Safeguarding Connected Autonomous Vehicle Communication: Protocols, Intra- and Inter-Vehicular Attacks and Defenses

Mohammed Aledhari[a], Rehma Razzak[b], Mohamed Rahouti[c], Abbas Yazdinejad[d], Reza M.Parizi[e], Basheer Qolomany[f], Mohsen Guizani[g], Junaid Qadir[h], Ala Al-Fuqaha[i]

[a]*Department of Data Science, University of North Texas, Denton, TX, 76207, USA, mohammed.aledhari@unt.edu*

[b]*College of Computing and Software Engineering, Kennesaw State University, Marietta, GA, 30060, USA, rrazzak@students.kennesaw.edu*

[c]*Department of Computer and Information Science, Fordham University, New York, NY, 10023, USA, mrahouti@fordham.edu*

[d]*Cyber Science Lab, Canada Cyber Foundry, University of Guelph, N1G4S7, ON, Canada, ayazdine@uoguelph.ca*

[e]*Decentralized Science Lab, Kennesaw State University, GA, USA, rparizi1@kennesaw.edu*

[f]*Department of Medicine, College of Medicine, Howard University, Washington, DC, 20059, USA, basheer.qolomany@howard.edu*

[g]*Machine Learning Department, Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), Abu Dhabi, UAE, mguizani@ieee.org*

[h]*Computer Science and Engineering Department, Qatar University, Doha, Qatar, jqadir@qu.edu.qa*

[i]*Information and Computing Technologies (ICT) Division, College of Science and Engineering (CSE), Hamad Bin Khalifa University, Doha, Qatar, aalfuqaha@hbku.edu.qa*

Abstract

The advancements in autonomous driving technology, coupled with the growing interest from automotive manufacturers and tech companies, suggest a rising adoption of Connected Autonomous Vehicles (CAVs) in the near future. Despite some evidence of higher accident rates in AVs, these incidents tend to result in less severe injuries compared to traditional vehicles due to cooperative safety measures. However, the increased complexity of CAV systems exposes them to significant security vulnerabilities, potentially compromising their performance and communication integrity. This paper contributes by presenting a detailed analysis of existing security frameworks and protocols, focusing on intra- and inter-vehicle communications. We systematically evaluate the effectiveness of these frameworks in addressing known vulnerabilities and propose a set of best practices for enhancing CAV communication security. The paper also provides a comprehensive taxonomy of attack vectors in CAV ecosystems and suggests future research directions for designing more robust security mechanisms. Our key contributions include the development of a new classification system for CAV security threats, the proposal of practical security protocols, and the introduction of use cases that demonstrate how these protocols can be integrated into real-world CAV applications. These insights are crucial for advancing secure CAV adoption and ensuring the safe integration of autonomous vehicles into intelligent transportation systems.

1. Introduction

Connected Autonomous Vehicles (CAVs) are a progression of various forms of autonomous technology [1]. CAVs enable vehicles to navigate from source to destination with limited or no human involvement, providing significant advancements in automation and connectivity. Self-driving cars can be categorized into several levels of autonomy, ranging from 0 to 5 [2]. At each level, the CAV gains more autonomous properties, with Level 0 being fully human-controlled, and Level 5 representing full automation without human input [3], [4]. While connectivity and automation are distinct aspects of CAVs, they often overlap, leading to complex communication requirements between vehicles and infrastructure. Figure 1 illustrates these differences and overlaps. CAVs promise numerous benefits, notably enhancing transportation safety and efficiency [5]. However, they also introduce significant security challenges, particularly in managing communication and control systems that involve sensing, computing, and vehicular inter-/intra-communication [6].
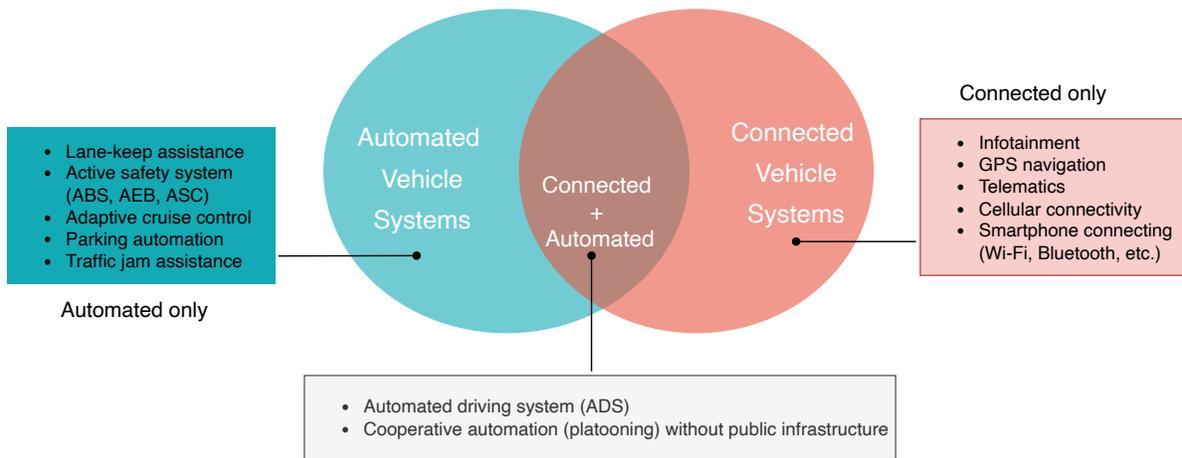

Figure 1: Connected Autonomous Vehicle (CAV) infrastructure.

CAVs have been the target of various cyberattacks, particularly against critical vehicular systems such as sensors, GPS, and control units. Over 126 cyber incidents have been reported against autonomous vehicles [7]. For example, the Nissan Leaf's mobile app vulnerability allowed hackers to access its heater and battery systems, leading to the app's shutdown [8]. Similarly, hackers have exploited vulnerabilities in BMW and Tesla vehicles, causing malfunctions and safety risks [7]. These attacks highlight the growing threat to CAV communication systems, especially those responsible for self-driving decision-making.

Securing CAVs remains a critical and open challenge [9]. The complexity of CAVs, combined with their reliance on multiple interconnected systems, increases their vulnerability to cyberattacks. Ensuring the secure operation of these vehicles requires robust legal and technical frameworks. Currently, there are no specific regulations mandating cybersecurity for CAVs [10]. As the amount of software in vehicles grows, so too does the potential attack surface, making it essential to implement advanced security measures throughout the design and operation of CAVs. Hackers can disrupt safety-critical systems, leading to severe consequences, such as loss of control and traffic accidents [11]. Figure 2 provides an overview of potential attack surfaces in CAVs.
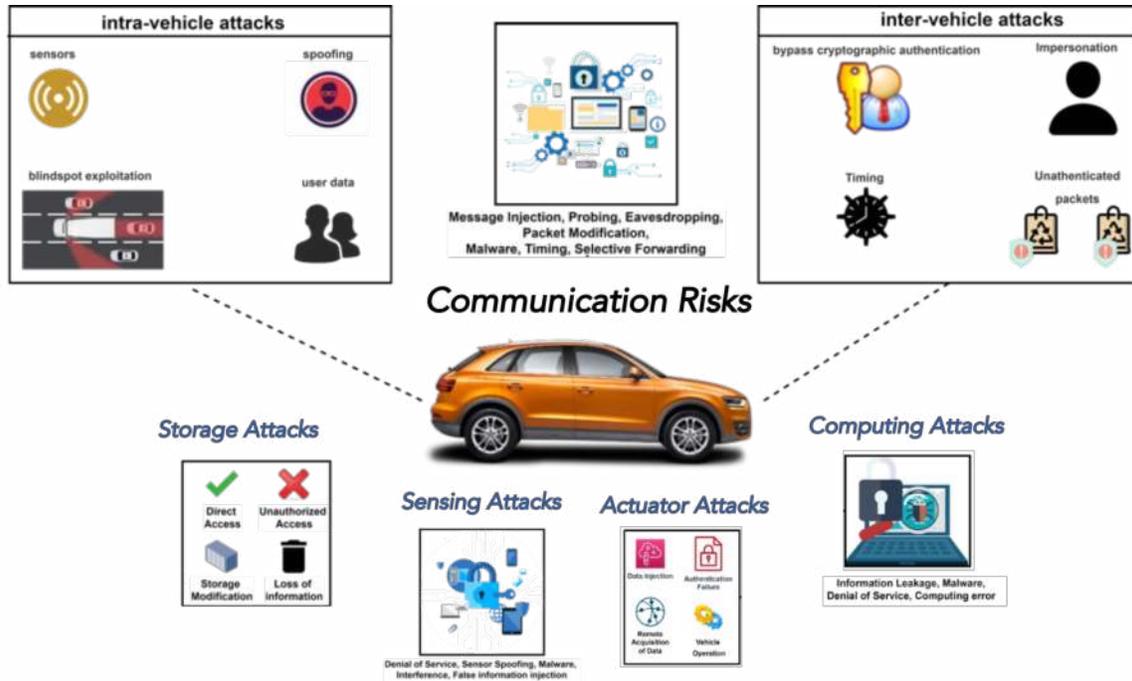
Figure 2: Attack surface in CAVs. *Top: communication risks (intra-vehicular and inter-vehicular attack).*

CAV communication faces numerous threats, including attacks on Vehicle-to-Vehicle (V2V) and Intra-vehicle communication systems. Inter-vehicle communication shares data about traffic, accidents, and road conditions [12], while Intra-vehicle communication relays information between sensors and control units [13]. Both systems are vulnerable to eaves-dropping, spoofing, man-in-the-middle attacks, and more. Recent incidents involving BMW and Tesla vehicles have exposed these vulnerabilities, leading to unauthorized control and unpredictable behaviors such as sudden braking or lane changes [14].

These examples prove how crucial it is to distinguish between what type of attack has occurred to mitigate it and properly prevent its future occurrences [15, 16, 17]. Identifying certain types of attacks can be difficult as they may target the overall infrastructure of the CAV [18]. Classification of attacks on CAVs is of critical importance as each attack can be associated with its own working mechanisms [19], [20]. To rectify this, we would first need to identify the most common attack vectors. Attack vectors are means by which hackers gain access, and a single incident can include multiple attack vectors. A report done by Upstream revealed that the most common attack vectors for CAVs included servers, keyless entry systems, and mobile apps. Additionally, the OBD (On-board Diagnostics) port, IT networks, sensors, and infotainment systems were also among the most common attack vectors for CAVs. Another unsettling discovery from the Upstream Report was that at least 80% of the attacks against CAVs were remote. This concern has still not been properly addressed because remote attacks against CAVs are harder to prevent and can lead to significantly more damage. Another step would be to categorize the attacks on CAVs in severity. A categorization of these attacks comes from the ISO/SAE 21434 standard, which requires vehicle manufacturers and suppliers to ensure that cybersecurity risks are managed efficiently and effectively. This standard contains the Threat Analysis and Risk Assessment

(TARA), which determines the extent to which a road user can be impacted by automotive cyber threats and vulnerabilities. The ISO/SAE 21434 standard also explains that one way to determine this is to use the CVSS 3.X (Common Vulnerability Scoring System) exploitability score, which has values that range between 0.12 (very low) and 3.89 (high).

Furthermore, traditional security solutions cannot be directly applied to CAV communication due to the following reasons:

- The number of software gradually increases in CAVs, which requires higher levels of security built into the vehicular technology from the ground up.

- CAVs share and exchange a high volume of data and decision-making-specific messages by accessing a digital infrastructure involving access to the public Internet. This information sharing, including personal data, can potentially broaden the range of security vulnerabilities in CAVs' communications.

- The ability to use traditional encryption and authentication solutions (from other industries) in CAVs is restricted as they impose unique requirements and limitations.

- Traditional intrusion detection systems (IDSs) typically deploy static analysis approaches, which could be inefficient in defending against the deformation of security attacks when exposing security loopholes.

- The enabling of third-party apps in CAVs is continuously increasing, making it challenging to ensure communication security due to the absence of security by design.

- Traditional Machine Learning (ML)–based attack detection solutions typically rely on conventional feedback controllers and can potentially degrade driving safety by generating inaccurate decisions over the varied road conditions and traffic dynamics.

To alleviate potential security threats, countermeasures must be implemented effectively for CAVs [21]. Unfortunately, adopting them can be ineffective or misguided for a few reasons [22]:

1. Depending on existing security guidelines and the assumed adversarial model(s), certain weaknesses may be unnecessary to consider.
2. When generalizing attacks across all CAVs, there is a tendency to ignore security perimeter modeling (SPM), a fundamental principle for designing security architectures for CAVs.

Beyond attacks, current networking and security protocols, techniques for securing communication, and other possible factors must be examined. Many security frameworks have been designed and implemented by researchers, from which best practices for designing effective security frameworks to achieve maximum security without sacrificing computational resources or user comfort can be generalized. A few use cases have also been developed to tackle some security issues relating to CAVs.

1.1. Scope of the Survey

This paper focuses on intra- and inter-vehicle communication security, discussing the state-of-the-art security frameworks, challenges, and techniques associated with CAV communication. Particular attention is given to the architectures, protocols, and frameworks that secure these systems at both levels. Given the substantial progress in CAV security, this article provides a comprehensive review of current technologies and explores new avenues for enhancing communication security in autonomous driving systems. By highlighting technical robustness and assurance requirements, this survey offers a detailed tutorial on the latest developments in securing CAV communications. The analysis presented here provides researchers and engineers with an up-to-date review of the most pressing security issues in CAV communication, while offering insights into potential solutions and unexplored research areas.

1.2. Literature Selection Methodology

To ensure a comprehensive and up-to-date review of the literature, a systematic methodology was employed in selecting relevant papers. The primary databases used for literature retrieval were IEEE Xplore, Google Scholar, and major academic journals in automotive cybersecurity. We prioritized papers published after 2015 to capture the latest advancements in CAV security, while also including seminal works that have laid the foundation for current research in this domain. The selection process emphasized papers relevant to intra- and inter-vehicular communication security, ensuring that each study offered significant insights into the challenges and solutions within this field. Our inclusion criteria also focused on papers that contribute to the development of new protocols, attack detection methods, and security enhancements for CAV systems. We ensured a balanced review by covering both cutting-edge technologies, such as machine learning-based security solutions, and traditional approaches like cryptographic protocols. Additionally, the relevance and impact of each paper were evaluated based on the proposed security frameworks and their applicability to real-world CAV communication challenges.

1.3. Related Papers

In this section, we review the existing literature on communication security in CAVs. Numerous studies have been conducted on different aspects of CAV security, ranging from attack taxonomies to proposed security frameworks and protocols. The reviewed literature spans both theoretical and empirical studies, with a focus on contributions that propose novel security frameworks, address communication vulnerabilities, or provide comprehensive surveys of the field. Key areas explored in the literature include cryptographic protocols, secure communication architectures, machine learning-based threat detection, and privacy-preserving mechanisms for CAVs. Notable works include both recent advancements published after 2015 and seminal papers that have significantly influenced the field of CAV security.

Table 1: Summary of existing surveys and reviews related to CAV Security.

Refs. (Author)	Year of Pub.	CAV Review	Sec. & Priv.	Attack Vect.	Inter-Comm.	Intra-Comm.	Auton. Driving Apps	Eval. Tools	Standards	Overview
Papadimitratos et al. [23]	2008	✗	✓	✓	✗	✗	✗	✗	✗	Reviews threats and types of adversaries, privacy and security requirements, and mechanisms to secure vehicular systems
Miller et al. [24]	2014	✗	✗	✗	✓	✓	✗	✗	✓	Features automotive remote attacks and effects of these attacks on automotive cyber-physical surfaces including defensive and precautions to administer
Viriyasitavat et al. [15]	2015	✗	✗	✗	✓	✓	✓	✗	✓	Provides vehicular communication and implementation in dynamic environments with associated propagation and channel modeling challenges
Gupta et al. [25]	2015	✓	✗	✗	✓	✓	✓	✗	✗	Highlights mobile communication networks and their applications to civil and military domains
Abraham et al. [9]	2016	✗	✗	✗	✓	✓	✗	✓	✗	Surveys AV consumer preferences particularly mobility and reduction of accidents
Thing et al. [26]	2016	✗	✗	✓	✗	✓	✗	✗	✗	Presents security attack mechanisms against AV along with a taxonomy of their corresponding defense strategies
Gifei et al. [27]	2017	✓	✓	✗	✗	✗	✗	✓	✗	Reviews ECUs and the integration of management systems for quality, safety and security purposes in the development of AVs
Căilean et al. [28]	2017	✗	✗	✗	✓	✓	✓	✗	✓	Emphasizes challenges for visible light communications in vehicle applications with solutions and supportive data
Karnouskos et al. [29]	2017	✗	✓	✗	✓	✗	✗	✗	✗	Discusses the feasibility of ensuring integrity, safety, and privacy in hyper-connected vehicle scenarios
Parkinson et al. [30]	2017	✗	✗	✓	✗	✗	✓	✗	✓	Reviews a large volume of accessible literature and compartmentalise existing security challenges based on the state-of-art vulnerabilities countermeasure techniques
Claybrook et al. [31]	2018	✓	✗	✗	✗	✗	✗	✗	✓	Provides statistical data regarding number of vehicle accidents and the safety benefits of AVs to due to the implemented federal regulations
De Bruyne et al. [32]	2018	✓	✗	✗	✗	✗	✗	✗	✓	Introduces regulation policies to self-driving cars by analyzing the legal issues and the limitations of product liability directives involved in AVs
Tomlinson et al. [33]	2018	✗	✓	✓	✓	✗	✗	✓	✗	Presents viable detection methods for the Controller Area Network of cars that are vulnerable to attack
Van et al. [34]	2018	✗	✓	✓	✓	✓	✗	✗	✗	Discusses the Intelligent Transportation System (ITS) and related security issues and presents a classification for security detection mechanisms
Hussain et al. [19]	2018	✓	✓	✗	✓	✗	✓	✗	✗	Analyzes challenges related to AV development and deployment and highlights applications issues hindering safe and cost-effective AV
Wang et al. [22]	2018	✓	✗	✗	✓	✓	✗	✗	✗	Analyzes autonomous driving from the networking and communication technologies based on intra- and inter-vehicle aspects
Ren et al. [35]	2019	✗	✓	✓	✓	✗	✗	✗	✗	Presents an in-depth study on security threats from the angles of perception, navigation, and control and summarizes the corresponding defense mechanisms
Goumidi et al. [36]	2019	✗	✓	✓	✗	✓	✓	✗	✗	Discusses and classifies the security challenges related to Vehicular Cloud Computing (VCC)
Al-Jarrah et al. [37]	2019	✓	✗	✓	✗	✓	✗	✓	✗	Presents a comprehensive review of the intrusion detection systems with a focus on intra-vehicle aspects
Sharma et al. [38]	2019	✗	✓	✗	✗	✓	✗	✗	✗	Presents a comprehensive review of security challenges and defense mechanisms for the ubiquitous CAN bus communication protocol
Wang et al. [39]	2019	✓	✓	✗	✓	✗	✗	✓	✗	Analyzes V2X challenges and requirements and discusses testing methods in the communication process from the architectural perspective
Sommer et al. [40]	2019	✗	✗	✓	✓	✗	✓	✗	✗	Presents a comprehensive taxonomy of security attacks with details to address them throughout the AV development process
Baldini et al. [41]	2020	✓	✓	✗	✗	✗	✗	✗	✓	Analysis on policy-based framework applications to AVs to regulate, manage, and implement data resources to traffic rules.
Qayyum et al. [42]	2020	✓	✓	✓	✓	✗	✗	✗	✗	Reviews challenges of ML applicability in the communication networks and further formulates the ML pipeline of CAVs along with security threats against ML
Halder et al. [43]	2020	✓	✓	✗	✓	✗	✗	✗	✗	Surveys the security needs for vehicle over-the-air (OTA) software updates

Continued on next page

Table 1 – continued from previous page

Refs. (Author)	Year of Pub.	CAV Review	Sec. & Priv.	Attack Vect.	Inter-Comm.	Intra-Comm.	Auton. Driving Apps	Eval. Tools	Standards	Overview
Luo et al. [44]	2020	✗	✓	✓	✗	✗	✗	✓	✗	Analyzes security risks of connected vehicles and proposes an evaluation approach to ensure safe system design
Promyslov et al. [45]	2020	✗	✓	✓	✗	✗	✗	✗	✓	Presents security properties and distributes them into graphs and models for smart AV system and remotely controlled vehicles regarding cybersecurity threats
Pham et al. [46]	2020	✗	✓	✓	✗	✓	✗	✗	✗	Presents an overview of CAV security attacks and a taxonomy of their corresponding countermeasures
Green [47]	2020	✓	✓	✓	✗	✗	✓	✓	✓	Explains the SELF DRIVE Act and NHTSA best safety practices in regard to the regulation of cybersecurity and vehicle hacking in self-driving cars.
Virag et al. [48]	2020	✗	✓	✗	✓	✗	✗	✗	✓	Investigates IT-related security issues for continuously connected vehicles
Wang et al. [49]	2022	✗	✓	✓	✓	✓	✗	✗	✗	Discusses security challenges in CAVs, focusing on sustainability
Taylor et al. [50]	2022	✗	✓	✓	✗	✗	✗	✗	✓	Reviews architectures and security issues in vehicular communication
Hataba et al. [51]	2022	✗	✓	✓	✓	✗	✗	✗	✗	Reviews security and privacy issues in AV from the platooning perspective
Ahmed et al. [52]	2023	✓	✗	✗	✓	✗	✗	✗	✗	Reviews data offloading, with a focus on inter-vehicle communication network
Deng et al. [53]	2023	✓	✗	✗	✓	✓	✗	✗	✗	This Provides an overview of real-time motion control in vehicles, addressing the impact of network issues like delays, packet dropouts, and congestion from intra-vehicle, inter-vehicle, and integrated perspectives
Wei et al. [54]	2023	✓	✗	✗	✗	✗	✓	✓	✗	Presents a comprehensive overview of the vehicle control technology, focusing on the evolution from vehicle state estimation and trajectory tracking control in AVs at the microscopic level to collaborative control in CAVs at the macroscopic level.
Hakak et al. [55]	2023	✓	✓	✗	✓	✗	✗	✗	✗	Provides a comprehensive review on AVs in the 5G and beyond era and discusses on the current advancements in AVs, automation levels, enabling technologies and the requirement of 5G networks. It also presents the impact of 5G and B5G on AVs and the envisaged security concerns in AVs.
Chellapandi et al. [56]	2023	✓	✓	✓	✗	✗	✗	✓	✗	Discusses advancements in applying federated learning to connected CAVs, analyzing both centralized and decentralized frameworks and their methodologies, and examining data sources, models, and security techniques crucial for ensuring privacy and confidentiality in federated learning.
Fang et al. [57]	2024	✓	✗	✓	✗	✗	✗	✓	✗	Considers anomaly detection and interpretation in CAVs. It covers aspects such as defining, classifying, and detecting anomalies, alongside reviewing techniques and advancements, while interpretation includes analyzing anomalies in the context of safety and security risks, ultimately discussing open issues and future directions for anomaly diagnosis in CAVs.
Pipicelli et al. [58]	2024	✗	✗	✓	✓	✗	✗	✓	✗	Evaluates the efficiency improvements of CAVs and provides a detailed overview of their architecture, including layout, data processing, and management strategies for energy. It employs statistical distributions in a Monte Carlo simulation to assess the impact of optimal driving behaviors and power consumption of CAV hardware on vehicle energy savings.
Qu et al. [59]	2024	✗	✗	✓	✗	✗	✗	✓	✗	Proposes an adaptive cooperative perception scheme for CAV pairs that optimizes between cooperative and stand-alone perception to enhance computing efficiency in mixed-traffic. Utilizing a model-assisted multi-agent reinforcement learning approach, our results demonstrate significant efficiency improvements over traditional methods.

