] Pan J, Popa IS, Borcea C.Divert: A distributed vehicular traffic re-routing system for congestion avoidance. IEEE Transactions on Mobile Computing. 2017;**16**(1):58–72

[29] de Souza AM, Botega LC, LA V. Fns: Enhancing traffic mobility and public safety based on a hybrid transportation system. In: 2018 14th International Conference on Distributed Computing in Sensor Systems (DCOSS). Ieee; 2018. p. 77–84

[30] de Souza AM, Yokoyama RS, Boukerche A, Maia G, Cerqueira E, Loureiro AA, et al. ICARUS: Improvement of traffic Condition through an Alerting and Re-routing System. Computer Networks. 2016;**110**:118–132

[31] Younes MB, Boukerche A. Efficient traffic congestion detection protocol for next generation vanets. In: 2013 IEEE international conference on communications (ICC). IEEE; 2013. p. 3764–3768

[32] Polydoros A, Dessouky K, Pereira J, Sun C, Lee K, Papavassiliou TD, et al. Vehicle to roadside communications study. PATH Research Report. 1993

[33] Sommer M, Tomforde S, Hähner J. Forecast-augmented route guidance in urban traffic networks based on infrastructure observations. In: Proceedings of the VEHITS 2016 - International Conference on Vehicle Technology and Intelligent Transport Systems; 2016

[34] Zuurbier FS, van Lint J, van Zuylen H. Comparison study of decentralized feedback strategies for route guidance purposes. In Sino-Dutch Joint Seminar on Traffic and Transport Theory. Nanjing, China; 2007. p. 100–114. TRAIL research school/School of transportation of SEU research school



Edited by Stefano de Luca, Roberta Di Pace, Facundo Storani and Francesca Bruno

The book aims to analyze, develop, and validate approaches, methodological tools, and procedures for testing Cooperative, Connected, and Automated Mobility (CCAM). It brings together contributions that present innovative control and analytical methods based on next-generation intelligent transportation systems, with the aim of advancing scientific and technological knowledge and providing methodological support to stakeholders involved in defining strategies, technical standards, and guidelines for future mobility. The volume integrates both review and methodological contributions, focusing on traffic optimization strategies, technological solutions, analytical frameworks, safety and security issues, and future market perspectives. It also includes assessments of the potential positive and negative impacts on transport system performance, environmental sustainability, safety, and equity. The book is structured into four interconnected sections, each addressing a key dimension of the evolving ecosystem of connected, cooperative, and automated mobility. Section I focuses on frameworks and strategy issues and brings together contributions that define roadmaps, governance models, and policy directions. Section II investigated security and resilience issues, exploring the cybersecurity threats, system vulnerabilities, and resilience strategies to safeguard both physical and digital components against malicious actors. Section III explores human factors and trust, investigating the interaction between users and technology through acceptance dynamics and the conditions under which trust in automated and connected systems can be established and maintained. Section IV (extends previously introduced perspectives to real-world contexts, presenting applied studies and experimental evidence on how advanced technologies can be implemented in practice, bridging the gap between theory and deployment). The sections offer a comprehensive, multidisciplinary perspective, combining strategic, technological, and human-centered perspectives to support the development of safe, resilient, and user-oriented mobility systems.

Assed Haddad, Civil Engineering Series Editor

ISSN 3029-0287
ISBN 978-1-83635-540-3

Published in London, UK
© 2026 IntechOpen
© Jarwis / iStock

IntechOpen