Table 1 – continued from previous page

Refs. (Author)	Year of Pub.	CAV Review	Sec. & Priv.	Attack Vect.	Inter-Comm.	Intra-Comm.	Auton. Driving Apps	Eval. Tools	Standards	Overview
Ibn-Khedher *et al.* [60]	2024	✓	✓	✗	✗	✗	✗	✓	✓	Surveys 6G technologies like mobile edge computing and artificial intelligence that can improve the Internet of Autonomous Vehicles (IoAV) network performance beyond current 5G solutions. We also discuss the convergence of 6G and IoAV for future CAV applications, addressing challenges and proposing directions for 6G-IoAV research.
Mohsen Sorkhpour *et al.* [61]	2024	✗	✓	✓	✗	✗	✗	✓	✓	Control Area Network (CAN) lacks built-in security mechanisms, making it vulnerable to cyber-attacks, and existing Intrusion Detection Systems (IDSs) for CAN require significant manual intervention. Auto-CIDS, an autonomous IDS using Deep Reinforcement Learning (DRL), reduces human intervention by enabling active learning and self-supervised detection of attacks, demonstrating effectiveness on the Car-Hacking dataset.
Our Survey	**2024**	✓	✓	✓	✓	✓	✓	✓	✓	**Discusses the state-of-art security frameworks, challenges, and techniques for securing both inter- and intra-vehicular communication along with related applications and use cases**

While this research area is not new, there was a heavy interest in the security of CAVs in the early 2000s. For instance, a group of researchers led by Jean-Pierre Hubaux *et al.* published a series of research papers establishing the groundwork for improving security in CAVs including [62], [63], and [64], and [65]. These works include highly detailed designs and frameworks for improving the security of CAVs, designing new mechanisms to improve vehicular communications, and designing protocols for managing communication from multiple pathways for CAVs.

There have been several newer research works that discuss the security of CAVs. Notably, the work [6] discussed the impact of security on the vehicular communication system, whereas the work [27] emphasizes the importance of dealing with the security of AVs in an integrative manner and further reviews the importance of establishing acceptable levels for cyber-security risks. Another work [48] identifies current challenges of securing AVs. The authors conducted interviews with security experts from fields such as consulting, manufacturing, and software engineering and researched topics of failing security in AVs. The work [29] also discusses security for AVs. The authors note that while data plays a crucial role in securing AVs, there are still concerns about privacy and integrity scenarios. Further works such as [41] review the Policy-based frameworks (PBFs) for AVs in various applications relevant to security and safety, including network management and access control. Another work [45] discusses the security of CAVs in the context of smart cities, focusing on the integrity of vehicular communications. Furthermore, the work [47] focuses on maintaining security for CAVs while considering the legal aspect, especially regarding users and the design of the CAV. The authors of [33] discuss the significance of the automotive CAN in its protection and safety against cyberattacks. The article [30] contributes to the cyber threats and automation levels of CAVs and emphasizes knowledge gaps to display vulnerable areas that need improvement in preventing cyberattacks.

Another work [24] surveys remote automotive attacks and their surfaces. By expanding

on the anatomy of a remote attack, analyzing automotive networks, and presenting ways to defend against remote attacks, the article contributes to preventing cyberattacks in AVs with a focus on ECUs. The article [22] expands on the usage of networking and communication devices in AVs, thereby contributing to an understanding of automobile technologies, such as intra- and inter-vehicle communications. The authors investigate and compare the intra- and inter-network connections, communication and networking challenges in CAVs to repair networking and communication issues. Moreover, an overview of CAVs, real-world test results, and the advancements of the technologies that contribute to the expansion of the field is provided in [19]. The article focuses on technical and non-technical issues between communications and networking, including software complexity, real-time data analytics, testing, and verification. Goumidi *et al.* [36] survey cloud computing security in vehicles to underline their importance in VANET improvements. Introducing vehicular ad hoc networks, or VANETs, and combining the technology with vehicular cloud computing (VCC) provides a solid foundation for CAVs. The work [38] highlights vehicle security and presents security measurements to maintain a beneficial driving experience. Security threats and countermeasures for the CAN bus communication protocol are also reviewed in this article. Moreover, the work [37] discusses the different types of intra-vehicle networks that control and monitor the vehicle's state and identifies challenges that the predominant detection systems cannot address.

Additional surveys such as [46] present security attacks and defense mechanisms for CAVs. In this article, security attacks are quantified and compartmentalized along with their corresponding countermeasures on CAVs. Additionally, the article [42] provides a comprehensive overview of techniques and challenges related to the application of ML in CAV networks. However, different from these two articles, our work discusses the state-of-art security protocols, architectures, and frameworks in addition to security challenges and implications, focusing on intra- and inter-communication.

Interestingly enough, mobile car apps for CAVs have become increasingly popular in recent years due to their benefits: convenience, control, and visibility to the users. However, mobile car apps for CAVs add additional risks: exposing vulnerabilities in the mobile app, the phone's operating system, and the app's usability. Additionally, sometimes vendors are eager to release a new mobile app for CAVs while overlooking security features. As such, these car apps for CAVs are often released and updated without necessary security requirements. Furthermore, mobile car apps for CAVs are challenging due to the complexity of the CAV ecosystem with mobile environments. Its complex data architecture makes it difficult to secure communications between multiple sources: the mobile phone, the mobile application, the application's servers, the connected vehicle itself, and the servers communicating with the car. Thus, To protect the multiple sources, it is not enough to secure each of them separately – the data between them must be correlated and analyzed to produce a coherent view of the data flow. There must be a network-based solution to secure the entire data center and the network [66].

Several studies have covered mobile car apps. For example, Eriksson *et al.* [67] explored on the Android automotive system architecture with a special focus on the permission model. The authors also addressed several vulnerabilities, implemented several attacks on the android automotive system, and measured the severity of these attacks using the Common Vulnerability Scoring System (CVSS3). It was found that the biggest vulnerabilities come

from Android's permission model. In [68], the authors also focused on Android and examined car apps available on Google Play and found that nearly 80% of the apps are potentially vulnerable. Similar findings were also discovered in works [69] and [70].

The works of [71] and [72] also discuss how using automotive smartphone apps provided by car manufacturers can offer numerous advantages to the vehicle owner, such as improved safety, fuel efficiency, monitoring of vehicle data, and timely software updates. However, the continuous tracking of the vehicle data by such apps may also pose a risk to the CAV owner. While the work [71] explores the OpenXC platform (an open-source API that allows Android apps to interact with the car's hardware) and shows how it is used to create interjection attacks, the work [72] assesses the security of all official single-vehicle management apps offered by major car manufacturers who operate in Europe. It is found that many apps remain susceptible to critical vulnerabilities due to misconfigurations, secure coding negligence, and latent or overt security flaws that relate to the use of third-party software. Further, the book by Singh [73] presents a cybersecurity overview and perspectives along with challenges that impact vehicular technology. It also discusses security structures and potential solutions to specific security issues. Additionally, the work [61] introduces Auto-CIDS, an autonomous IDS for CAN networks that leverages deep reinforcement learning to enhance intrusion detection, significantly reducing the need for manual intervention.

As the aforementioned works reveal, security mechanisms must be considered fully for the CAVs. Furthermore, both technical and non-technical aspects—such as security implications, impact assessments, security evaluation metrics, and regulatory issues—must also be considered. While the works discussed in this section may arguably seem similar to some, they are notable in terms of the areas they address and potential future trends for CAVs.

1.4. Contributions and Paper Organization

The complex digital ecosystems in CAVs introduce unique security vulnerabilities across sensors, controllers, and communication interfaces. These security concerns, ranging from potential vehicle hijacking to traffic data manipulation, directly impact public safety, trust, and the broader economic potential of CAVs. Thus, this review is essential in addressing and understanding these challenges [74, 75]. It aims to foster public trust, guide regulatory frameworks, highlight research gaps in communication security, and help balance rapid technological advancements with safety assurances.

While numerous related surveys exist in the literature, none bridges the gap between intra- and inter-vehicular communication attacks. This gap arises because: 1) Covering both areas requires a comprehensive understanding of multiple disciplines, such as cybersecurity, automotive engineering, and wireless communications; 2) Addressing both intra- and inter-vehicular communication in a single review is intricate due to the range of components and communication protocols involved. Researchers often find it more manageable to focus on one aspect rather than both; and 3) The integration of CAVs into mainstream transportation is still relatively new. As technologies evolve and new research emerges, up-to-date comprehensive reviews will remain essential for researchers and practitioners. This paper is the first to systematically synthesize both intra- and inter-vehicular attacks and defenses, making a significant contribution to the existing body of literature summarized in Table 1.

This paper makes significant contributions to the field of CAV communications, which are detailed as follows:

- We present a thorough outline of cutting-edge protocols recently introduced in scholarly literature, emphasizing their advancements and applications in CAVs.

- The paper offers a comprehensive examination of prevalent CAV architectures, providing in-depth insights into each architecture's structure, functionality, and impact on CAV operations.

- We propose a set of practical security protocols designed for easy integration into existing CAV systems. These protocols enhance data integrity and confidentiality without imposing significant overhead on system resources, striking an optimal balance between security and performance.

- Unlike prior studies that focus on isolated security threats, our work offers an exhaustive analysis of both intra- and inter-vehicular attack vectors. We categorize these attacks and demonstrate through simulations how they impact CAV operations, providing a holistic view that aids in better security planning and system design.

- A variety of use cases are explored to demonstrate the practical applications of the discussed protocols. Additionally, the paper incorporates insights from academic researchers, industry professionals, and international regulatory bodies, offering a multi-dimensional understanding of CAV architectures.

- We identify and propose potential areas for future research, focusing on unexplored aspects of CAV communication security and technology development. This includes suggestions for advancing current protocols and architectures, exploring new security challenges in evolving CAV ecosystems, and developing innovative solutions to enhance the safety and efficiency of autonomous vehicles.

- Our study leverages interdisciplinary approaches, combining insights from cybersecurity, automotive engineering, and wireless communications to forge comprehensive solutions that are robust against a wide spectrum of potential vulnerabilities.

The paper is organized into eight comprehensive sections. Specifically, the structure is as follows: Section 2 provides background on communication security in CAVs, and Section 3 reviews communication security architectures and challenges. Next, Section 4 presents an up-to-date taxonomy of communication security attacks on CAVs. While Section 5 discusses state-of-the-art communication security solutions and evaluation tools, Section 6 explores communication security protocols for CAVs and best practices. Section 7 then provides in-depth insights on open issues and future research directions. Last, Section 8 concludes the article.

2. Background on Communication Security

This section presents key use cases and applications involving communication security in autonomous driving, followed by a discussion on standards related to CAV security.

2.1. Autonomous Driving Applications that Demand Security

The need for efficient security mechanisms in CAVs has driven researchers to develop specific use cases that highlight their approaches to securing various applications of CAVs [76, 77]. Key applications of autonomous driving will be discussed next.

2.1.1. Valet Parking

Secure communication plays a crucial role in the valet parking use case for CAVs [78]. One key aspect is establishing a secure channel between the CAV and the parking infrastructure, ensuring that sensitive information—such as the vehicle's identity, location, and authorization credentials—is protected from eavesdropping and tampering by malicious actors [79]. Secure communication is particularly important during the initial authentication and authorization process, where the CAV securely identifies itself with the parking system and obtains the necessary permissions to park. Additionally, secure communication must be maintained throughout the parking duration to enable continuous monitoring and control over the vehicle's status and prevent unauthorized access. By employing robust encryption algorithms, authentication mechanisms, and secure protocols, CAVs can safeguard communication with the parking infrastructure, minimizing the risk of unauthorized access and ensuring a secure valet parking experience [80].

Driverless parking is one of the benefits of CAVs that has gained notable attention due to the increased focus on designing automated and secure parking models [81, 82]. However, location and identity privacy issues persist because parking data is sometimes shared improperly. To address this, a privacy-centric framework for secure parking reservations has been proposed [83]. Additionally, an Autonomous Valet Parking System (AVPS) uses connected communication technologies to locate available parking spots in garages and park the vehicle autonomously [84]. A critical factor emphasized in [84] is ensuring that the reserved parking space remains available until the CAV is parked or the timer expires, which can increase the risk of a Multiple Reservation Attack (MRA). Under this attack, the user attempts to reserve all other possible parking spaces, assuming other users have already reserved them. Furthermore, the registration process required to secure a parking spot may inadvertently expose user identity and personal data, such as unique identifiers, email addresses, and home addresses.

2.1.2. Lane Changing

Lane changing is another prominent use case of autonomous driving applications [85]. After all, inappropriate lane following and changing behaviors of CAVs can lead to accidents. Using deep-reinforcement learning as a widely used approach to ensure this does not occur [86]. However, there are still issues with validating reinforcement learning systems for autonomous systems. This can lead to incoherent interpretations of the performance of the reinforcement learning algorithms and how well they generalize [87, 85]. Other issues with deep-reinforcement learning are sample efficiency, difficulty in reproducing reinforcement-learning results, and high sensitivity to hyper-parameter choices [88, 89]. As such, a blockchain-based learning (BCL) framework for autonomous lane-change systems was proposed in [85]. In the BCL architecture, four main issues are addressed: learning rate, data security, users' privacy, and communication burden while achieving a success rate of 96.5% for lane changes, with the likelihood of accidents or failures occurring ranging between 1% to 2%.

When a CAV is performing a lane change maneuver, it needs to communicate with other vehicles and the surrounding infrastructure to ensure a safe and efficient transition [90]. Secure communication comes into play at various stages of this process. Initially, the CAV needs to securely broadcast its intent to change lanes, informing nearby vehicles of its planned action. This communication ensures that other vehicles can adjust their behavior accordingly to maintain a safe distance and avoid collisions. Further, secure communication is critical for the CAV to receive feedback from surrounding vehicles, confirming their acknowledgment and cooperation [91]. Throughout the lane change maneuver, continuous secure communication is necessary to exchange real-time information, such as the CAV's position, speed, and trajectory, with other vehicles and the traffic management infrastructure.

2.1.3. Image and Audio-based AI Service for Security Applications

Image and audio-based approaches can incorporate various AI (Artificial Intelligence) methods to increase security and trust inside an autonomous shuttle [92]. This approach runs in real-time and can be used to detect petty crime scenarios (e.g., screaming, bag snatching, people fighting, vandalism). This system can further enable notifications to authorized personnel so they can dictate proper actions. Thirteen different scenarios were simulated using different camera perspectives for each one, and 29 video sequences were also captured with 46,127 frames, achieving up to 96% accuracy for target classes classification [92]. When image and audio-based AI services are deployed for security applications in CAVs, such as detecting and responding to suspicious activities using image and audio analysis, secure communication becomes crucial. Firstly, the CAV must securely transmit the captured image and audio data to the central security system for analysis [93]. This involves employing encryption techniques and secure protocols to protect the confidentiality and integrity of the data during transmission, ensuring that sensitive information is not compromised. Additionally, secure communication is critical when receiving instructions or updates from the central security system. This ensures that the CAV can authenticate and verify the authenticity of the commands it receives, preventing unauthorized access or tampering.

2.1.4. Web-Based Car Control and Monitoring for Safe Driving

The security of vehicular communications, especially the V2I (vehicle-to-infrastructure) and V2V (vehicle-to-vehicle) communications is considered to enhance autonomous driving security and experience. A web-based car monitoring was proposed to enable vehicles in vehicular networks to exchange their mobility information, achieving quick road awareness using W3C Vehicle Information Service Specification (VISS) and Vehicle Signal Specification (VSS) [94]. This use case takes advantage of the vehicle network infrastructure to control and monitor road mobility to enhance the safety of autonomous driving. The implemented use case typically incurs a delay of 0.055 seconds for V2I communication and an average delay of 0.0015 seconds for V2V, enabling distant CAVs to proactively react.

2.1.5. Blockchain-inspired Event Recording System

What is unique about [95] is that this particular use case covers the liability aspect of security. When CAVs are involved in accidents among themselves or with human subjects, liability must be based on accident forensics. Thus, a blockchain-based event recording system was proposed for CAVs [95]. A new PoE (Proof of Event) mechanism was also designed to

achieve indisputable accident forensics by ensuring that event information is trustworthy and verifiable. Along with the event recorder system, the consensus mechanism efficiently verifies and confirms new blocks of event data without any central authority. Additionally, accidents are recorded as time-stamped transactions that are supposed to be saved into new blocks in real-time. A cellular network-based infrastructure is adopted to define a vehicular network for each accident.

Secure communication comes into play in this use case when the CAV transmits the event data to the blockchain network for recording [96]. This may involve encrypting the data to protect its confidentiality and integrity during transmission, preventing unauthorized access or tampering. Further, secure communication is necessary when verifying and validating the event data with other network participants. This ensures that the recorded events are authenticated and cannot be tampered with, maintaining the integrity and immutability of the blockchain ledger.

2.2. Standards Relating to CAV Communication Security

For this subsection, we focus on relevant standards related to the communication security of CAVs. Standards developed for CAVs often cover multiple aspects, such as functional safety, operation correctness, etc. These standards are not nearly talked about enough, likely due to the complexities of the CAV itself and the challenges of developing threat models to ensure maximum testing of the CAV.

The unfortunate reality is that threat modeling is challenging, and it can be used as a tool to aid software and algorithm design, as well as to help design teams think more clearly about what types of security issues they may face. However, without real-world experience of how systems are attacked at an engineering level, it can be far too abstract. Therefore, It is essential that those involved in forming standards for CAVs and the teams involved truly understand the types of threat environments and help formulate guidelines to cover as much basis as possible. This is because a threat or security risk scored too highly can increase the development cost. Conversely, a score that is too low will starve funds and engineering resources from an area that sorely needs attention. Numerous standards have been designed to address these concerns, including the International Organization for Standardization (ISO) 26262 SAE J3061, among others, which are detailed next. Communication security is a critical aspect of CAVs, and it is typically addressed through specific standards and frameworks that complement baseline standards such as ISO 26262. Prominent, relevant standards and frameworks that specifically address communication security in CAVs are summarized next.

2.2.1. SO/SAE 21434

This standard, also known as Automotive Cybersecurity Engineering, provides guidelines for automotive cybersecurity throughout the vehicle's lifecycle. It addresses various aspects of cybersecurity, including secure communication protocols, secure software development, risk assessment, and vulnerability management [50].

2.2.2. SAE J3061

Developed by the Society of Automotive Engineers (SAE), this document provides a cybersecurity guidebook for the automotive industry. It covers the entire vehicle ecosystem, including communication security, threat analysis, risk assessment, incident response, and

security lifecycle management. This particular standard is based on the ISO 26262 standard and covers the growing threat landscape of CAVs. SAE J3061 establishes the terminology of threat, vulnerability, and risk, providing an overview and distinction between system safety and system cybersecurity. It also presents a few general guiding cybersecurity principles that apply to any organization within a company. Another notable component is that this standard provides information regarding some common existing tools and approaches for the design, verification, and validation of CAVs. A foundation is presented for further development approaches for CAV cybersecurity. The most important contribution this standard offers is this distinction: that a cybersecurity-critical system may not be safety-critical [80].

2.2.3. AUTOSAR Security

The AUTOSAR (Automotive Open System Architecture) consortium defines a set of standards and specifications for automotive software architectures. Within AUTOSAR, security-related standards and mechanisms are defined, including secure communication protocols, secure bootstrapping, secure onboard communication, and secure software updates [97].

2.2.4. NIST Cybersecurity Framework

Although not specific to the automotive industry, the National Institute of Standards and Technology (NIST) Cybersecurity Framework offers a comprehensive set of guidelines and best practices for managing and improving cybersecurity risk. This framework can be applied to CAVs to address communication security aspects [98].

2.2.5. ISO 21434

The ISO 21434 standard guides cybersecurity risk management by specifying engineering requirements relating to cybersecurity risk in terms of concept, product development, operation, maintenance, and decommissioning. The standard also covers various components and interfaces. Additionally, the ISO 21434 standard includes a framework that includes a common language for communicating and managing cyber security risk [80]. ISO 21434 is intended to provide guidelines and requirements for incorporating cybersecurity into the engineering processes of road vehicles. It is expected to address various aspects of automotive cybersecurity, including communication security.

2.2.6. ISO 20078-3:2021

The focus of this standard is on user authentication. Specifically, it describes how to authenticate users and other parties on a web service interface. A definition of how a resource owner can delegate access to a trusted party is also provided. The standard also defines the necessary roles and crucial separation of duties to fulfill tasks relating to security, data privacy, and data protection. A reference implementation using an OAuth 2.0 compatible framework and OpenID Connect 1.0 compatible framework is also provided [99].

2.2.7. ETSI TR 103 460

This standard provides an overview of relevant misbehavior detection mechanisms suitable for CAVs. The standard also provides information regarding performance and applicability on different misbehavior mechanisms and describes minimum requirements for security architecture [100]. Further, ETSI TR 103 460 provides guidance on the security architecture and

governance framework for Cooperative Intelligent Transport Systems (C-ITS) systems. It addresses the specific security challenges and requirements associated with CAV communication and aims to ensure secure and trusted communications between vehicles, infrastructure, and other entities in the C-ITS ecosystem. It is worth noting that baseline standards such as ISO 26262 and other related standards and frameworks are not mutually exclusive. For instance, while ISO 26262 primarily focuses on functional safety, cybersecurity, and communication security are essential components of overall safety in CAVs. Therefore, organizations developing CAV systems typically consider ISO 26262 and other relevant standards to address both functional safety and communication security aspects effectively.

3. Communication Security Architectures and Challenges

This section presents the prominent CAV security architectures along with key communication security challenges.

3.1. Security Architectures for CAVs

3.1.1. RACE

The authors of [101] propose a security framework called RACE (reinforced cooperative autonomous vehicle collision avoidance) geared toward collision avoidance. CAVs typically gain proficiency with their general surroundings and ideal driving procedures via onboard sensors like Lidar, radar, and acceleration sensors. In any case, due to the restrictive communication range of the vehicles, the gathered data from one vehicle is inadequate to satisfy enormous large-scale road safety requirements and improve collision performance efficiently. As such, the authors designed the RACE architecture to overcome these shortcomings. The authors built their framework using a simulator and evaluated their framework on the simulator as well. Upon examining the evaluation results, the authors concluded their framework can learn from the environment and its neighboring agents. RACE also managed to outperform other frameworks and reduce collisions by 65%.

One of the key innovations of RACE is its utilization of cooperative perception, where data from multiple vehicles is combined to enhance situational awareness. This collaborative approach allows vehicles to have a broader view of their surroundings beyond the limitations of their own sensors, significantly improving decision-making accuracy. Additionally, the framework incorporates reinforcement learning algorithms, which adapt the behavior of vehicles based on past experiences, allowing the system to progressively optimize collision avoidance strategies. However, further analysis is required to assess how well the system performs in highly congested environments and under scenarios involving unexpected road events, such as sudden pedestrian crossings. This deeper exploration can provide insights into the scalability and real-world applicability of RACE.

3.1.2. Blockchain Frameworks for Securing CAVs

Recently, many researchers are incorporating blockchain frameworks for CAVs [102, 103, 3]. Blockchain is a popular and viable choice for securing CAVs due to its high security and immutability. The work by Rathee *et al.* [104] proposes a blockchain architecture for securing CAVs that emphasizes secrecy and protection and is presented as a use case for service delivery. For the proposed framework, CAVs are registered into a network before services

can be accessed. The required information on the CAVs is entered into a database first, then stored on the blockchain-centric framework permanently so that every event can be accounted for in the CAVs. The framework also involves IoT devices (Internet of Things), which are also connected to CAVs. The quantity of CAVs connecting to those IoT devices depends on communication and transmission ranges. In addition, To account for the likelihood of the CAVs or devices being hacked, every device that provides the information about the CAVs needs to register itself on the network before providing services to the connected vehicles. This security framework leverages blockchain capabilities to enforce both privacy and secrecy for vehicle drivers by recording all activities and tracing them inside the blockchain ledger [105]. The extracted IoT data is further recorded and inspected by various authorities to ensure the driver's safety and the IoT device's security.

However, while blockchain offers high levels of immutability and security, the inherent challenge of scalability and latency remains unresolved. Specifically, the time required to process and validate transactions within a blockchain network may hinder real-time vehicular communication, which is critical in safety-sensitive CAV environments. For instance, scenarios such as rapid lane changes or emergency braking require near-instantaneous data sharing across the network. Implementing off-chain solutions or hybrid blockchain architectures could mitigate these latency issues. Furthermore, the computational overhead for resource-constrained IoT devices involved in blockchain verification processes must be optimized to ensure seamless integration into CAV ecosystems. Future work could focus on lightweight consensus algorithms to reduce the burden on these devices while maintaining security guarantees.

Blockchain technology can also be leveraged to handle information access to restricted entities within the CAV ecosystems and authentication mechanisms for fog computing-enabled Internet of Vehicles [106]. For instance, a challenge/response-based exchange of information between roadside units (RSUs) and connected vehicles can be leveraged to monitor the internal state of vehicles and detect intra-vehicle security compromise events. Furthermore, through blockchain technology, valid and legitimate communication traffic accuracy can be enhanced within the intra-vehicle network by assuring only vehicles with a verifiable record in the public ledger can exchange messages. A remarkable solution is presented in [107], where the authors propose a Blockchain-based Framework for sEcuring smaRt vehicLes (B-FERL), a permissioned blockchain-based framework, to regulate information access in the CAV ecosystem. Here, quantitative-based emulation scenarios demonstrate the efficiency of B-FERL in ensuring reliable trust management and response time to vehicle network attack identification.

3.1.3. Privacy-Preserving Raw Data Sharing Framework

Xiong *et al.* [108] focus on establishing a security architecture for CAVs, but their framework is more focused on data sharing, data leakage, and encryption. Because CAVs will often share data, protection must be provided to prevent possible data leakage [109, 110]. However, encrypting data often leads to tremendous overhead being generated, and even with current research, this is still a persistent issue. To alleviate these issues, the authors implement a privacy-preserving raw data-sharing framework using Edge Assist. The authors note that because their architecture incorporates edge computing, their proposed architecture is lightweight and privacy-preserving. A significant technical challenge in this approach

is balancing data privacy with real-time processing efficiency. By offloading data processing to edge servers, the framework reduces the computational burden on CAVs; however, edge nodes themselves must remain highly secure and capable of handling large volumes of encrypted data without introducing latency. Another aspect worth deeper investigation is the framework's resilience to adversarial attacks targeting the edge servers. These servers could become central points of failure if compromised, leading to widespread data breaches across connected vehicles. A possible solution is the integration of distributed edge computing models, where no single node has complete control over the data, thereby reducing the attack surface. Furthermore, analyzing the trade-offs between encryption strength and computational overhead in various traffic conditions will be critical for determining the framework's scalability in real-world applications.

In this proposed framework, the architecture consists of CAVs, edge-based servers, and an overall main trusted server. A CAV has to understand its surrounding environment by using different sensors and generating real-time sensor data. Each captured image is encrypted into two encrypted images, called ciphertexts. The two ciphertexts are transferred to two edge servers, both implementing a deep learning (DL) framework for image processing. Another component involved in the author's proposed framework is a Privacy-Preserving Convolutional Neural Network (P-CNN). The P-CNN handles object classification. The authors used the VGG-16 CNN model and modified it to design the P-CNN. Afterward, the authors tested their proposed framework on the KITTI dataset. Upon examining the results, the proposed framework was able to reduce computational costs and overhead without leaking private data.

3.1.4. AC4AV

In another work [111], Zhang *et al.* propose an architecture called AC4AV, which revolves around securing the sensing data of AVs. After all, sensing data allows AVs to perceive their environments, and tampering with this data leads to inaccurate driving decisions while also threatening passenger safety [112]. Due to how complex the AVs' sensing data is, establishing a secure framework is challenging. There is currently no suitable framework that can solve this issue, and current architectures only focus on one element. This is why the authors proposed the AC4AV architecture: to provide a flexible and dynamic way of implementing security for AVs. As such, AC4AV focuses on access control, which is supposed to shield information from fraudulent access. A key strength of AC4AV is its adaptability, particularly in how it can adjust access control policies based on the dynamic nature of AV environments. The framework's context monitoring component continuously updates the system's understanding of its surroundings, which allows for real-time adjustments to access permissions. However, there is a need for further analysis on how AC4AV handles conflicting access control decisions, especially in scenarios where multiple entities (e.g., passengers, external devices) request access simultaneously. Additionally, the framework's reliance on predefined access policies may limit its ability to handle novel security threats. Enhancing the system with machine learning techniques could enable it to detect and adapt to new attack vectors that have not been explicitly accounted for in the access control engine. Performance evaluations of AC4AV in diverse real-world conditions, such as urban and rural environments, would provide valuable insights into its robustness and scalability.

Regarding the AC4AV architecture, the Access Control Engine has four main components:

access enforcement, context monitoring, data abstraction, and engine API. The context monitor obtains the CAV system's status information. Next, the data abstraction component's goal is to make the data from CAVs easier to comprehend and distinguish. The Engine API component is meant to support a customized policy regarding security. The Engine API also has several implemented access control modules so that various programs can assign different access control models to protect their information. Finally, the access control engine is in charge of ensuring that permissions to access various actions for CAVs are accurately verified. In terms of evaluation, the authors evaluated AC4AV based on performance and concluded that AC4AV reduces latency and has low overhead. There is also little impact on real-time data access.

3.1.5. ML-Based Detection for Cybersecurity Attacks on CAV

In [113], the authors highlight that there is no standard framework for securing CAVs, especially regarding some attacks that CAVs are prone to. The work explicitly centers around the network safety aspect of self-governing vehicles. The authors propose a Unified Modeling Language (UML)-based cybersecurity framework and utilize that framework to identify and distinguish other possible vulnerabilities of CAVs. In the framework, the authors also developed a new data set for CAVs named CAV-KDD, which is based on the KDD99 dataset. The CAV-KDD data set has 14 communication-based sub-attacks. The authors also used the Decision Tree and Naive Bayes classifiers for the new dataset and compared their performances based on accuracy, precision, and runtime. For the authors' experiment, the authors split their data between normal data and malevolent data for training and testing. To avoid possible over-fitting, the authors used 10-fold validation. Upon examining the experiment results, the authors note that the decision tree model achieved the best results and is suitable for detecting various types of cyberattacks on CAVs. However, both ML models performed poorly when tested on new types of unseen CAV cyber-attacks. One of the major challenges identified in this work is the poor performance of ML models when faced with unseen attack types. This is particularly problematic in the highly dynamic environment of CAVs, where new attack strategies emerge frequently. Future work should focus on developing adversarial training methods to improve the generalizability of ML models across a wider range of potential threats. Moreover, the authors could explore federated learning as an alternative approach, where models are trained collaboratively across multiple CAVs without sharing sensitive data. This would allow the system to learn from a broader dataset while preserving privacy and increasing robustness against diverse attack patterns. The trade-offs between model accuracy and computational efficiency must also be analyzed, as resource-constrained CAVs may struggle to run complex models in real-time.

Additionally, a considerable challenge here is the design of an efficient autonomous controller to carry out real-time control-based autonomous driving decisions (e.g., acceleration level when merging or changing lanes on the highway). Existing frameworks and prototypes mainly rely on conventional feedback controllers, which are traditional ML-based controllers trained through the local data of CAVs. Therefore, such solutions may degrade driving safety by providing inaccurate decisions over the various traffic dynamics and road conditions [114]. A notable work carried out by Zeng *et al.* [114], where they propose a novel dynamic federated framework (DPF) leveraging a proximal learning algorithm. The authors' proposed solution accounts for the CAV wireless fading channels, unbalanced distributed data across

multiple vehicles, and CAV mobility conditions. The proposed solution uses at-scale-based connectivity to develop the CAV autonomous feedback controller, where the controller learning and training models are collaboratively carried out over multiple CAVs to provide optimal decision convergence.

Software Defined Networking (SDN) technology supports efficient communication within the data plane and management plane (through the OpenFlow protocol) [115, 116]. It further enables executing complex traffic flow transmission rules using inexpensive and simplified forwarding devices such as virtual software switches (e.g., Open vSwitch). Security, time-sensitive forwarding, and easily updatable network devices can benefit from integrating SDN into autonomous driving systems. To support this, Hackel *et al.* [117] discussed the potential integration of SDN technology and Time Sensitive Networks (TSN) into intra-vehicular networks. The authors proposed a Time-Sensitive Software-Defined Networking (TSSDN) framework that deploys time-sensitive traffic over SDN-enabled switches by registering data flows with OpenFlow. The proposed framework was evaluated with respect to real-time capabilities on a standard event-based network simulator, namely, OMNeT++. Last, the authors concluded that although SSSDN frameworks add control computational overhead and latency, no latency penalty applies to the TSN traffic.

3.1.6. 5G-V2X

The 5G-V2X architecture has been developed by the 5G Automotive Association (5GAA), which is a corporate coalition to design and develop standardized architectures and protocols for vehicular technology using 5G-based communications [118]. 5GAA has developed the 5G-V2X architecture, which focuses on leveraging 5G technology for CAVs [119]. The architecture encompasses the following key components and functionalities:

- **Radio Access Network (RAN)**: The RAN component includes the 5G base stations that provide wireless connectivity for CAVs. It enables direct communication between vehicles, infrastructure, and other devices through the 5G air interface.

- **Cellular Core Network**: The cellular core network manages the communication between CAVs and other entities within the 5G network. It includes various elements, such as the user plane function (UPF) and the control plane function (CPF), that handle data forwarding and control signaling, respectively.

- **V2X Communication**: The 5G-V2X architecture supports Vehicle-to-Everything (V2X) communication, which involves data exchange between vehicles, infrastructure, pedestrians, and the cloud. This communication enables real-time information sharing related to traffic conditions, road hazards, and cooperative maneuvers.

- **Edge Computing**: Edge computing is integrated into the 5G-V2X architecture to enable low-latency processing and decision-making closer to the network edge. By deploying computing resources near the RAN, edge computing enhances the responsiveness of CAV applications that require real-time data processing [120].

- **Cloud Connectivity**: Cloud platforms play a vital role in the 5G-V2X architecture by providing storage, processing capabilities, and data analytics for CAVs. The cloud

allows for functions such as remote monitoring, firmware updates, and advanced data analysis, contributing to enhanced decision-making and personalized services.

- **Security and Privacy**: The 5G-V2X architecture prioritizes robust security mechanisms to protect the privacy of users and ensure the integrity and confidentiality of the data exchanged. Encryption, authentication, access control, and intrusion detection systems are typically incorporated to secure CAV systems.

While the 5G-V2X architecture offers significant advancements in terms of communication speed and reliability, one of the critical challenges lies in maintaining consistent low-latency communication in highly congested urban environments. The density of vehicles and infrastructure in such settings may result in interference, which can degrade communication quality and delay real-time decision-making processes. Additionally, the integration of edge computing is promising for reducing latency, but it introduces the need for robust and scalable infrastructure at the network edge to handle the massive volumes of data generated by CAVs. Further research is required to explore the optimization of edge node distribution and resource management, particularly in rural or less-developed areas where infrastructure may be sparse. Another challenge is the security aspect, where the use of 5G networks increases the attack surface due to the higher number of connected devices and distributed components. While encryption and authentication mechanisms are integral to the architecture, the complexity of managing security across multiple layers, from the edge to the cloud, requires advanced intrusion detection systems that can adapt to evolving threats. Moreover, the security of V2X communication must account for the varying trust levels among different communication entities, such as pedestrians, vehicles, and infrastructure, which could introduce vulnerabilities if not properly managed. Implementing zero-trust security models within 5G-V2X environments could enhance overall security by ensuring that every entity is continuously authenticated and verified before communication.

3.2. Communication Security Challenges

Even with current research and progress regarding CAVs, there are still many challenges that persist, especially concerning security [121]. The challenges include privacy, real-time response, data validation, malware detection, and liability, as shown in Table 2.

3.2.1. Privacy

As CAVs advance, privacy will remain an essential concern [29]. Despite the consistent improvement of self-governing vehicles, it is still unclear what personal data might be gathered via CAVs [122]. Different kinds of data that could be gathered via CAVs include the following.

- **Owner and passenger information:** This relates to information about the owner and passenger(s). The CAV would need to collect this information regarding authorized users. There are several legislations regarding this aspect, which could apply to certain aspects of CAV data and communications. However, due to the type of data, the manner of collection, or the entity collecting the data for CAVs, these laws may not be applicable.

Table 2: An overall summary of AV components, their tasks, attacks/risks they are vulnerable to, and the potentially compromised security goals.

CAV Component	Area(s) of Focus	Attack(s)	Compromised Security Goals	CAV Challenges
GPS	Navigation	Jamming, Spoofing	Data integrity, Data confidentiality	Real-time Response
LIDAR	Sensing	Relay, Spoofing	Data integrity, Data confidentiality, Authentication	Privacy, Real-time Response
MMW Radar	Warning System	Jamming, Spoofing	Data integrity, Data confidentiality	Liability
Ultrasonic Sensors	Park Assist	Spoofing, Jamming	Data integrity, Data confidentiality	Malware Detection
Camera(s)	Visual representation of Environment	Blinding	Integrity, Availability	Real-time Response
OBD Port	Real-time data	Malicious OBD devices, Remote exploitation	Data integrity, Availability	Malware Detection
ECU	Controlling other subsystems	ECU access through CAN, ECU access via other connection mechanisms	Data integrity, Availability	Liability, Real-time Response, Malware Detection
CAN	Communication	Malicious attacks, Passive Attacks, Denial of Service, Man-in-the-Middle attacks	Data integrity, Data confidentiality, Authentication	Privacy
VANETs	Communication and Road infrastructure	Denial of Service, Eavesdropping assault, Node impersonation	Data Accuracy, Authentication	Data verification, Privacy, Scalability, Availability
OBU	Sharing inter-vehicle safety related information	Sybil Attack	Data Accuracy, Authentication	Access Control
RSU	Controlling and supervising the whole network	Distributed Denial of Service	Data Accuracy	Access Control

- **Location tracking:** Here, the privacy issue emerges from the ability to view travel data and patterns over time, which can enable a malicious adversary to obtain other information about the vehicle owner or passengers, such as their residence and work as well as other establishments that they frequently visit. Determining the present location or historical travel patterns of a particular person could make them more susceptible to physical harm if the information is accessible to the wrong person. In this aspect, an individual's reasonable expectation of privacy includes concerns about how location data is collected and shared.

- **Sensor data:** In AVs, their sensors constantly collect data regarding their environments; Unfortunately, the sensors of AVs can be prone to hacking, leading to potential data leakage.

However, there have been multiple solutions for fortifying the privacy of CAVs that were implemented by researchers with successful results.

3.2.2. Data validation

CAVs generate a lot of data from their sensors that must be collected and analyzed. Furthermore, the data from CAVs need to be verified by the vehicle and/or user that obtained it to prevent any false reporting [123, 124]. CAVs are reliant on their sensors to assess their environment. Unfortunately, this means that the CAVs tend to trust the provided information from the sensors to formulate navigation decisions without data validation [20]. This leaves the CAV open to attackers; They could feed inaccurate sensor data to disrupt or take control of the system.

Data validation is also an issue in training and testing CAVs [20]. After all, a CAV is expected to have different behavioral conduct during activity than what was shown during testing [125]. Current validation approaches cannot handle this circumstance because they

need to consider all conceivable system behaviors in advance in the plan and approval measure for the independent vehicle [126]. Designers of CAVs would need to test for additional long hours of exposure and gather and validate that much data for validating is a significant issue. The data validation process must also check that the CAVs can recognize nearby or distant objects and guarantee that they will perform effectively in suboptimal climate conditions or degraded environment settings [98]. One way to make data validation easier for CAVs is by simulation. Simulation environments comprise several modules (e.g., Environment module, Vehicle module, Physics engine, Sensor module) [127]. Simulation and modeling tools greatly benefit data validation in the automotive domain due to their high-quality frameworks for design, analysis, data training, and validation [128]. However, simulation has its disadvantages—models trained solely on simulation data fail to generalize to the real world due to the differences between the simulated and realistic environments regarding both physical and visual entities [129].
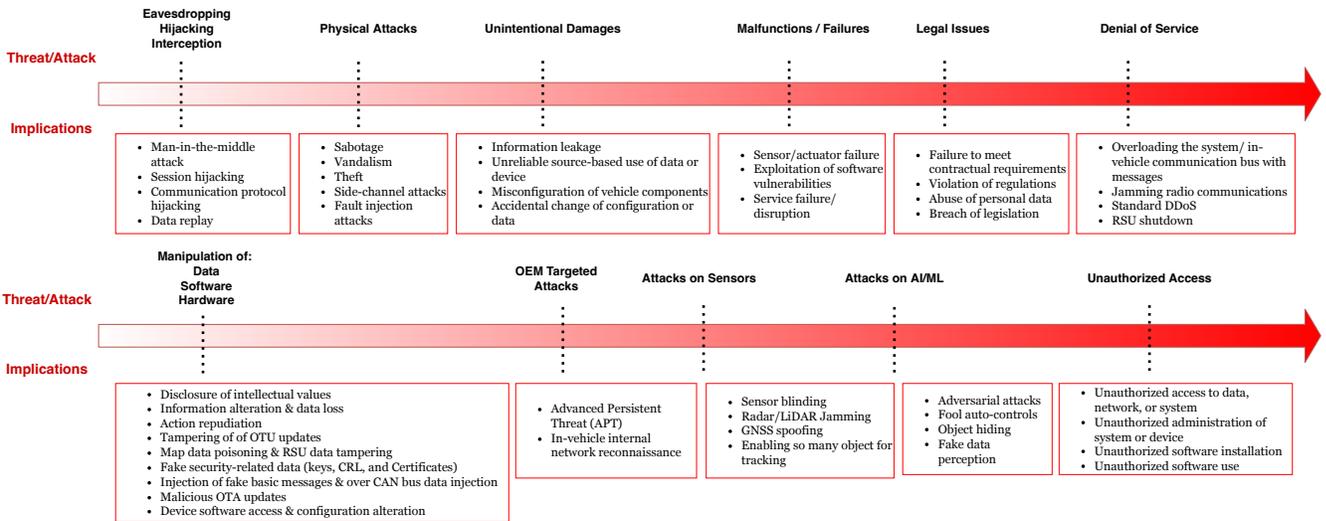

Figure 3: Taxonomy of threats and attacks against CAVs: visualizing the attack landscape.

3.2.3. Liability

While many works constantly emphasize the need for secure CAVs, these works also gloss over the fact that every decision made regarding the employment of security for CAVs, including the decision to provide little to no security at all, has consequences for the liability of both the manufacturers of CAVs, and those who are involved in implementing the security measures (e.g., algorithms, software, hardware). Security and liability are often correlated, especially concerning automobile accidents. In a typical car accident scenario, liability largely falls on the driver. In CAVs, other entities must be considered, including the manufacturer, software provider(s), service technician(s), and the vehicle owner. A significant challenge in the context of liability is determining the proportionate responsibility among various stakeholders when a security breach occurs. For instance, in cases where a CAV's decision-making process leads to an accident, it can be difficult to attribute fault to the vehicle's AI, its sensors, or the broader communication infrastructure. The introduction of autonomous decision-making further complicates legal responsibility, as traditional

concepts of driver liability no longer apply. One potential approach to mitigating liability concerns is the development of transparent and auditable security mechanisms that track decision-making in real-time, allowing for post-incident analysis. Furthermore, regulatory bodies need to evolve with these technological advancements to define clear liability frameworks that consider the distributed nature of CAV systems, ensuring that responsibility is appropriately assigned to manufacturers, software developers, or operators depending on the failure's origin.

3.2.4. Malware Detection

Malicious updates pose a critical danger to CAVs since such malware can cause accidents that may be life-threatening. Furthermore, the network of ECUs for CAVs is indeed linked to both the telematics and infotainer systems to which all the outside devices, vehicles, and infrastructures are connected. This high amount of connectivity gives the attacker multiple paths to have the malware enter the vehicle [130]. Attackers can also replace legitimate software with malicious software to get control over the CAV [131]. Malware detection also correlates with the safety of the CAV because attacks look for even the most trivial of bugs to gain access to the CAV. This, in turn, will lead to the endangerment of people's lives - both inside the vehicle and among other people on the road. As a result, security updates that address potential malware issues for CAVs must be robust to properly guarantee the CAVs' safety [132]. One of the key challenges in malware detection for CAVs is the rapid evolution of malware techniques, which can bypass traditional signature-based detection systems. Advanced persistent threats (APTs) that target vulnerabilities in the communication between CAV components—such as the infotainment system and the ECU—require sophisticated, real-time detection mechanisms. Machine learning-based anomaly detection systems show promise in identifying malware behaviors that deviate from established norms. However, these systems must be designed to minimize false positives, which can lead to unnecessary interruptions in the vehicle's operations. Another critical area of focus is securing the supply chain for software updates, ensuring that every stage—from code development to deployment—incorporates strong integrity checks to prevent the injection of malware into CAV systems. Future research should also explore distributed malware detection techniques that leverage the collaborative nature of CAV ecosystems, where vehicles share information about detected threats in real time, enhancing collective security.

3.2.5. Over-the-Air (OTA) Updates

Communication features enable secure over-the-air (OTA) updates for CAVs. OTA updates utilize communication channels to securely deliver software patches, firmware updates, and security patches to vehicles. Secure communication protocols are employed to ensure the integrity and authenticity of the updates, preventing unauthorized modifications and reducing the risk of tampering or malware injection during the update process. CAVs often receive software updates over the air, which introduces potential vulnerabilities if not properly secured. Malicious updates or compromised update mechanisms could lead to unauthorized access or control of the vehicle's systems [43]. While OTA updates offer significant convenience and efficiency in maintaining the security and functionality of CAVs, they also introduce several security risks. A major concern is the potential for a man-in-the-middle attack during the update transmission, where an attacker intercepts the update and injects

malicious code. To mitigate these risks, strong encryption and multi-factor authentication must be used to verify the authenticity of the update source and protect the integrity of the data during transmission. Another issue is rollback attacks, where an attacker forces the system to revert to an older, vulnerable version of the software. Implementing secure version management and update logs, which are cryptographically protected, can prevent such attacks. Moreover, the reliance on OTA updates emphasizes the need for redundant security measures that ensure a CAV can operate safely even if an update fails or is compromised. Further exploration into blockchain-based secure update mechanisms may offer decentralized, tamper-proof solutions for managing OTA updates in the future.

4. Taxonomy of Communication Security Attacks on CAVs

In this section, we present a taxonomy of communication security attacks on CAVs and briefly discuss the various types of attacks. Figure 3 illustrates this taxonomy. Generally, several components are involved in an attack on CAVs. The first component is *the attacker*, which is the source of the attack on the CAV. In the event of a system error, it is crucial not only to mitigate and resolve the issue but also to identify the attacker. Identifying the attacker helps reduce the likelihood of future attacks and offers insights into attack vectors (discussed next). Strengthening proactive security measures is therefore critical [26, 133].

The next component is *the attack vector*. The attack vector represents the path through which an adversary gains unauthorized access to a CAV. This can occur through physical or remote wireless access, enabling exploitation of vulnerabilities within the CAV [35]. Another important aspect of understanding and addressing security attacks on CAVs is the motivation behind them. According to [46], there are three common motivations for security attacks on CAVs:

1. **Interrupting operations:** The goal here is to compromise critical components required for autonomous driving, rendering the autonomous driving mode inoperable.
2. **Gaining control over CAVs:** In this scenario, attackers seek to gain control of the CAV, allowing them to manipulate its behavior, such as altering the vehicle's route, speed, or triggering emergency brakes.
3. **Stealing information:** The adversary aims to collect confidential information from the CAV, which can be used for future attacks. This may also include theft of the user's personal data.

Furthermore, the components of the AV (Autonomous Vehicle) play a significant role in security attacks on CAVs [134]. These components are crucial because many of them are vulnerable to attacks [135, 30]. Examples of these components include GPS, Lidar, MMW Radar, Ultrasonic Sensors, Cameras, OBD, ECUs, and CAN systems. Table 2 summarizes the components' capabilities, their tasks, and the types of attacks they are susceptible to. Notably, some components are vulnerable to multiple types of attacks, including spoofing and jamming [136]. Additionally, attackers may use certain components, like the ECU, as a means to carry out their attacks [40]. Other critical factors to consider include the importance of assets, the difficulty of attacks, detection rates, and the severity of both information leakage and physical damage, as elaborated in Table 3. Table 4 provides a summary of various attacks on CAVs.

Table 3: CAV attack threats categorized in severity from low (L), medium (M), to high (H).

	Focus	Severity
Asset Importance	Importance of each component	L - AV not affected, M - may influence functions, but no direct impact on operation, H - will cause direct damage to the vehicle
Attack Difficulty	Ease of conducting the attack	L - no relevant knowledge needed, not time-consuming, M - time-consuming, but requires a short time to learn required knowledge, H - extensive knowledge required
Detection Rate	Odds of detecting attacks via the users or vehicle	L - no function affected, M - some functions are affected, but the vehicle can detect it and warn users, H - attacks will influence operational functions immediately
Severity of Information Leakage	Type of data leaked and how much of the data was leaked	L - no private information is leaked, M - unimportant information is leaked, H - crucial confidential information is leaked
Severity of Physical Damage	Amount of damage sustained from the security attack, if any	L - not likely to cause physical damage to the user or vehicle, M - small hazards and damage is caused, but not fatal, H - high possibility of causing fatal injuries
Recovery Rate	Time needed to recover back to normal after attack is detected.	L - seconds, M - minutes to hours, H - hours to days

Moreover, categorizing communication security attacks on CAVs into intra-vehicle and inter-vehicle attacks is challenging because many attacks affect both levels of communication. CAVs rely on complex communication systems that include intra-vehicle communication (within the vehicle) and inter-vehicle communication (between vehicles or with infrastructure) [137]. Numerous attacks target the communication channels and protocols used by CAVs, aiming to compromise the entire vehicular network, rather than focusing exclusively on intra- or inter-vehicle communication [49]. For example, an attack on a CAV's internal communication system could hinder its ability to receive critical information from external sources or transmit data to other vehicles or infrastructure. Similarly, an attack on inter-vehicle communication could disrupt the coordination and safety of multiple vehicles within the network. Therefore, communication security attacks on CAVs often transcend the strict boundaries of intra-vehicle and inter-vehicle communication, making it difficult to categorize them strictly within one domain. An in-depth, general taxonomy of these attacks is presented next.

4.1. Zero-day Exploit

This attack is geared toward potential vulnerabilities. In a Zero-day exploit, vulnerabilities are critical and can result in other devastating security attacks until that vulnerability is taken care of [138]. For hacking CAVs, hackers can use a Zero-Day attack to affect either additional CAVs, the network of CAVs, or other programs, to transfer malware, and to pose serious threats [139]. A key challenge with Zero-day exploits is that they remain undetected until after an attack occurs, which leaves CAVs vulnerable for extended periods. Additionally, the interconnected nature of CAV networks means that a single exploit can spread quickly across multiple vehicles, amplifying the impact. Effective countermeasures, such as predictive threat intelligence and behavior-based anomaly detection, need to be developed to identify these vulnerabilities before they are exploited. Continuous software updates and patching strategies are essential to mitigate such risks.

4.2. Replay Attacks

Replay attacks send out a previously stored message to deceive other components on the CAV network. Messages used can include elements such as previous updates on traffic or road conditions, accident alerts, etc. [140]. As such, the attack usually stores these types of

messages and re-transmits them at different locations or times, so the components believe that these conditions are happening now, even though they occurred in the past. What makes this particular attack dangerous for CAVs is that replay attacks can be used in combination with other attacks, making the impacts more severe [35]. To defend against replay attacks, CAV systems need to incorporate time-sensitive authentication mechanisms that ensure messages are only valid for a specific timeframe. Moreover, cryptographic solutions, such as nonces or timestamps, can be implemented to validate the freshness of the transmitted data. Combining these techniques with intrusion detection systems can enhance the CAV network's resilience against such attacks. Real-time monitoring of communication patterns is essential to identify unusual message duplication or delays.

4.3. Relay Attacks

Relay attacks usually target the CAVs' communication systems [35]. A relay attack is capable of breaking distance restrictions in communication systems. They do so by placing devices between a signal sender and receiver and relaying signals between them. Simply put, an attacker intercepts communication between two entities and, without viewing or manipulating them, relays it to another component in the CAV. This type of attack can also target keyless entry systems of CAVs [141]. Relay attacks can be particularly dangerous in keyless entry systems, as attackers can unlock or start vehicles without physical access. To prevent such attacks, manufacturers are implementing technologies like signal jamming or limiting communication range. Additionally, using cryptographic methods to validate the proximity between sender and receiver can mitigate the effectiveness of relay attacks. Enhanced encryption and frequency-hopping techniques are also promising defenses.

4.4. DoS Attacks

This is one of the most common security attacks targeting any layer of the network model [142]. The idea of a Denial of Service (DoS) attack is to flood the communication network with irrelevant data so that the network cannot respond to genuine users. It is highly adaptive because this type of attack confuses and dodges anomaly detection systems [143]. DoS uses multiple devices to execute the same attack from different locations. DoS may result in damages to the vehicle and can potentially shut down the entire communication network. Many types of DoS attacks come in various types, such as a flooding attack, jamming attack, and others [123]. A significant threat of DoS attacks in CAVs is that they can disrupt critical vehicular functions such as collision avoidance and navigation. This poses serious safety risks, especially in high-speed or congested environments. To counteract these attacks, CAVs need to implement more robust network segmentation, where high-priority messages are isolated from low-priority traffic. Additionally, AI-driven anomaly detection can help identify early signs of DoS attacks by analyzing unusual network behavior.

4.5. Sybil Attack

The Sybil attack is considered one of the most dangerous attacks on CAV networks. This attack involves falsifying the identity of the vehicle/user to disrupt the normal operation of the network [144]. There are two ways to execute a Sybil attack: one way is by assuming multiple identities to provide false information and have it appear like the information is coming from multiple devices, and the second way is impersonating another's identity and

providing false information [145]. Sybil attacks exploit both the topology and mobility of the network and can provide false information about its location; using that, it can provide false information about events at those locations [123]. Further, by creating multiple fake identities or nodes, adversaries in a Sybil attack can deceive the CAV network, leading to several security vulnerabilities [146]. Firstly, fake identities can disrupt the establishment of secure communication channels between vehicles (inter-vehicular communication). These malicious nodes can inject false messages or interfere with the transmission of legitimate messages, causing confusion, misinformation, or even DoS. Secondly, Sybil attacks can compromise the trustworthiness and integrity of the communication network by spreading false information [147]. For instance, fake identities can provide inaccurate data about a vehicle's position, speed, or intentions, leading to potentially dangerous situations such as collisions or incorrect decision-making by other vehicles [147].

4.6. Blackhole Attack

In this scenario, an attacker coerces other components into transmitting as much network traffic as possible to an attacker node [148]. A blackhole attack is executed by informing other entities in the network that the attacker node has the shortest route to their objective. Then, when an entity sends data packets to the attacker, all of them are dropped. This leads to data loss for the network. A blackhole attack causes critical damage by dropping essential data packets, for example, accident alerts [149]. To mitigate blackhole attacks, CAV networks can use multipath routing techniques, where data packets are transmitted through multiple paths instead of relying on a single route. This reduces the likelihood of data being lost entirely if one path is compromised. Additionally, continuous monitoring of routing behaviors and real-time detection of anomalies in data flow can help identify blackhole nodes early. Implementing reputation-based systems can also prevent malicious nodes from misleading the network by dynamically adjusting trust levels for each node.

4.7. Passive Eavesdropping Attack

This kind of attack is known as a reconnaissance or stealth attack and involves collecting as much information about a network as possible by constantly monitoring the network traffic. The attack analyzes the traffic to recognize patterns and deduce information regarding the vehicles [150]. This information is then used to carry out attacks by either identifying key entities or replaying recorded network transmissions to act as a smokescreen to avoid detection. Insecure or unencrypted communication channels within the vehicle (intra-vehicle communication) are the key enablers for attackers to eavesdrop on sensitive information. This includes data on passenger privacy, location, or personal preferences [97]. To prevent passive eavesdropping, CAV systems must employ strong encryption protocols for both intra- and inter-vehicular communication. Regular updates to encryption algorithms are critical to staying ahead of evolving eavesdropping techniques. Additionally, implementing secure key exchange protocols will ensure that even if communication is intercepted, the attacker cannot decrypt the data. Lastly, continuous monitoring of network traffic and the use of obfuscation techniques can help obscure patterns that attackers might otherwise exploit.

4.8. Side-channel Attacks

A side-channel attack is a type of security attack that exposes important information in terms of transmitted data or the inner mechanisms of the CAV system via alternative routes

[151]. A side-channel attack tries to obtain information indirectly and mainly exploits information leakage [26]. Side-channel attacks are particularly challenging because they do not target the software directly but rather exploit physical phenomena such as power consumption, timing, or electromagnetic emissions. To defend against such attacks, CAV systems need to implement hardware-level countermeasures like noise generation and power equalization, which make it difficult for attackers to deduce meaningful information from side-channel data. Additionally, securing cryptographic operations from side-channel leakage is critical in ensuring that sensitive operations cannot be monitored. Future research should focus on developing side-channel attack-resistant architectures for CAVs.

4.9. Code Modification and False Data Injection

These attacks target the OBD-II scanner and affect the ECU [26]. Specifically, the OBD-II scanner enables personnel to perform diagnoses of CAVs, and more advanced versions can modify a part of the ECU, such as the ECU code. Unfortunately, adversaries can exploit these tools to execute malicious code modifications to compromise the CAV [25]. Further, adversaries may attempt to inject false data into the communication network, misleading vehicles about road conditions, traffic patterns, or obstacles. This can disrupt the cooperative behavior of autonomous vehicles and potentially cause accidents [152]. Code modification attacks can be mitigated by securing diagnostic tools like OBD-II scanners with encryption and access control mechanisms, ensuring that only authorized personnel can modify the ECU. Additionally, integrity-checking algorithms should be implemented to detect unauthorized changes to the ECU code in real-time. False data injection attacks can be countered through redundancy in data sources, where vehicles cross-check information from multiple sensors or other vehicles to detect inconsistencies. Securing sensor data with cryptographic signatures can also help prevent tampering.

4.10. Packet Sniffing

In CAVs, particularly for communication, a packet sniffer is an entity that can intercept and log traffic transferred over a communication link. Packet sniffers are typically used for diagnosing network-centric issues [153]. In simpler terms, packet sniffers allow viewing communication information between two or more nodes. While useful, an attacker can use packet sniffers to access unencrypted data and obtain information. Packet sniffers can also be used for a replay attack [26]. To prevent packet sniffing attacks, CAV networks must employ end-to-end encryption for all communication channels, ensuring that even if data is intercepted, it remains unreadable to attackers. Furthermore, intrusion detection systems can be configured to monitor for abnormal data interception activities, triggering alerts when unauthorized sniffing is detected. Employing secure tunneling protocols such as VPNs can further add a layer of protection to sensitive communication. Ensuring timely updates of encryption protocols and implementing secure key exchange methods is also critical.

4.11. Sensor Spoofing

A sensor spoofing attack can severely impact intra-vehicular communication security in a CAV. In such an attack, adversaries manipulate or deceive the sensors within a vehicle to provide false or misleading information [154]. This can compromise the integrity of the

intra-vehicular communication system, leading to several security threats. Specifically, sensor spoofing can impact the perception capabilities of the vehicle, causing it to misinterpret the surrounding environment [155]. For instance, if the spoofed sensors provide inaccurate data about the vehicle's position, speed, or the presence of obstacles, it can lead to incorrect decision-making and potentially hazardous situations. Additionally, the compromised sensors can propagate false information within the vehicle's internal communication network, affecting the cooperation and coordination among different systems and components [156].

4.12. Packet Fuzzing

In a packet fuzzing approach, invalid data gets sent over to the targeted CAV component(s) or module(s) to explore the likelihood of triggering an error condition or fault [157]. These error conditions result in vulnerabilities that are exploitable and reveal security loopholes. Ironically, Packet fuzzing can also be used for security testing. When used for testing the security of CAVs, fuzzing is implemented for detecting potential problems in the CAV system that could contribute to security issues at a later stage [26, 158].

4.13. Communication Jamming

Malicious actors can jam communication signals between vehicles or with infrastructure systems, disrupting the flow of critical information and resulting in communication breakdowns [159]. Here, adversaries deliberately interfere with the wireless communication signals between vehicles (inter-vehicular communication), causing disruptions or complete DoS. This type of attack can disrupt the exchange of critical information among vehicles, leading to compromised safety, coordination, and situational awareness. By jamming the communication channels, adversaries can prevent vehicles from receiving important messages, such as collision warnings, traffic updates, or cooperative maneuvering signals. As a result, CAVs may fail to respond appropriately to changing road conditions or the presence of other vehicles, increasing the risk of accidents [156]. Moreover, jamming attacks can create confusion within the vehicular network, as vehicles may lose connectivity with each other and the infrastructure, leading to a breakdown in cooperative operations and coordination.

4.14. Attacks on Global Positioning Systems (GPS) and Localization

The GPS delivers position data with an accuracy level. An increased number of satellites has been deployed to provide better GPS coverage and overcome the reported difficulties and obstruction impact in connected vehicles [30]. Although the public GPS domain is an openly accessible standard, rogue signals can be feasibly carried out to block or mislead GPS-based devices. This adversarial conduct leads to jamming and spoofing attacks, which involve disseminating wrong yet valid and realistic GPS signals to misguide the receivers. As such, the adversary can broadcast synchronized signals (i.e., synchronization with valid signals observed by the target receiver) to alter the target position increasingly.

Moreover, the creation of plug-and-play attack devices is becoming a reality since the GPS spoofing rewards are augmenting in parallel, and theories on how to conduct the attack are already publicly available [160]. Examples of proof-of-concept attacks can be concluded from the existing literature, e.g., establishing a counterfeit GPS signal to overpower genuine signals of the GPS incrementally.

Last, anomaly detection for GPS is another solution proposed to enhance autonomous driving security [161]. The key motivation is to provide sufficient security measures for the GPS sensor, as protecting an environment in constant motion will be challenging in regard to securing against attacks and detecting threats. A model is proposed in [161] to help secure the GPS sensor based on deep learning. The model further managed to improve both the accuracy and scalability of the vehicle.

4.15. Adversarial ML Attacks on Perception Systems

This subsection discusses examples of adversarial ML attacks on CAVs' perception systems. Typically, the adversarial attacks on ML comprise two categories: poisoning attacks and evasion attacks. The poisoning attacks primarily impact the training stage during the learning process. The adversary here aims at compromising the learning process of ML/DL via a successful manipulation of the data used in the training phase [162]. Unlike poisoning attacks, evasion attacks mainly target the inference stage of the learning process. The adversary in this scenario aims to create a false output by manipulating the real-time inputs or the test data in the ML model [163]. Note that the examples utilized in falsifying the ML/DL applications during the inference stage are generally called adversarial examples.

Further, an attacker may aim for a partial perturbation of the images collected by cameras in a CAV. The goal is to make the ML/DL implemented for the vehicle's vision application produce incorrect predictions. Although the DL modules implemented within Electronic Control Units (ECUs) are the primary targets of this adversarial attack, cameras also enable adversarial channels to inject malicious images at ease. Additionally, adversarial patches and stickers with patterns were successful in fooling a broad range of artificial algorithms [164]. An adversary can easily print and bind these pattern-based adversarial stickers to critical transportation objects like road and traffic signs.

Several research efforts have further demonstrated the feasibility of misleading AI algorithms for traffic sign classification. Notably, unlike the attack setups carried out by authors in [165], which were not successful in compromising the stop signs through a neural network (NN) model, authors in [166] were more successful in their proposed attack mechanism. Specifically, the authors decorated the traffic signs using light black and white adversarial patches, which led to the learning algorithm failing to identify the stop signs by a moving vehicle efficiently.

The authors in [167] have performed a similar adversarial scenario by remotely leveraging the electromagnetic interference while leaving traffic signs physically unmodified (i.e., without adversarial patches). The authors' setups made the adversarial attack easy to conduct but challenging to identify. Although there are little to no experiment explorations against the CAVs, such an adversarial model can be applied to them with ease. This is of great concern in CAVs as they become inefficient in identifying traffic alerts or even falsely read speed limits. Furthermore, adversarial ML-based sensor attacks on the Lidar-based perception in autonomous driving can lead to semantically impactful security results in CAV settings. Here, an attack goal could be fooling the Lidar-enabled perception to perceive untruthful obstacles before a victim's CAV. As a result, the driving decisions will, in turn, be maliciously manipulated. An example of such attack implementation is presented in [168]. The authors herein conduct the Lidar-based perception system attack by targeting the front-near false obstacles near the front of a victim CAV (i.e., assuming this scenario can provide the highest

Table 4: A taxonomy of existing security attacks against CAVs.

Attack	Main Target(s)	Impact(s)/Implications
Blinding	Camera	Disruption of visual environment representation
Spoofing	GPS Lidar MMW Radar Ultrasonic Sensors	Disseminate wrong but realistic signals Create counterfeit GPS signals
Jamming	GPS MMW Radar Ultrasonic Sensors	Disseminate wrong yet realistic signals Misguide signal receivers Perform plug-and-play attack
Relay	Lidar	Break distance restrictions in systems Target keyless entry systems of vehicles
Malicious OBD Device	OBD Port	Explicit violation of logical constructs and controls to manipulate the vehicle's
DoS	Intra/inter-communication CAN OBD ports	Target the CAN protocol Transmit volume of high-priority messages via OBD ports Disrupt processing of legitimate traffic
MITM	Intra/inter-communication	Access unencrypted data Intercept messages exchanged between vehicles
Remote Exploitation	OBD Port	Execute code on telematics via long-range wireless connections
Zero-Day Exploit	Intra-Vehicle Network	Transfer malware Cause average to critical threats
Replay	Intra-Vehicle Network	Deceive vehicle's network components Perform location-enabled message tampering
Sybil	Intra-Vehicle Network	Falsify vehicle/user's identity to disrupt network operation Exploit topology and mobility of the network Deliver false information in events and locations
Blackhole	Intra-Vehicle Network	Coerce components into transmitting packets to the attacker node Drop essential packets (e.g., accident alerts)
Eavesdropping	Intra-Vehicle Network	Constant monitoring of network traffic Recognize patterns and deduce information Replay recorded packets to avoid detection
Side-Channel	Intra-Vehicle Network	Expose data and inner mechanisms via alternative routes
Code Modification	OBD-II scanner ECU	Execute malicious modifications of code
Sniffing	Intra-Vehicle Network	Gain access to unencrypted data Perform replay attacks
Packet Fuzzing	Intra-Vehicle Network	Transmit invalid data Trigger an error condition or fault
Adversarial ML: Poisoning & Evasion	Sensing Image Construction	Compromise the image learning process Target the inference stage of the image learning
CAN Access via OBD-II	CAN	Perform DoS attack Perform eavesdrop attacks Transmit unauthorized data
ECU Access via CAN	ECU	Compromise ECUs on the CAN Perform code injection, code reprogramming
CAN Access via Telematics ECUs	CAN	Compromise the CAN Bypass intrusion detection and cryptography

potential to launch an immediate faulty driving decision). Moreover, Lidar spoofing attacks are considered in the attack model presented in [168] since they are proven practical attacks against Lidar perception sensors [169]. Lastly, laser aiming can also be performed in this attack scenario. Here, the adversary can deploy techniques such as camera-based object identification and tracking [168]. From the CAV settings perspective, such adversarial attacks are stealthy as the shooting-based laser devices are significantly small, and laser pulses are considerably invisible.

Currently, various adversarial mechanisms exist to tamper with ML implementations for object detection tasks, like traffic signs. Such mechanisms are usually referred to as universal adversarial perturbations [170, 171, 172]. Last, an IBM research group published Adversarial Robustness 360 Toolbox, an open-source library developed in Python to simulate and thwart adversarial attacks on ML-based image tasks [173]. Figure 3 provides a summary and visual taxonomy of the existing security attacks and threats against CAVs, along with their primary targets, impacts, and security implications. Additionally, when determining the severity of attacks, it is helpful to base these attacks off specific parameters such as those in Table 3. Throughout this sub-section, the attack taxonomy and current attacks on CAVs were

discussed. While the majority of CAV components are prone to jamming and spoofing, it is essential to distinguish between the types of jamming and spoofing attacks the components of CAVs are prone to. Not every jamming or spoofing attack works the same way when attacking a specific component of a CAV.

5. Communication Security Solutions and Evaluation Tools

Communication features play a crucial role in security solutions in CAVs [174]. For instance, secure communication protocols, such as Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS), establish encrypted and authenticated communication channels between CAVs and infrastructure. These protocols utilize cryptographic algorithms and digital certificates to ensure secure identification, authentication, and key exchange between communicating entities. However, CAVs face numerous formidable challenges, including liability, privacy preservation, real-time response, data validation, and malware detection, as previously highlighted in Table 2. Many solutions have been developed in this regard, and our discussion in this section will be focused on these advances.

5.1. Privacy

Communication features are employed to ensure secure data transmission and privacy preservation in CAVs [175]. Encryption mechanisms, such as symmetric or asymmetric encryption, protect the confidentiality and integrity of data transmitted between vehicles, infrastructure, and other entities. Privacy-enhancing technologies, such as data anonymization or pseudonymization, can also be applied to protect the privacy of individuals while enabling necessary communication and information exchange. An overview of existing solutions aiming at CAV communication privacy enhancement is provided next.

5.1.1. Location Privacy- Stealthy Tracking of CAVs

In [176], the authors specifically focus on location privacy. The authors emphasize that the location privacy of CAVs can be compromised via software side-channel attacks. Side-channel attacks happen when the vehicle's driving software and the attack software share a hardware platform and can reveal the physical properties of a vehicle or its environment. Interestingly, this type of attack exploits a vulnerability in the Adaptive Monte-Carlo Localization (AMCL) algorithm, which has been widely utilized in CAVs. To prove their point, the authors simulate a side-channel attack; To evaluate the effectiveness of their attack, the authors used real-world data collected on a Nissan Leaf driving around Oxford. This was to ensure the attack was tested in a realistic environment. Upon testing, the authors achieved a route prediction accuracy of 81%. The high accuracy of this attack highlights a critical need for enhanced defenses against location tracking in CAVs. Strengthening isolation between software components or implementing hardware-level countermeasures can reduce the risk of side-channel attacks. Furthermore, future work should explore machine learning techniques that can detect and mitigate side-channel vulnerabilities before they are exploited. Proactive identification of software-level leaks will be essential in preserving CAV location privacy [177].

5.1.2. Privacy-Preserving Three-factor Authentication and Key Agreement

In [178], the approach to privacy is cloud-based. Specifically, the authors propose a cloud-based architecture incorporating three-factor authentication and a key agreement protocol known as CT-AKA, the proposed framework integrates elements such as passwords, biometrics, and smart cards to ensure authorized access to both the cloud and CAVs. The biometric approaches the authors incorporated include fuzzy vault, fuzzy commitment, and fuzzy extractor to ensure there is no leakage of the users' privacy [179]. Furthermore, the authors' proposed framework includes two session keys: one between the user and CAV to ensure secure remote control of the CAV, and the other is negotiated between a mobile device and the cloud to make sure that security parameters are not compromised and to ensure cloud data access securely with a high guarantee of security.

The CT-AKA protocol has 6 phases: (1) system setup, (2) CAV registration, (3) user registration, (4) user authentication, (5) password and bio-metrics change, and (6) smart card revocation. In (1), the cloud boots the CAV system and initializes the system parameters. Next, in (2), the cloud generates and distributes a secret key for each CAV. In (3), the cloud issues a smart card storing the secret key to each user. For (4), the three-factor authentication is executed to verify the user identity and build secure channels among the cloud, the CAV, and the user. To verify the effectiveness of the proposed architecture, the authors used a tool called ProVerif, a type of protocol verifier that verifies mutual authentication between users, the cloud, and CAVs, and ensures the secrecy of the session key they have negotiated. Results indicated the proposed architecture does achieve secrecy and mutual authentication between the involved entities. Additional testing also revealed that the authors' proposed architecture is efficient even with a large number of users. The use of ProVerif to validate the protocol adds credibility to the framework's security claims, making it a viable option for real-world applications. However, implementing such a three-factor authentication system at scale might introduce latency concerns, especially for users accessing CAVs in high-demand environments. Future research could focus on optimizing the framework to reduce latency while maintaining strong security guarantees. Additionally, biometric data security must be prioritized to ensure that sensitive personal information is not exposed in the event of a breach [180].

5.1.3. SDN-based Secure and Privacy-Preserving Scheme

In the work of [181], the authors focus on the privacy of vehicular networks, which are quickly becoming incorporated into CAVs regarding communication. 5G has also been incorporated into CAVs due to its promise to make CAVs faster, smarter, and safer [182, 183]. Unfortunately, 5G still faces challenges in guaranteeing reliable and secure communications for CAVs [184, 185, 186]. The authors propose a Software-Defined Networks (SDN) centric architecture that provides end-to-end security and privacy in 5G-enabled networks for CAVs. The proposed architecture is meant to simplify network management while also achieving optimized network communications. There are two phases of operation: First, there is a cryptographic-based authentication protocol that authenticates authority in SDN-centric CAV setups. Then, there is an intrusion detection module that is meant to reduce computational complexity and determine possible intrusions in the network. The authors did an extensive evaluation of their framework using three simulators. Metrics that were evaluated included overall security in terms of the detection rate, false positive rate, accuracy, time

of detection, and communication overhead. The authors' proposed framework outperforms other frameworks (in terms of higher performance and lower communication overhead), making this framework highly applicable for securing privacy for CAVs. The integration of SDN into 5G-enabled networks offers substantial benefits for network management and privacy. However, one of the key challenges is the centralized nature of SDN, which could introduce a single point of failure in the system. Future research should explore decentralized SDN solutions to mitigate this risk. Additionally, optimizing the intrusion detection module to handle emerging 5G-based threats will be critical for maintaining robust security in CAV networks [187].

With such an SDN-assisted security solution, communication features can play a role in the following contexts:

- **SDN**: Allowing for dynamic, centralized management of network traffic, enhancing security by quickly adapting to threats and potentially isolating malicious nodes thanks to its decentralized and decoupled infrastructure.

- **5G**: Offering faster speeds, lower latency, and better support for device density than its predecessors. For vehicular networks, this translates to quick and reliable communication between vehicles (V2V), between vehicles and infrastructure (V2I), and with other networks.

- **Dynamic configuration**: With SDN's centralized control capabilities, the network can be dynamically reconfigured in response to observed traffic patterns, potential security threats, or specific vehicle requirements, thus enhancing the overall security and performance of vehicular networks.

- **Quality of Service (QoS) management**: Given the critical nature of some vehicular communications, SDN can prioritize certain types of messages, ensuring timely and reliable delivery, especially in scenarios where latency or bandwidth is a concern.

5.2. Data Validation

5.2.1. SAVIOR

The authors of [188] propose an architecture called SAVIOR to address data validation. SAVIOR is focused on both securing CAVs and data validation. The SAVIOR framework is inspired by what is known as the Physics-based Attack Detection (PBAD) model, where PBAD has two major steps. The first step is performed offline and extracts the physical components of the CAV to generate a model that captures expected correlations between the inputs and the outputs of the system. The second step is online and involves an anomaly detection algorithm that compares prediction with observed states and raises an alarm when the discrepancy between the predicted and the observed states exceeds a given threshold. What is most impressive about this framework is that it applies to both aerial and grounded CAVs. In the offline stage of this proposed architecture, parameters of the physical components of the vehicle are learned. The online stage is where the model is used to predict sensor measurements and compare them accordingly. Next, a prediction is made via the EKF and compared to the observed state. Lastly, the anomaly detection test shows if the differences between the observed and expected data are significant over time.

Robust physical invariants suggest using consistent physical or behavioral properties of vehicles to ensure their security. Communication features can play a role in the following contexts:

- **Data exchange and verification**: Communication protocols can be established where vehicles frequently exchange data about their physical state or surrounding environment. Using robust physical invariants, each vehicle can verify the authenticity of the received data, ensuring it matches expected physical behaviors or constraints.

- **Secure V2V and V2I**: In a CAV environment, secure V2V and V2I communications are vital. They can be designed to utilize physical invariants as a layer of verification, ensuring that received messages are consistent with the known physics of vehicles.

- **Anomaly detection**: By continuously monitoring and comparing communicated data against established physical invariants, it's possible to detect anomalies that might indicate malicious activity or sensor spoofing.

- **Tamper-proof logging**: Communication features can be used to maintain tamper-proof logs based on physical invariants, ensuring a secure record of vehicle behaviors and states for post-analysis or forensic purposes.

- **Feedback and control**: Secure communication channels might provide real-time feedback to the vehicle's control system if deviations from expected physical invariants are detected, enabling corrective actions or emergency measures.

- **Collaborative verification**: In dense CAV environments, neighboring vehicles can collaborate through secure communication channels to verify each other's reported physical states, providing an additional layer of security through distributed consensus.

5.2.2. Validation Database - Relevant Traffic Scenarios

In [189], Pütz *et al.* tackles the challenge of data validation by adopting a database-centric approach. Specifically, the authors implement a database called PEGASUS, which addresses the challenge of collecting and validating data for CAVs. According to the authors, The PEGASUS database contains relevant traffic scenarios for training CAVs. PEGASUS combines different database entities and a data processing approach that determines the required test specifications based on various types of collected input data. The types of input data collected could include traffic simulation data, driver simulation data, field data, and others.

In step 1, the data owner generates a common environment and traffic description. Only the data owner can convert the recorded data into a suitable format. Step 2 is the first step for data processing and validation. It is concerned with the correct data formatting and indexes and assigns access rights based on data provider requirements. Step 3 involves enriching the raw data to interpret potential scenarios CAVs may encounter. Step 4 involves calculating the likelihood of a situation, and Step 5 aids in scenario interpretation. Step 6 is where the scenarios are clustered into predefined logical scenarios, and the parameters of the recorded scenario events get transferred into frequency distributions. Step 7 is where the testing and data validation happens.

5.2.3. Simulation-Based Platform - Algorithm Validation

While not explicitly focused on the 'data' validation aspect, the work [190] explores another aspect of data validation that the previous examples did not cover: the algorithms used for data validation. The algorithms used for validating data of CAVs are crucial to ensure the data validation process operates as smoothly as possible, and the algorithms themselves are efficient and flexible on the type of data formats used for CAVs. The author notes that developing algorithms for data validation of CAVs requires large quantities of training data. Still, the cost of collecting such training data limits the size and diversity of this data. To remedy this, the author implements a simulation-based platform for testing and validation that combines the autonomous driving simulator (CARLA) and their own approach. The proposed platform manages to be capable of both validation and development of data validation and autonomous driving algorithms.

5.3. Liability

5.3.1. Liability Attrition Model

In [191], liability for CAVs is discussed and categorized into two main types:

- **Product liability:** This refers to damages caused by product defects such as design and manufacturing shortcomings. In this case, the auto manufacturer is liable. If the car accident occurs while the vehicle is in autonomous mode, the software provider is liable, especially when a software program is determined to have led to the accident.

- **Negligence liability:** In this case, this refers to damages due to neglecting to execute an action. Here, the vehicle owner is liable when they do not execute an instruction from an auto manufacturer or software provider.

Furthermore, the authors also design and propose a liability attribution model. From there, the authors then implement a blockchain approach for liability attribution. In doing so, the authors' proposed architecture is resilient to evidence tampering, false information, and unavailable evidence. In doing so, this proposed framework fortifies security for CAVs by providing untampered evidence and allows for multiple participants to agree on evidence needed to process insurance claims. This architecture could be applicable in digital forensics, especially since liability for incidents that involve CAVs is a currently developing area of law.

5.4. Malware Detection

5.4.1. eUF

In [131], the authors develop a framework called Enhanced Uptane Framework (eUF) for the detection of malicious software updates in CAVs. The proposed solution uses a combination of transfer learning and Convolutional Neural Networks (CNNs) to enhance security. Regarding its architecture, there are two ECUs in eUF, the primary and the secondary. The primary ECU contains more storage and computational resources, so most functions are performed on this part. Meanwhile, the secondary ECU performs fewer functions (e.g., verification of hashes) to reduce the risk of man-in-the-middle attacks inside the CAV. Regarding the CNNs the authors used, the authors trained both CNNs for 20 epochs. Additionally, for training and testing of eUF, the authors created two datasets by collecting executables of

Windows and Linux operating systems. Overall, the proposed framework can distinguish between malicious and benign software executables with high accuracy.

Given such a solution, the communication features play a role in the following key contexts:

- **Authentication and verification**: A secure communication protocol would be established to authenticate OTA update sources. Cryptographic signatures might be used to ensure the update's legitimacy.

- **Encrypted communications**: To protect the updated data during transmission, encryption can be used to safeguard against eavesdropping or tampering.

- **Integrity checks**: After an OTA update is received, integrity checks can be performed to confirm the data hasn't been altered during transmission.

- **Behavior analysis**: Post-update behavior of the vehicle can be monitored to detect anomalies or deviations from expected behaviors. If the updated software behaves suspiciously, it might indicate a malicious update.

- **Version control and rollback**: Maintaining a secure record of software versions can help roll back to a previous, trusted state if a malicious update is detected.

- **Notification and alerts**: If a potential malicious OTA update is detected, it could have mechanisms to alert the vehicle operator, manufacturer, or other relevant entities.

- **Collaborative detection**: Such a solution could employ information from a fleet of vehicles. If multiple vehicles experience issues post-update, this collective information can aid in faster detection of malicious updates.

5.4.2. Security Architecture for Protecting CAVs from Malware

In [192], the authors propose a characterization of CAV malware and security architecture to protect the CAV from various malware. The authors attempt to characterize CAV malware in terms of intention, propagation, exploitation, types, and methods of attacks. Furthermore, the proposed architecture uses multiple computational platforms and the virtualization technique to limit the attack surface. There is also a real-time operating system (OS) to control critical vehicle functionalities and multiple other operating systems for non-critical functionalities (infotainment, telematics, etc.). The security architecture also describes groups of components for the operating systems to prevent malicious activities and perform policing (monitor, detect, and control).

5.5. Performance Evaluation Tools for Secure Vehicle Communications

Here, we discuss some evaluation tools that have also been developed for CAVs. Having these evaluation tools would provide further insight into the operation of the CAV, as well as its strengths and shortcomings regarding security. Interestingly, there do not seem to be too many evaluation tools that have been proposed. As such, in the future, more attention needs to be paid to designing evaluation tools for CAVs. Evaluation tools also need to account for current methods used in communication. Furthermore, when designing evaluation tools, they need to be multi-purpose, as some only have a few purposes.

5.5.1. SEPAD

Proposed in [193], this specific system is interesting since it is less of an 'architecture' but more of a platform for assessing security for self-sufficient driving. An interesting point when planning security systems for self-governing vehicles is what new technologies can the autonomous systems support [194]. Further, one also has to consider the alteration of parts of the self-sufficient vehicle, which is done either by coordinating new security arrangements or by performing assaults. However, there is a risk of damage to the vehicle. This is why many researchers implement theoretical models when developing security frameworks [195]. Unfortunately, the drawback of using theoretical models is that the results and data obtained may not mirror real CAVs [196]. So the creators proposed the Security Evaluation Platform for Autonomous Driving (SEPAD) to help scientists demonstrate their security models. Hence, newly created security components can be effortlessly incorporated and assessed in a sensible situation without danger to the specialist. Additionally, the architectural design choices can be demonstrated and evaluated in terms of security, leading to more precise assessments and helping researchers gain a better understanding of how to incorporate security into autonomous vehicles.

SEPAD uses numerous communication technologies as well, such as the IEEE 802.11p network to handle vehicle-to-vehicle communication. Authentication is covered by using ISO 15118 communication technology. SEPAD also contains 5 modules that can be used to enhance a secure development process, resulting in stronger and more intuitive mechanisms. These modules are: Simulate Attacks, Analyze Impact, Evaluate Risk, Adapt Security Strategy, and Evaluate in Operation; The simulated attacks module uses an attack simulation component of SEPAD to mimic relevant attacks from the attacker. Then, the Analyze Impact module simply analyzes the impact of the attack. The Evaluate Risk component deals with risk for the vehicle, the passengers, external persons, and the overall environment. It also provides information about the probability of an attack by providing data about the preconditions for an attack or how easy it is to execute in realistic environments. Then based on whatever risk(s) are found, the adapt security strategy module can be used to modify current security mechanisms accordingly. In the Evaluate in Operation module, an evaluation of the operating car is performed without implementing attacks to identify any possible issues introduced by the security mechanisms. Then the process repeats itself.

It is of utmost importance that one can evaluate the performance of a CAV's ability to secure communications [197, 198]. However, there does not seem to be much literature on performance evaluation tools used for evaluating a CAV's performance in securing their communication. This can present problems in verifying whether the CAVs are operating correctly and whether communication in CAVs is secure (and any possible data leakage is minimized). The following subsections address the topic of developing performance evaluation tools for securing CAV communication in detail.

5.5.2. V2X Testing

The authors of [39] specifically focus on V2X application technology for CAVs. V2X employs current information and communication technology to enable V2V, vehicle to V2I, vehicle to pedestrian (V2P), and vehicle to network/cloud (V2N/V2C) network connections [186, 182]. Specifically, the authors emphasize that the V2X technology is rigorously tested. A notable testament to the article is that it focuses on current evaluation methods for V2X

technologies for CAVs. An issue that the authors noticed is that the current evaluation approaches and tools used are independent, and each of them has only one or two testing purposes. The authors propose an end-to-end evaluation tool that combines virtual and real environments that can handle the testing task of the full communication protocol stack. While the article effectively discusses current evaluation tools for V2X testing, it falls short of detail regarding their proposed evaluation tool.

5.5.3. BEHAVE

While the research work in [199] does not explicitly focus on communication (the article concerns traffic analysis), it does provide an architecture for an evaluation tool called BEHAVE. Technically, BEHAVE is a simulator, but simulation tools have been used in the performance evaluation of CAVs. Therefore, this article is applicable to be included in this section. Interestingly, the authors note that available models and evaluation tools are not sufficient to fully evaluate mixed traffic scenarios because most of them focus only on the lower level control of the CAV [200]. Securing CAVs' communication is crucial for mixed traffic analysis because the CAV needs to communicate traffic data to its sensors, such as the changing of red light to green light, the location of other CAVs about traffic lanes, speed limit, and other factors [201]. The BEHAVE evaluation tool is powered via the agent-based traffic simulator CityMoS. Additionally, the BEHAVE evaluation tool also has a data monitoring component that accounts for different traffic scenarios. The framework also includes a way to visualize and evaluate the evolution of agent-specific parameters for traffic analysis.

5.5.4. VeRA

Risk analysis was studied as an essential use case related to developing CAVs [202]. Risk analysis/assessment concerns itself with determining whether the risk of an attack on the CAV is critical or minor. The main argument is that current risk analysis methods are either too time-consuming or not suitable for CAVs. To remedy these issues, a security risk analysis method called Vehicles Risk Analysis (VeRA) is developed to help evaluate the risks of attacks in the context of CAVs. VeRA uses a simpler analysis process and fewer factors in comparison to other benchmarks (e.g., SAE J3061), significantly reducing required analysis time without negatively impacting accuracy. A mathematical model is also deployed in this use case to assess risk value whereas the previous methods used the tedious process of looking up tables. VeRA can obtain the same analysis results in 43% less time compared to three other risk analysis methods-EVTA, RACE, and CSRL.

5.6. Analysis of Security Frameworks for CAVs

As we conclude our discussion on communication security solutions for CAVs, it is essential to evaluate how the proposed solutions compare with existing frameworks. The comparative analysis Table 5 provides a side-by-side comparison, highlighting the distinct advantages and potential limitations of each approach. This table synthesizes the key attributes of each framework, offering a comprehensive overview that aids in understanding their applicability in addressing the specific security challenges faced by CAVs. Such analysis is crucial for informing future developments and guiding the selection of appropriate security measures tailored to the needs of the CAV ecosystem

Table 5: Comparative Analysis of Security Frameworks for CAVs

Security Frameworks Comparison				
Feature	Proposed Solutions	Existing Solutions	Benefits	Drawbacks
Scalability	Highly scalable using distributed architecture	Often centralized, less scalable	Can handle large fleets of CAVs efficiently	More complex to set up initially
Robustness	Utilizes advanced encryption and AI-based anomaly detection	Relies on traditional encryption methods	Higher security against modern cyber threats	Potentially higher computational overhead
Flexibility	Modular design allows for easy updates	Rigid frameworks with infrequent updates	Quick adaptation to emerging threats	Requires continuous development effort
Ease of Implementation	Requires initial setup and training of AI models	Generally simpler to deploy	Customizable to specific fleet needs	Steeper learning curve for system operators
Addressing Vulnerabilities	Specifically targets intra- and inter-vehicular communications	Broad focus, not specific to CAVs	Enhanced protection for CAV-specific threats	May overlook broader cybersecurity concerns

6. Communication Security Protocols for CAVs and Best Practices

This section discusses prominent security protocols that have been newly developed for CAV and summarizes best security design practices.

6.1. Security Protocols

The typical well-known protocols include (but are not limited to): CAN (Controller-Area Network), LIN (Local Interconnect Network), FlexRay, MOST (Media Oriented Systems Transport), DSRC (Dedicated Short Range Communications), LTE-V (long-term evolution-vehicle), DSR (Dynamic Source Routing), AODV (Ad hoc on Demand Distance Vector), DSDV (Destination Sequenced Distance vector), and GPSR (Geographic Perimeter Stateless Routing). Since these well-known protocols have already been comprehensively discussed in previous work, we discuss new protocols. Table 6 gives a brief overview of the well-known protocols and their advantages and drawbacks and Table 7 discusses some newly proposed protocols that have been proposed for CAVs.

Some of the newer protocols were meant to alleviate the shortcomings of some more well-known protocols. These examples come from [203], [204], [205], [206]. These authors proposed newer protocols to fix some shortcomings of the AODV protocols regarding its performance in packet delivery, packet delay, and congestion.

6.1.1. Li-Fi Vehicle Network (Li-Net)

This protocol was proposed by [207] and uses Li-Fi, which is expected to have better connectivity, security, and bandwidth in comparison to WiFi. Li-Net is used for V2V and V2I communication. The protocol also tackles various highway scenarios that could occur with CAVs, with a focus on traffic congestion. As such, the protocol has potential use in managing traffic. Li-Net also manages to achieve low packet loss. Notably, Li-Net was tested as a use-case for smart cities in terms of collision avoidance. To further enhance Li-Net, the

41

Table 6: Summary of security issues related to well-known vehicular protocols along with their pros and cons.

Intra-Vehicle Communication Protocols				
Protocol	Area(s) of Focus	Advantages	Drawbacks	Security Issue(s)
CAN	Performance	Low cost, high reliability, relatively low bandwidth, easy configuration	Lack of message authentication, unencrypted traffic	Denial of Service
LIN	Remote application	Open source, cheaper than CAN, low complexity, low cost	Low bandwidth	False data injection
FlexRay	Fault tolerance, communication	High-speed communication, versatile system layouts, error detection capability	More expensive, higher complexity, lower voltage operating levels	Spoofing, Denial of Service, lacks confidentiality and authentication, eavesdropping, masquerading, injection, and replay attacks
MOST	Vehicular infotainment systems	High speed, flexibility	Limited work regarding security of MOST	Jamming, vulnerable to attacks targeting synchronization
Inter-Vehicle Communication Protocols				
Protocol	Area(s) of Focus	Advantages	Drawbacks	Security Issue(s)
DSRC	Security, communication	Flexibility, low latency	Low scalability	Jamming, spoofing, interference
LTE-V	Reliability	Wider coverage, better resource allocation	Unpredictable delays	Message flooding
Ad-Hoc Routing Protocols				
Protocol	Area(s) of Focus	Advantages	Drawbacks	Security Issue(s)
DSR	Route calculation, route maintenance, route discovery	Less latency, lower delay, lower overhead, efficient, high throughput, lower packet loss	Scalability	Malicious forwarding nodes
DSDV	Consistency, delivery time, packet rate	Less modification, congestion control	Low packet delivery rate, high overhead	Malicious routing updates, routing table poisoning
GPSR	Wireless routing	Little memory needed, scalability	Instability, inaccuracy	Location misreporting, excessive packet overload
AODV	Routing	Better communication performance, reduced communication overhead, quick response to changes	Congestion, instability	Blackhole attacks

authors in [208] proposed a scheduling method to better handle message transmissions. This proposed method was the Intel Quartus Prime II, which provided a simulation environment for the Li-Fi. Codes were separated for the sender and receiver nodes prior to analyzing their characteristics. The authors in [208] also conducted experiments on a regular VANET simulation that was prone to various message delays and message throughput issues. Test results revealed that the proposed scheduling method helped reduce packet loss ratios and average packet delay even more.

6.1.2. Authentication Based on Smart Card (ASC)

The authors in [209] proposed the ASC protocol, an anonymous and lightweight authentication based on the smart card. A low-cost cryptographic mechanism is used by ASC to authenticate the legitimacy of the users (vehicles) and to validate data messages. ASC consists of five phases: (1) user registration, (2) user login phase, (3) user authentication phase, (4) password change phase, and (5) data authentication phase. According to the authors, the user login and user authentication phases are intended to check for legitimacy. The password change phase aims to resist an offline password-guessing attack. Finally, messages are authenticated among vehicles in the data authentication phase. For testing, the authors used VanetMobiSim and they were able to reduce communication and computational cost by more than 50%. Further, ASC has a login identity that is changed dynamically to prevent an attack from linking a target vehicle, allowing the protocol to be anonymous. Although the authors provided formal proof of how their protocol treats the security issue, the proof would be dis-proven by the authors in [210].

Table 7: A review of recent CAV protocols.

Proposed Protocols			
Protocol	**Year**	**Area(s) of Focus**	**Benefit(s)**
ASC	2017	Authentication	Reduced communication and computational cost, anonymity, lower packet loss ratio
RHR	2019	Network bandwidth	Reduced communication overhead, improved performance, real-time feedback
SAP-IoV	2019	Privacy, Authentication	Better security and performance, reduced time cost
Distributed Multi-Channel MAC Protocol for VANET	2019	Flexibility, Network topology, Control channel access	No excessive overhead
CoMACAV	2019	Data transmission	Increased throughput
NC-MAC	2020	V2V/X broadcasting, Beacon transmission and reliability for VANETS	Improved reliability
MD-AODV	2020	Communication	Lower packet delay
Li-Net	2020	Connectivity	Reduced message delay
CVIP	2020	Scalability	High flexibility
DTMR	2021	Communication Overhead	Stability, applicable in highways and urban environments
PARRoT	2021	Mobility, Predictive Routing	Lower end-to-end latency
TLBGR	2021	Data Acquisition, Packet loss, Real-time data transmission	Avoid data congestion, high delivery rate of data packets
AnonSURP	2022	Location Privacy, Data Privacy	Reduced communication overhead, resistance from various known attacks

6.1.3. Secure Authentication Protocol for Internet of Vehicles (IoV)

The authors in [210] tested the ASC protocol and found that the ASC protocol suffered from numerous attacks (e.g., offline identity guessing attack, location spoofing attack, and replay attack) despite the authors in [209] claiming the opposite. The authors in [210] also found that the ASC protocol took a considerable amount of time for authentication and had issues with scaling. To fix these issues, a new protocol was proposed the Secure Authentication Protocol for Internet of Vehicles (referred to as SAP-IoV in our paper). SAP-IoV was supported with formal proof to demonstrate its security. For testing, the authors used an iPhone 6S smartphone as the testing platform; Specifically, the system specifications were: iOS 10.11, CPU Apple A9+M9 co-processor up to 2.1 GHz, RAM 2GB. Overall testing results showed the proposed protocol was more secure and can reduce the authentication time cost.

6.1.4. Decentralized Privacy-preserving Routing Service Protocol (DPPRSP)

In [211], the authors propose a decentralized privacy-preserving routing service protocol (referred to as DPPRSP) with a focus on location. The authors emphasize that in most current routing services, users give their individual location data directly to routing services in exchange for route recommendations. Since this data is associated with the users' identity, schedules, habits, preferences and other private information can be inferred through repeated interactions with routing services. This would support the need for privacy preservation so that user's data is not compromised. To provide strong security, DPPRSP uses the Laplace mechanism in combination with Secure Multi-Party Computation (SMPC) to provide privacy and ensure the protocol is cryptographically secure. Although the Laplace mechanism is used for enforcing differential privacy, it tends to return semantically impossible values, such as negative count [212]. Nevertheless, DPPRSP can obtain the aggregate effect of traffic on travel time, allowing an estimate of travel time accurately and privately. The authors conducted experiments using the Sioux Fall transportation network and were able to demonstrate that DPPRSP manages to provide minimal performance overhead and guarantees privacy.

6.1.5. B-IoMV

The work in [213] is unique in the sense the article covers the Internet of Military Vehicles (IoMVs). While this is technically out of the scope of this paper, the article is justified in being included since it addresses relevant concepts, concerns, and methodologies for CAVs. Furthermore, [213] incorporates blockchain technology for building the proposed protocol. Specifically, the proposed protocol, B-IoMV addresses issues relating to security and anonymity. Upon testing, the authors of the proposed protocol showed that the B-IoMV system achieved better communication latency, data storage cost, and network bandwidth utilization.

6.1.6. AnonSURP

The authors in [214] propose an anonymous and secure ultra-lightweight RFID protocol for the Internet of Vehicles called AnonSURP. AnonSURP aims to ensure the user's location privacy, and data privacy, and to resist typical known attacks. Upon conducting an informal analysis, the authors were able to confirm that AnonSURP meets the various security requirements and provides resistance to various known attacks. The authors also conducted a comparative analysis against other protocols and noted that AnonSURP outperformed other protocols in terms of performance.

6.1.7. Hybrid Software-Defined Networking-based Geo-graphical Routing Protocol (HSDN-GRA)

The authors in [215] propose a novel protocol for CAVs called HSDN-GRA (Hybrid Software-Defined Networking-based Geo-graphical Routing Protocol). The authors note that SDN is optimal for CAVs due to reduced interference, the ability to increase exploitation of wireless channels, and enhanced resource management for networks. HSDN-GRA uses a clustering approach and considers three factors: (1) contact duration between vehicles, (2) each CAV's available load, and (3) log of communication errors. By considering multiple criteria, HSDN-GRA enables choosing the most trustworthy CAVs by avoiding communication problems and ensuring there is connection availability. To test HSDN-GRA, the authors compared it against a few other protocols: MA-DSDV [216] and PSO-C-MA-DSDV [217]. Simulation of their network was done on the JADE simulation platform. HSDN-GRA managed to outperform the other two protocols and achieve better throughput and stability and minimal overhead.

6.2. Lessons Learned

When designing security protocols for CAV communication, it usually includes the accompanying crucial steps: (1) identify security objectives and requirements of the system; (2) assess the CAV's value and sensitivity to be protected; (3) define security policies in accordance with the security requirements; (4) estimate the potential adversaries capabilities; (5) design those protocols that align with the sensitivity of the system and the risks it is exposed to [218]. Further, when studying the cybersecurity of CAVs, it is useful to recognize steps and cycles where individuals are engaged while considering the CAV's life-cycle security [219]. The people, social, and environmental factors are some of the key sources of weaknesses inside CAVs, which can fluctuate from system to system [13].

6.2.1. Defining Security Objectives

To improve intra- and inter-vehicular communications, security objectives must consider the management and people aspects for CAVs [220], [221]. As such, it is imperative that when implementing the security protocols, security objectives are designed in a way where everyone can understand what is being required (security is meaningful only when people understand what needs to be focused on [42]). Having clearly defined security objectives for these protocols not only allows us to consider the cost of potential cybersecurity attacks but also the cost of implementing security mechanisms and the opportunity cost of limiting certain features for protocols [222]. Even so, the primary objective for designing security protocols must be concerned with the resilience of the CAVs' safety feature functions [218].

6.2.2. Establishing a Trust Model

The Trust Model is essential to all useful security designs, including protocols, since it sets up the foundation of who is reliable, permitting clients to figure out what can be trusted, and empowering the architects to figure out who is the trusted authority for executing these protocols [223]. Security protocols should begin from a reasonable and practical trust model, with cryptographic systems being established afterward to protect the communication of data exchange and guarantee that no malignant assailants can bypass them [43]. The trust model is particularly significant in the CAV's communication connectivity infrastructure [224, 225] because the communication connectivity aspect of CAVs includes establishing and preserving identity and privilege management of the involved devices for CAVs [226].

6.2.3. Establishing a Security Perimeter

By using a security perimeter, the CAV is segregated into different security domains, each having different threat environments [227]. This would improve the design and implementation of security protocols for CAVs' communications in terms of adaptability and flexibility. By establishing security perimeter(s), the proposed security protocols can distinguish between cybersecurity incidents and physical tampering attacks of CAVs [228]. Ultimately, including security perimeters in security protocols enables a systematic and comprehensible approach to communication security analysis and the overall design of the CAV.

6.2.4. Establishing a Secure and Trustworthy Network Management Infrastructure

Security protocols must have a secure and trustworthy network management infrastructure to ensure a balance between preventing malicious attackers from exploiting potential vulnerabilities and efficient communication so that data can be exchanged quickly, allowing enhanced communications [149]. Network management is crucial for security protocols as they must account for resource constraints in CAVs' devices. The resource constraints in the CAV's devices imply that there needs to be accountability for how much bandwidth can be allocated, which security protocols must consider [229]. Although there are several components that need to be included here, we precisely cover the following two, as they are relevant to security and communication protocols.

- **Infrastructure for trust management**: Some primary examples of communication are V2V and V2I [149]. In these types of communications, control systems for admitting new nodes and detecting malevolent nodes are important prerequisites to keep the security protocols intact [230].

- **Heterogeneous network integration**: Because CAVs are integrated with a variety of devices, they usually have a mix of wireless communication systems, and these often come with their own security protocols [231]. Hence, when designing security protocols for CAVs, they need to be generalized enough to account for all involved devices. As such, interoperability is an important aspect of security protocols as well since the communication of data for CAVs may require different conversion of data formats [232, 233].

Other best practices should be considered as well, such as communication overhead, throughput, and run-time. These additional metrics should be considered when designing security protocols as a protocol that is secure but slow will result in massive delays in data transmission. While there may not be a guarantee that the protocol will run as fast as possible on every component of the CAV (due to the components' restraints), there should still be effort dedicated to minimizing delays in communication.

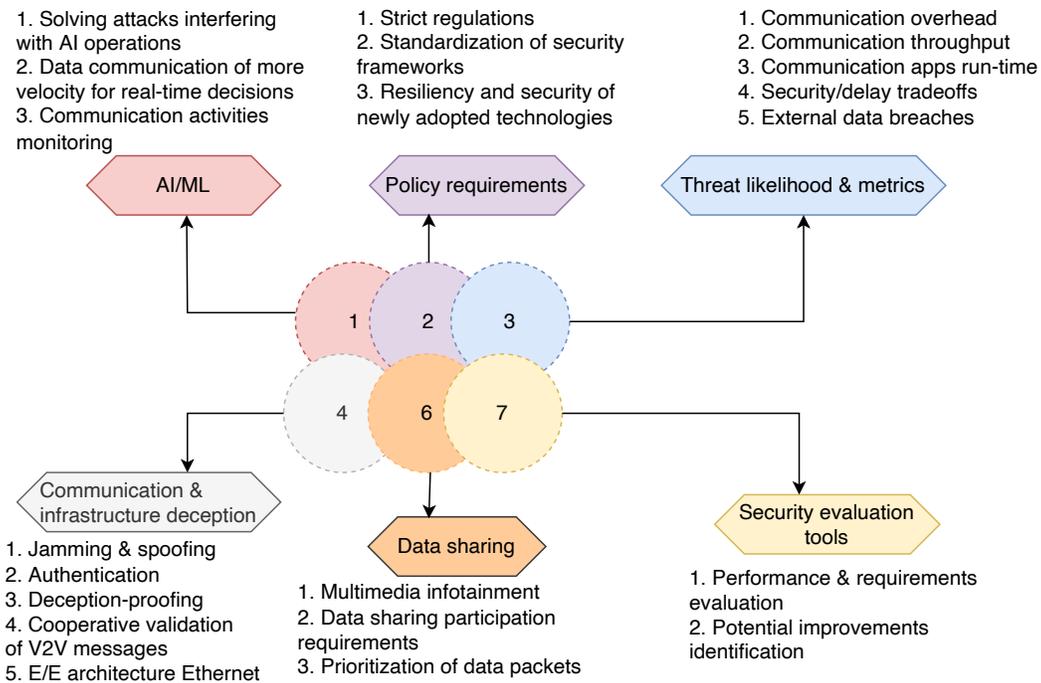## 7. Open Issues and Future Directions

Figure 4: Categorizing future research avenues in CAV security: a taxonomy.

Overall, many security architectures have been proposed for CAVs. Unfortunately, there is a lack of standardization for security frameworks for CAVs. This could be because there are multiple aspects to consider when designing security architectures for CAVs, such as privacy, data leakage, communication ranges of CAV devices, and others. As seen in the discussed security architectures, it is imperative to evaluate proposed security frameworks to ensure the framework can be applied to CAVs. New technologies can be incorporated for building security frameworks for CAVs, such as blockchain and edge computing. However these new

technologies still need to be flexible, efficient, and secure to ensure less likelihood of data leakage.

Various security challenges have been addressed through existing CAVs' solutions and protocols. However, some challenges remain significant in some of these solutions. The biggest challenges mainly include privacy, real-time response, data validation, and liability. Very few articles have attempted to mitigate these four key challenges with their own implementations, achieving optimal results in the process. A few limitations also persist in some existing vehicular protocols such as the FlexRay protocol. Precisely, there are lower operating voltage levels, which contribute to problems for extending network length. Additionally, some CAV protocols have only been implemented in high-end vehicles. As a result, it is difficult, or even impossible, to predict how the protocol would work for CAVs that are not premium [234].

It is important to implement CAVs' protocols to satisfy higher security and performance requirement levels, such as fault tolerance, dependability, bandwidth, and other related factors for intra- and inter-vehicular communications. The key open challenges and research directions related to CAVs and their communication security are depicted in Figure 4 and discussed in detail next.

7.1. Strict Regulations

Unlike traditional vehicles, where the vehicle's key control belongs to the driver, the driving task of CAVs is partially or completely controlled by the autonomous driving system. In order for this system to enable control and decision-making tasks, it significantly depends on the CAV's status (e.g., high precision maps, road conditions, etc.) that is gathered by communication components and sensors in real-time. As a result, a second delay may occur, leading to catastrophic incidents/accidents. Therefore, rigorous requirements and regulations must be designed and implemented to enhance the resiliency and security of CAV communication by minimizing this type of delay within the autonomous driving process.

7.2. Standardization of Security Frameworks

Despite the existence of remarkable security architectures for CAVs, a lack of standardization remains considerable for some of the proposed security frameworks of CAVs as there are various aspects to consider when designing its security architectures, including privacy, data leakage, and vehicular communication ranges. Further, newer technologies can be incorporated in the future to design security frameworks for CAVs, such as blockchain and edge computing. Several existing solutions have already incorporated such technologies. However, future work must consider flexibility, efficiency, and reliability to ensure less likelihood of data leakage.

7.3. Threat Likelihood and Metrics

Several existing solutions and protocols are considered reasonably robust against the likelihood of vehicular cyberattacks. Additionally, there are remarkable aspects to be considered in future security protocols and solutions for CAVs. Such aspects mainly include the communication overhead, throughput, and application run-time. By considering these additional metrics, delays associated with data transmission (i.e., end-to-end inter-communication delay) can be lowered. Furthermore, since connectivity is a primary component of CAVs, it

is also crucial to ensure the most efficient security architectures are being implemented in a way that communication is secure without adding latency and increasing communication overhead. The security design of CAVs requires that both the individual components and communication technologies used are rigorously protected and that access from outside of the vehicle, if applicable, is strictly controlled. Without proper security architectures, even the strongest communication technologies will be vulnerable to data breaches.

7.4. E/E Architecture Security

The current E/E architectures with a large number of ECUs and a single central vehicle gateway are expanding and yet becoming complex. Dedicated domain controllers have been leveraged for these architectures to consolidate ECUs in the area of ADAS and Cockpit Electronics. Yet, future works must consider the automotive Ethernet in this vehicular architecture in terms of wiring harness, complexity, and security.

7.5. Authentication

Authentication is another considerable concern to be addressed in the future within wireless communication in CAVs as adversaries can compromise users' data (through false identities). Moreover, communication solutions for CAVs must address the computing power aspect, which is substantial for improving the power consumption and the individual devices involved in the communication of vehicles [235].

7.6. Communication Jamming and Spoofing

According to the existing attack surface against CAVs, the majority of CAV components are vulnerable to jamming and spoofing. It is important to distinguish between the types of jamming and spoofing attacks the components of CAVs are vulnerable to. Many existing protocols do not consider that in some scenarios, jamming or spoofing attacks do not work the same way when attacking a specific CAV's component. Further, when determining the severity of attacks, many existing security frameworks and vehicular protocols only base these attacks on certain parameters. Hence, further efforts are still needed to secure vehicular communications against jamming and spoofing attacks.

7.7. Data Sharing and Prioritization

Multimedia infotainment in traditional vehicle networks mainly relies on service providers, whereas in CAVs, it relies on individual autonomous vehicles sharing their information. Therefore, future works in CAV need to consider the popularity of CAVs, specifying the minimum number of vehicles required to participate in information sharing in order to ensure more real-time data and enable further precise decision-making. The key insight upon this open challenge is that the data sharing rate will remain low if CAVs are not widespread (i.e., a limited number of CAVs). This challenge impacts not only real-time-based decision-making in the autonomous driving task but also its overall communications.

Currently, the communication channel bandwidth remains relatively low, and the distribution of CAVs is decreasing drastically, potentially leading to a large increase in the number of propagated data packets. This challenge will become even more significant as the distance among CAVs continues to shrink. Hence, the priority of transmitted/propagated data packets must be accurately considered by future works in CAVs to guarantee that vehicles are

enabled to have timely access to information that is important to them. Specifically, future priority-based communication solutions may support varying message priorities to include, for instance, periodically broadcast data (e.g., location data), warning data (e.g., dangerous road conditions), and emergency data (e.g., emergency responders vehicle approaching).

7.8. Trusted Communications and Deception-Proofing

It remains unclear when and which communication messages must be trusted in CAVs. CAVs may receive messages related to false incidents and can thus react in a manner endangering other vehicles. Therefore, CAVs must consider their context or situation when replying to other data messages. Although some recent works in the literature attempted to identify and handle false/fake deceptive messages (i.e., verification and validation of V2V communication messages), the context of cooperation has not been considered. Future works in CAV deception-proofing must consider designing cooperative mechanisms that are secure and resilient to invalid messages and misinterpretation of messages received from other vehicles.

7.9. Security Evaluation Tools

Furthermore, additional attention must be given to designing performance evaluation tools for evaluating the CAVs' ability to secure communications. The lack of literature addressing this aspect indicates that another challenge is evaluating how well these security architectures perform apart from designing effective security architectures. Potentially, this could be another area of research regarding the implementation of security for CAVs. Without effective tools to evaluate proposed frameworks, there is no way of knowing where improvements to the proposed frameworks could be made.

8. Future Roadmap

As we navigate the evolving landscape of CAVs, we must chart a future roadmap that addresses emerging challenges and harnesses new opportunities in communication security. This section outlines key areas that constitute promising avenues for future research and development:

- **Enhanced Security Protocols**: Future studies should focus on developing more resilient security protocols that adapt to evolving cyber threats. This includes exploring advanced cryptographic methods and AI-based anomaly detection systems to safeguard CAV communications.

- **Integration of Blockchain Technology**: Investigating the integration of blockchain technology for secure and transparent CAV operations. Blockchain can offer decentralized security solutions, ensuring data integrity and trust in vehicle-to-vehicle and vehicle-to-infrastructure communications.

- **Quantum Computing and Post-Quantum Cryptography**: With the advent of quantum computing, current cryptographic standards may become vulnerable [236]. Future research should explore post-quantum cryptography to prepare CAV systems for quantum-era threats.

- **Autonomous Vehicle Ethics and Legislation**: As technology advances, the ethical implications and legal frameworks governing autonomous vehicles need further exploration. Future research should address the development of comprehensive guidelines and standards that ensure the responsible and ethical use of CAVs.

- **5G and Beyond Networking Technologies**: Investigating how emerging networking technologies, particularly 5G and beyond, can enhance CAV communication systems. This includes research on minimizing latency, improving bandwidth, and ensuring consistent connectivity for seamless CAV operation.

- **Human-Machine Interface (HMI) and User Experience:** Studying the evolving role of HMI in CAVs and its impact on user experience and safety [237]. This includes user-centric designs, intuitive interfaces, and seamless integration of autonomous functionalities.

- **Cross-Disciplinary Collaboration**: Encouraging collaborative research between computer science, automotive engineering, and cyber-physical systems to foster innovative solutions in CAV security.

- **Simulation and Real-World Testing**: Developing advanced simulation models and conducting extensive real-world testing to validate the effectiveness and reliability of proposed CAV security solutions in various scenarios.

- **Adapting to Environmental Challenges**: Researching the impact of different environmental conditions on CAV communication systems and developing adaptive technologies to maintain consistent performance under varied conditions.

By addressing these areas, we can propel the CAV industry toward a future that not only embraces technological advancements but also prioritizes security, safety, and ethical considerations.

9. Conclusions

This article has presented and discussed the latest developments in security protocols, architectures, and frameworks, highlighting best practices for designing robust security measures for CAVs. As the shift towards CAV adoption accelerates, this paper contributes significantly by categorizing various security frameworks, aiding in the development of secure and intelligent transportation systems. We have paid particular attention to vehicular communication security, outlining the challenges and opportunities presented by state-of-the-art solutions in the context of autonomous driving technologies. Specifically, this research has examined both intra- and inter-vehicular communication security challenges, proposing techniques to secure these critical aspects. Our findings enabled us to propose comprehensive security frameworks and outline relevant use cases, offering a foundation upon which future research can expand. Although considerable progress has been made in enhancing CAV security, the journey is far from complete. Ensuring the security of CAVs is a dynamic process that requires continuous technical assurances, especially as CAV technologies evolve and new

cyber threats emerge. This necessitates that security frameworks be designed with adaptability and scalability in mind, capable of responding to evolving cyber threats. To advance this field, future research should focus on developing adaptive security algorithms that can dynamically adjust to new threats as they are identified. Furthermore, the integration of artificial intelligence and machine learning techniques has the potential to enhance the ability to predict and mitigate potential attacks before they cause harm. Collaborative efforts between academia, industry, and regulatory bodies are also essential to develop standardized security protocols that address both current and future cybersecurity challenges in CAV systems. This paper emphasizes the importance of proactive approaches in securing CAVs, setting the stage for ongoing research and innovation in this critical area of transportation technology. The safety and reliability of future transportation depend not only on advancements in vehicle automation but also on the continuous improvement of cybersecurity measures.

References

[1] D. J. Fagnant, K. Kockelman, Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations, Transportation Research Part A: Policy and Practice 77 (2015) 167–181.

[2] T. Litman, Autonomous vehicle implementation predictions, Victoria Transport Policy Institute Victoria, Canada, 2017.

[3] S. Narbayeva, T. Bakibayev, K. Abeshev, I. Makarova, K. Shubenkova, A. Pashkevich, Blockchain technology on the way of autonomous vehicles development, Transportation Research Procedia 44 (2020) 168–175.

[4] N. Kalra, S. M. Paddock, Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability?, Transportation Research Part A: Policy and Practice 94 (2016) 182–193.

[5] C. Hodge, K. Hauck, S. Gupta, J. C. Bennett, Vehicle Cybersecurity Threats and Mitigation Approaches, Technical Report, National Renewable Energy Lab.(NREL), Golden, CO (United States), 2019.

[6] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, A. Lioy, On the performance of secure vehicular communication systems, IEEE transactions on dependable and secure computing 8 (2010) 898–912.

[7] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, R. Das, Attacks on self-driving cars and their countermeasures: A survey, IEEE Access 8 (2020) 207308–207342.

[8] A. O. Al Zaabi, C. Y. Yeun, E. Damiani, Autonomous vehicle security: Conceptual model, in: 2019 IEEE Transportation Electrification Conference and Expo, Asia-Pacific (ITEC Asia-Pacific), IEEE, 2019, pp. 1–5.

[9] H. Abraham, C. Lee, S. Brady, C. Fitzgerald, B. Mehler, B. Reimer, J. F. Coughlin, Autonomous vehicles, trust, and driving alternatives: A survey of consumer preferences, Massachusetts Inst. Technol, AgeLab, Cambridge 1 (2016) 16.

[10] IEEE, How can autonomous vehicles be protected against cyber security threats?, https://innovationatwork.ieee.org/how-can-autonomous-vehicles-be-protected-against-cyber-security-threats/, 2021. Accessed: 2021-04-18.

[11] M. Zorz, Are we doing enough to protect connected cars?, https://www.helpnetsecurity.com/2020/04/15/protect-connected-cars/, 2020. Accessed: 2021-04-18.

[12] S. Tsugawa, Inter-vehicle communications and their applications to intelligent vehicles: an overview, in: Intelligent Vehicle Symposium, 2002. IEEE, volume 2, IEEE, 2002, pp. 564–569.

[13] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, P. Ranganathan, Cybersecurity challenges in vehicular communications, Vehicular Communications 23 (2020) 100214.

[14] Upstream Security: 2020 Global Automotive Cyber security Report, Network Security 2020 (2020) 4–4. doi:10.1016/S1353-4858(20)30005-2.

[15] W. Viriyasitavat, M. Boban, H.-M. Tsai, A. Vasilakos, Vehicular communications: Survey and challenges of channel and propagation models, IEEE Vehicular Technology Magazine 10 (2015) 55–66.

[16] D. Singh, M. Singh, I. Singh, H.-J. Lee, Secure and reliable cloud networks for smart transportation services, in: 2015 17th International Conference on Advanced Communication Technology (ICACT), IEEE, 2015, pp. 358–362.

[17] B. Ying, D. Makrakis, Z. Hou, Motivation for protecting selfish vehicles' location privacy in vehicular networks, IEEE Transactions on Vehicular Technology 64 (2015) 5631–5641.

[18] S. Abbott-McCune, L. A. Shay, Techniques in hacking and simulating a modem automotive controller area network, in: 2016 IEEE International Carnahan Conference on Security Technology (ICCST), IEEE, 2016, pp. 1–7.

[19] R. Hussain, S. Zeadally, Autonomous cars: Research results, issues, and future challenges, IEEE Communications Surveys & Tutorials 21 (2018) 1275–1313.

[20] P. Koopman, M. Wagner, Challenges in autonomous vehicle testing and validation, SAE International Journal of Transportation Safety 4 (2016) 15–24.

[21] A. Maimaris, G. Papageorgiou, A review of intelligent transportation systems from a communications technology perspective, in: 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), IEEE, 2016, pp. 54–59.

[22] J. Wang, J. Liu, N. Kato, Networking and communications in autonomous driving: A survey, IEEE Communications Surveys & Tutorials 21 (2018) 1243–1274.

[23] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, J.-P. Hubaux, Secure vehicular communication systems: design and architecture, IEEE Communications magazine 46 (2008) 100–109.

[24] C. Miller, C. Valasek, A survey of remote automotive attack surfaces, black hat USA 2014 (2014) 94.

[25] L. Gupta, R. Jain, G. Vaszkun, Survey of important issues in UAV communication networks, IEEE Communications Surveys & Tutorials 18 (2015) 1123–1152.

[26] V. L. Thing, J. Wu, Autonomous vehicle security: A taxonomy of attacks and defences, in: 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2016, pp. 164–170.

[27] S. Gifei, A. Salceanu, Integrated management system for quality, safety and security in developing autonomous vehicles, in: 2017 10th International Symposium on Advanced Topics in Electrical Engineering (ATEE), IEEE, 2017, pp. 673–676.

[28] A.-M. Căilean, M. Dimian, Current challenges for visible light communications usage in vehicle applications: A survey, IEEE Communications Surveys & Tutorials 19 (2017) 2681–2703.

[29] S. Karnouskos, F. Kerschbaum, Privacy and integrity considerations in hyperconnected autonomous vehicles, Proceedings of the IEEE 106 (2017) 160–170.

[30] S. Parkinson, P. Ward, K. Wilson, J. Miller, Cyber threats facing autonomous and connected vehicles: Future challenges, IEEE transactions on intelligent transportation systems 18 (2017) 2898–2915.

[31] J. Claybrook, S. Kildare, Autonomous vehicles: No driver... no regulation?, Science 361 (2018) 36–37.

[32] J. De Bruyne, J. Werbrouck, Merging self-driving cars with the law, Computer law & security review 34 (2018) 1150–1153.

[33] A. Tomlinson, J. Bryans, S. A. Shaikh, Towards viable intrusion detection methods for the automotive controller area network, in: 2nd ACM Computer Science in Cars Symposium, 2018.

[34] R. W. van der Heijden, S. Dietzel, T. Leinmüller, F. Kargl, Survey on misbehavior detection in cooperative intelligent transportation systems, IEEE Communications Surveys & Tutorials 21 (2018) 779–811.

[35] K. Ren, Q. Wang, C. Wang, Z. Qin, X. Lin, The security of autonomous driving: Threats, defenses, and future directions, Proceedings of the IEEE 108 (2019) 357–372.

[36] H. Goumidi, Z. Aliouat, S. Harous, Vehicular cloud computing security: A survey, Arabian Journal for Science and Engineering (2019) 1–27.

[37] O. Y. Al-Jarrah, C. Maple, M. Dianati, D. Oxtoby, A. Mouzakitis, Intrusion detection systems for intra-vehicle networks: A review, IEEE Access 7 (2019) 21266–21289.

[38] C. Sharma, S. Moylan, G. Amariucai, E. Y. Vasserman, An extended survey on vehicle security, arXiv preprint arXiv:1910.04150 (2019).

[39] J. Wang, Y. Shao, Y. Ge, R. Yu, A survey of vehicle to everything (v2x) testing, Sensors 19 (2019) 334.

[40] F. Sommer, J. Dürrwang, R. Kriesten, Survey and classification of automotive security attacks, Information 10 (2019) 148.

[41] G. Baldini, R. Neisse, On the application of policy-based frameworks to autonomous vehicles, in: 2020 Global Internet of Things Summit (GIoTS), IEEE, 2020, pp. 1–6.

[42] A. Qayyum, M. Usama, J. Qadir, A. Al-Fuqaha, Securing connected & autonomous vehicles: Challenges posed by adversarial machine learning and the way forward, IEEE Communications Surveys & Tutorials 22 (2020) 998–1026.

[43] S. Halder, A. Ghosal, M. Conti, Secure over-the-air software updates in connected vehicles: A survey, Computer Networks (2020) 107343.

[44] F. Luo, S. Hou, X. Zhang, Z. Yang, W. Pan, Security risk analysis approach for safety-critical systems of connected vehicles, Electronics 9 (2020) 1242.

[45] V. Promyslov, K. Semenkov, Security threats for autonomous and remotely controlled vehicles in smart city, in: 2020 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), IEEE, 2020, pp. 1–5.

[46] M. Pham, K. Xiong, A survey on security attacks and defense techniques for connected and autonomous vehicles, arXiv preprint arXiv:2007.08041 (2020).

[47] A. Green, The self drive act: An opportunity to re-legislate a minimum cybersecurity federal framework for autonomous vehicles, Santa Clara Law Review 60 (2020) 217.

[48] D. Virag, T. Offerman, B. de Jong, M. Preuss, It security challenges for continuously connected near-autonomous vehicles, in: 2020 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), IEEE, 2020, pp. 1–8.

[49] Z. Wang, H. Wei, J. Wang, X. Zeng, Y. Chang, Security issues and solutions for connected and autonomous vehicles in a sustainable city: A survey, Sustainability 14 (2022) 12409.

[50] S. J. Taylor, F. Ahmad, H. N. Nguyen, S. A. Shaikh, Vehicular platoon communication: architecture, security threats and open challenges, Sensors 23 (2023) 134.

[51] M. Hataba, A. Sherif, M. Mahmoud, M. Abdallah, W. Alasmary, Security and privacy issues in autonomous vehicles: A layer-based survey, IEEE Open Journal of the Communications Society 3 (2022) 811–829.

[52] M. Ahmed, M. A. Mirza, S. Raza, H. Ahmad, F. Xu, W. U. Khan, Q. Lin, Z. Han, Vehicular communication network enabled cav data offloading: A review, IEEE Transactions on Intelligent Transportation Systems (2023).

[53] B. Deng, J. Nan, W. Cao, W. Wang, A survey on integration of network communication into vehicle real-time motion control, IEEE Communications Surveys & Tutorials 25 (2023) 2755–2790. doi:10.1109/COMST.2023.3295384.

[54] W. Liu, M. Hua, Z. Deng, Z. Meng, Y. Huang, C. Hu, S. Song, L. Gao, C. Liu, B. Shuai, et al., A systematic survey of control techniques and applications in connected and automated vehicles, IEEE Internet of Things Journal (2023).

[55] S. Hakak, T. R. Gadekallu, P. K. R. Maddikunta, S. P. Ramu, M. Parimala, C. De Alwis, M. Liyanage, Autonomous vehicles in 5g and beyond: A survey, Vehicular Communications 39 (2023) 100551.

[56] V. P. Chellapandi, L. Yuan, C. G. Brinton, S. H. Żak, Z. Wang, Federated learning for connected and automated vehicles: A survey of existing approaches and challenges, IEEE Transactions on Intelligent Vehicles (2023).

[57] Y. Fang, H. Min, X. Wu, W. Wang, X. Zhao, B. Martinez-Pastor, R. Teixeira, Anomaly diagnosis of connected autonomous vehicles: A survey, Information Fusion 105 (2024) 102223.

[58] M. Pipicelli, A. Gimelli, B. Sessa, F. De Nola, G. Toscano, G. Di Blasio, Architecture and potential of connected and autonomous vehicles, Vehicles 6 (2024) 275–304.

[59] K. Qu, W. Zhuang, Q. Ye, W. Wu, X. Shen, Model-assisted learning for adaptive cooperative perception of connected autonomous vehicles, IEEE Transactions on Wireless Communications (2024).

[60] H. Ibn-Khedher, M. Laroui, M. Alfaqawi, A. Magnouche, H. Moungla, H. Afifi, 6g-edge support of internet of autonomous vehicles: A survey, Transactions on Emerging Telecommunications Technologies 35 (2024) e4918.

[61] M. Sorkhpour, A. Yazdinejad, A. Dehghantanha, Auto-cids: An autonomous intrusion detection system for vehicular networks, in: Proceedings of the Workshop on Autonomous Cybersecurity (AutonomousCyber '24), 2024, p. 11. URL: https://doi.org/10.1145/3689933.3690837. doi:10.1145/3689933.3690837.

[62] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, J.-P. Hubaux, Secure vehicular communication systems: design and architecture, IEEE Communications Magazine 46 (2008) 100–109. doi:10.1109/MCOM.2008.4689252.

[63] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, A. Lioy, On the performance of secure vehicular communication systems, IEEE Transactions on Dependable and Secure Computing 8 (2011) 898–912. doi:10.1109/TDSC.2010.58.

[64] N. Ristanovic, P. Papadimitratos, G. Theodorakopoulos, J.-P. Hubaux, J.-Y. Le Boudec, Adaptive message authentication for multi-hop networks, in: 2011 Eighth International Conference on Wireless On-Demand Network Systems and Services, 2011, pp. 96–103. doi:10.1109/WONS.2011.5720206.

[65] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, D. C. Parkes, Non-cooperative location privacy, IEEE Transactions on Dependable and Secure Computing 10 (2013) 84–98. doi:10.1109/TDSC.2012.85.

[66] V. Mothukuri, R. M. Parizi, J. L. Massa, A. Yazdinejad, An ai multi-model approach to defi project trust scoring and security, in: 2024 IEEE International Conference on Blockchain (Blockchain), IEEE, 2024, pp. 19–28.

[67] B. Eriksson, J. Groth, A. Sabelfeld, On the road with third-party apps: Security analysis of an in-vehicle app platform., in: VEHITS, 2019, pp. 64–75.

[68] A. K. Mandal, A. Cortesi, P. Ferrara, F. Panarotto, F. Spoto, Vulnerability analysis of android auto infotainment apps, in: Proceedings of the 15th ACM International Conference on Computing Frontiers, 2018, pp. 183–190.

[69] A. K. Mandal, F. Panarotto, A. Cortesi, P. Ferrara, F. Spoto, Static analysis of android auto infotainment and on-board diagnostics ii apps, Software: Practice and Experience 49 (2019) 1131–1161.

[70] Y. Lee, S. Woo, J. Lee, Y. Song, H. Moon, D. H. Lee, Enhanced android app-repackaging attack on in-vehicle network, Wireless Communications and Mobile Computing 2019 (2019).

[71] A. K. Mandal, F. Spoto, Static analysis of android apps interaction with automotive can, in: Smart Computing and Communication: Third International Conference, SmartCom 2018, Tokyo, Japan, December 10–12, 2018, Proceedings, volume 11344, Springer, 2018, p. 114.

[72] E. Chatzoglou, G. Kambourakis, V. Kouliaridis, A multi-tier security analysis of official car management apps for android, Future Internet 13 (2021) 58.

[73] M. Singh, Information Security of Intelligent Vehicles Communication: Overview, Perspectives, Challenges, and Possible Solutions, Springer Verlag, Singapor, 2021.

[74] D. Namakshenas, A. Yazdinejad, A. Dehghantanha, R. M. Parizi, G. Srivastava, Ip2fl: Interpretation-based privacy-preserving federated learning for industrial cyber-physical systems, IEEE Transactions on Industrial Cyber-Physical Systems (2024).

[75] A. Yazdinejad, A. Dehghantanha, H. Karimipour, G. Srivastava, R. M. Parizi, A robust privacy-preserving federated learning model against model poisoning attacks, IEEE Transactions on Information Forensics and Security (2024).

[76] M. Oehl, K. Ihme, A.-A. Pape, M. Vukelić, M. Braun, Affective use cases for empathic vehicles in highly automated driving: results of an expert workshop, in: International Conference on Human-Computer Interaction, Springer, 2020, pp. 89–100.

[77] A. Dehghantanha, A. Yazdinejad, R. M. Parizi, Autonomous cybersecurity: Evolving challenges, emerging opportunities, and future research trajectories, in: Proceedings of the Workshop on Autonomous Cybersecurity (AutonomousCyber '24), 2024, p. 10. URL: https://doi.org/10.1145/3689933.3690832. doi:10.1145/3689933.3690832.

[78] A. Chehri, H. T. Mouftah, Autonomous vehicles in the sustainable cities, the beginning of a green adventure, Sustainable Cities and Society 51 (2019) 101751.

[79] M. S. Salek, S. M. Khan, M. Rahman, H.-W. Deng, M. Islam, Z. Khan, M. Chowdhury, M. Shue, A review on cybersecurity of cloud computing for supporting connected vehicle applications, IEEE Internet of Things Journal 9 (2022) 8250–8268.

[80] X. Sun, F. R. Yu, P. Zhang, A survey on cyber-security of connected and autonomous vehicles (cavs), IEEE Transactions on Intelligent Transportation Systems (2021) 1–20. doi:10.1109/TITS.2021.3085297.

[81] S. R. Pokhrel, Y. Qu, S. Nepal, S. Singh, Privacy-aware autonomous valet parking: Towards experience driven approach, IEEE Transactions on Intelligent Transportation Systems (2020).

[82] D. V. Iroshnikov, L. Y. Larina, A. I. Sidorkin, Autonomous vehicles within the urban space and transport security challenges: Legal aspect, J. Pol. & L. 13 (2020) 133.

[83] J. Scholliers, P. Pyykönen, A. Virtanen, E. Aittoniemi, F. Malin, M. Federley, S. Nikolaou, Automated valet parking using IoT: Design, user experience and business opportunities, in: 8th Transport Research Arena, TRA 2020-Conference cancelled, 2020, p. 6.

[84] M. Khalid, Y. Cao, K. Wang, P. Dhawankar, M. Raza, Toward autonomous valet parking: A broader perspective, Toward Sustainable And Economic Smart Mobility: Shaping The Future Of Smart Cities (2020) 99.

[85] Y. Fu, C. Li, F. R. Yu, T. H. Luan, Y. Zhang, An autonomous lane changing system with knowledge accumulation and transfer assisted by vehicular blockchain, IEEE Internet of Things Journal (2020).

[86] T. Liu, X. Mu, B. Huang, Y. Xie, D. Cao, Driving tasks transfer in deep reinforcement learning for decision-making of autonomous vehicles, arXiv preprint arXiv:2009.03268 (2020).

[87] A. Ferdowsi, U. Challita, W. Saad, N. B. Mandayam, Robust deep reinforcement learning for security and safety in autonomous vehicle systems, in: 2018 21st International Conference on Intelligent Transportation Systems (ITSC), IEEE, 2018, pp. 307–312.

[88] W. Xia, H. Li, B. Li, A control strategy of autonomous vehicles based on deep reinforcement learning, in: 2016 9th International Symposium on Computational Intelligence and Design (ISCID), volume 2, IEEE, 2016, pp. 198–201.

[89] A. E. Sallab, M. Abdou, E. Perot, S. Yogamani, Deep reinforcement learning framework for autonomous driving, Electronic Imaging 2017 (2017) 70–76.

[90] Y. Ma, Q. Liu, J. Fu, K. Liufu, Q. Li, Collision-avoidance lane change control method for enhancing safety for connected vehicle platoon in mixed traffic environment, Accident Analysis & Prevention 184 (2023) 106999.

[91] P. Ghorai, A. Eskandarian, Y.-K. Kim, G. Mehr, State estimation and motion prediction of vehicles and vulnerable road users for cooperative autonomous driving: A survey, IEEE transactions on intelligent transportation systems 23 (2022) 16983–17002.

[92] D. Tsiktsiris, A. Vafeiadis, A. Lalas, M. Dasygenis, K. Votis, D. Tzovaras, A novel image and audio-based artificial intelligence service for security applications in autonomous vehicles, Transportation Research Procedia 62 (2022) 294–301.

[93] B. R. Mudhivarthi, P. Thakur, G. Singh, Aspects of cyber security in autonomous and connected vehicles, Applied Sciences 13 (2023) 3014.

[94] J. Kwon, B. A. Mugabarigira, J. P. Jeong, Web-based car control and monitoring for safe driving of autonomous vehicles, in: 2022 International Conference on Information Networking (ICOIN), 2022, pp. 435–440. doi:10.1109/ICOIN53446.2022.9687175.

[95] H. Guo, E. Meamari, C.-C. Shen, Blockchain-inspired event recording system for autonomous vehicles, in: 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), 2018, pp. 218–222. doi:10.1109/HOTICN.2018.8606016.

[96] A. Yazdinejad, Secure and Private ML-based Cybersecurity Framework for Industrial Internet of Things (IIoT), Ph.D. thesis, University of Guelph, 2024.

[97] M. Benyahya, A. Collen, S. Kechagia, N. A. Nijdam, Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments, Computers & Security 122 (2022) 102904.

[98] B. Sheehan, F. Murphy, M. Mullins, C. Ryan, Connected and autonomous vehicles: A cyber-risk classification framework, Transportation research part A: policy and practice 124 (2019) 523–536.

[99] 14:00-17:00, ISO 20078-3:2021, ???? URL: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/08/01/80185.html.

[100] M. R. Ansari, J.-P. Monteuuis, J. Petit, C. Chen, V2X misbehavior and collective perception service: Considerations for standardization, arXiv preprint arXiv:2112.02184 (2021).

[101] Y. Yuan, R. Tasik, S. S. Adhatarao, Y. Yuan, Z. Liu, X. Fu, Race: reinforced cooperative autonomous vehicle collision avoidance, IEEE Transactions on Vehicular Technology (2020).

[102] M. Singh, S. Kim, Blockchain based intelligent vehicle data sharing framework, arXiv preprint arXiv:1708.09721 (2017).

[103] A. Dorri, M. Steger, S. S. Kanhere, R. Jurdak, Blockchain: A distributed solution to automotive security and privacy, IEEE Communications Magazine 55 (2017) 119–125.

[104] G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan, R. Kumar, A blockchain framework for securing connected and autonomous vehicles, Sensors 19 (2019) 3165.

[105] A. Yazdinejad, A. Dehghantanha, H. Karimipour, G. Srivastava, R. M. Parizi, An efficient packet parser architecture for software-defined 5g networks, Physical Communication 53 (2022) 101677.

[106] M. S. Eddine, M. A. Ferrag, O. Friha, L. Maglaras, Easbf: An efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles, Journal of Information Security and Applications 59 (2021) 102802.

[107] C. Oham, R. A. Michelin, R. Jurdak, S. S. Kanhere, S. Jha, B-ferl: Blockchain based framework for securing smart vehicles, Information Processing & Management 58 (2021) 102426.

[108] J. Xiong, R. Bi, M. Zhao, J. Guo, Q. Yang, Edge-assisted privacy-preserving raw data sharing framework for connected autonomous vehicles, IEEE Wireless Communications 27 (2020) 24–30.

[109] L. Wei, C. Zhang, Trinc-based secure and privacy-preserving protocols for vehicular ad hoc networks, in: 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring), IEEE, 2016, pp. 1–5.

[110] R. Hussain, D. Kim, A. O. Tokuta, H. M. Melikyan, H. Oh, Covert communication based privacy preservation in mobile vehicular networks, in: MILCOM 2015-2015 IEEE Military Communications Conference, IEEE, 2015, pp. 55–60.

[111] Q. Zhang, H. Zhong, J. Cui, L. Ren, W. Shi, AC4AV: A flexible and dynamic access control framework for connected and autonomous vehicles, IEEE Internet of Things Journal (2020).

[112] Z. Xu, C. Yang, Z. Tan, Z. Sheng, Raptor code-enabled reliable data transmission for in-vehicle power line communication systems with impulsive noise, IEEE Communications Letters 21 (2017) 2154–2157.

[113] Q. He, X. Meng, R. Qu, R. Xi, Machine learning-based detection for cyber security attacks on connected and autonomous vehicles, Mathematics 8 (2020) 1311.

[114] T. Zeng, O. Semiari, M. Chen, W. Saad, M. Bennis, Federated learning on the road: Autonomous controller design for connected and autonomous vehicles, arXiv preprint arXiv:2102.03401 (2021).

[115] A. Yazdinejad, A. Bohlooli, K. Jamshidi, Efficient design and hardware implementation of the openflow v1. 3 switch on the virtex-6 fpga ml605, The Journal of Supercomputing 74 (2018) 1299–1320.

[116] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, K.-K. R. Choo, An energy-efficient sdn controller architecture for iot networks with blockchain-based security, IEEE Transactions on Services Computing 13 (2020) 625–638.

[117] T. Hackel, P. Meyer, F. Korf, T. C. Schmidt, Software-defined networks supporting time-sensitive in-vehicular communication, in: 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), IEEE, 2019, pp. 1–5.

[118] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, Blockchain-enabled authentication handover with efficient privacy protection in sdn-based 5g networks, IEEE Transactions on Network Science and Engineering 8 (2019) 1120–1132.

[119] S. A. Abdel Hakeem, A. A. Hady, H. Kim, Current and future developments to improve 5g-newradio performance in vehicle-to-everything communications, Telecommunication systems 75 (2020) 331–353.

[120] A. Yazdinejad, B. Zolfaghari, A. Dehghantanha, H. Karimipour, G. Srivastava, R. M. Parizi, Accurate threat hunting in industrial internet of things edge devices, Digital Communications and Networks 9 (2023) 1123–1130.

[121] A. Al-Sabaawi, K. Al-Dulaimi, E. Foo, M. Alazab, Addressing malware attacks on connected and autonomous vehicles: recent techniques and challenges, in: Malware Analysis Using Artificial Intelligence and Deep Learning, Springer, 2021, pp. 97–119.

[122] A. Taeihagh, H. S. M. Lim, Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks, Transport Reviews 39 (2019) 103–128.

[123] D. Cao, L. Li, C. Marina, L. Chen, Y. Xing, W. Zhuang, Special issue on internet of things for connected automated driving, IEEE Internet of Things Journal 7 (2020) 3678–3680.

[124] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, Federated learning for drone authentication, Ad Hoc Networks 120 (2021) 102574.

[125] K. M. Deliparaschos, G. Santha, L. Z. Fragonara, I. Petrunin, A. C. Zolotas, A. Tsourdos, A preliminary investigation of an autonomous vehicle validation infrastructure for smart cities, in: 2020 International Conference Mechatronic Systems and Materials (MSM), IEEE, 2020, pp. 1–5.

[126] Y. Shao, M. A. M. Zulkefli, Z. Sun, P. Huang, Evaluating connected and autonomous vehicles using a hardware-in-the-loop testbed and a living lab, Transportation Research Part C: Emerging Technologies 102 (2019) 121–135.

[127] K. M. Gurumurthy, F. de Souza, A. Enam, J. Auld, Integrating supply and demand perspectives for a large-scale simulation of shared autonomous vehicles, Transportation Research Record (2020) 0361198120921157.

[128] J. D. Castro, S. Singh, A. Arora, S. Louie, D. Senic, Enabling safe autonomous vehicles by advanced mm-wave radar simulations, in: 2019 IEEE MTT-S International Microwave Symposium (IMS), IEEE, 2019, pp. 1476–1479.

[129] Q. Chao, X. Jin, H.-W. Huang, S. Foong, L.-F. Yu, S.-K. Yeung, Force-based heterogeneous traffic simulation for autonomous vehicle testing, in: 2019 International Conference on Robotics and Automation (ICRA), IEEE, 2019, pp. 8298–8304.

[130] J. S. Kiran, P. R. Jakkala, Cyber security and risk analysis on connected autonomous vehicles, Solid State Technology 63 (2020).

[131] A. Qureshi, M. Marvi, J. A. Shamsi, A. Aijaz, Euf: A framework for detecting over-the-air malicious updates in autonomous vehicles, Journal of King Saud University-Computer and Information Sciences (2021).

[132] D. Jadav, M. S. Obaidiat, S. Tanwar, R. Gupta, K.-F. Hsiao, Amalgamation of blockchain and ai to classify malicious behavior of autonomous vehicles, in: 2021 International Conference on Computer, Information and Telecommunication Systems (CITS), 2021, pp. 1–5. doi:10.1109/CITS52676.2021.9618005.

[133] A. Yazdinejadna, R. M. Parizi, A. Dehghantanha, M. S. Khan, A kangaroo-based intrusion detection system on software-defined networks, Computer Networks 184 (2021) 107688.

[134] S. Zang, M. Ding, D. Smith, P. Tyler, T. Rakotoarivelo, M. A. Kaafar, The impact of adverse weather conditions on autonomous vehicles: how rain, snow, fog, and hail affect the performance of a self-driving car, IEEE vehicular technology magazine 14 (2019) 103–111.

[135] A. Yadav, G. Bose, R. Bhange, K. Kapoor, N. C. S. N. Iyenger, R. Caytiles, Security, vulnerability and protection of vehicular on-board diagnostics, International Journal of Security and Its Applications 10 (2016) 405–422. doi:10.14257/ijsia.2016.10.4.36.

[136] B. S. Lim, S. L. Keoh, V. L. Thing, Autonomous vehicle ultrasonic sensor vulnerability and impact assessment, in: 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), IEEE, 2018, pp. 231–236.

[137] H. Taslimasa, S. Dadkhah, E. C. P. Neto, P. Xiong, S. Ray, A. A. Ghorbani, Security issues in internet of vehicles (iov): A comprehensive survey, Internet of Things (2023) 100809.

[138] S. Malik, W. Sun, Analysis and simulation of cyber attacks against connected and autonomous vehicles, in: 2020 International Conference on Connected and Autonomous Driving (MetroCAD), IEEE, 2020, pp. 62–70.

[139] Z. Hou, H. Liu, Y. Zhang, Zero-day vulnerability inspired hazard assessment for autonomous driving vehicles, in: 2019 IEEE 19th International Conference on Communication Technology (ICCT), IEEE, 2019, pp. 1348–1354.

[140] M. Porter, S. Dey, A. Joshi, P. Hespanhol, A. Aswani, M. Johnson-Roberson, R. Vasudevan, Detecting deception attacks on autonomous vehicles via linear time-varying dynamic watermarking, arXiv preprint arXiv:2001.09859 (2020).

[141] U. Ahmad, H. Song, A. Bilal, M. Alazab, A. Jolfaei, Securing smart vehicles from relay attacks using machine learning, The Journal of Supercomputing 76 (2020) 2665–2682.

[142] Z. A. Biron, S. Dey, P. Pisu, Real-time detection and estimation of denial of service attack in connected vehicle systems, IEEE Transactions on Intelligent Transportation Systems 19 (2018) 3893–3902.

[143] K. M. Ali Alheeti, K. McDonald-Maier, Intelligent intrusion detection in external communication systems for autonomous vehicles, Systems Science & Control Engineering 6 (2018) 48–56.

[144] X. Feng, C.-y. Li, D.-x. Chen, J. Tang, A method for defending against multi-source sybil attacks in VANET, Peer-to-Peer Networking and Applications 10 (2017) 305–314.

[145] K. Lim, T. Islam, H. Kim, J. Joung, A sybil attack detection scheme based on adas sensors for vehicular networks, in: 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), IEEE, 2020, pp. 1–5.

[146] D. Suo, J. Moore, M. Boesch, K. Post, S. E. Sarma, Location-based schemes for mitigating cyber threats on connected and automated vehicles: a survey and design framework, IEEE transactions on intelligent transportation systems 23 (2020) 2919–2937.

[147] M. L. Bouchouia, H. Labiod, O. Jelassi, J.-P. Monteuuis, W. B. Jaballah, J. Petit, Z. Zhang, A survey on misbehavior detection for connected and autonomous vehicles, Vehicular Communications (2023) 100586.

[148] J. Tobin, C. Thorpe, L. Murphy, An approach to mitigate black hole attacks on vehicular wireless networks, in: 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), IEEE, 2017, pp. 1–7.

[149] A. Nanda, D. Puthal, J. J. Rodrigues, S. A. Kozlov, Internet of autonomous vehicles communications security: overview, issues, and directions, IEEE Wireless Communications 26 (2019) 60–65.

[150] Q. He, X. Meng, R. Qu, Towards a severity assessment method for potential cyber attacks to connected and autonomous vehicles, Journal of Advanced Transportation 2020 (2020).

[151] A. Chattopadhyay, K.-Y. Lam, Security of autonomous vehicle as a cyber-physical system, in: 2017 7th International Symposium on Embedded Computing and System Design (ISED), IEEE, 2017, pp. 1–6.

[152] F. Al-Turjman, J. P. Lemayian, Intelligence, security, and vehicular sensor networks in internet of things (iot)-enabled smart-cities: An overview, Computers & Electrical Engineering 87 (2020) 106776.

[153] S. Tayeb, M. Pirouz, G. Esguerra, K. Ghobadi, J. Huang, R. Hill, D. Lawson, S. Li, T. Zhan, J. Zhan, et al., Securing the positioning signals of autonomous vehicles, in: 2017 IEEE International Conference on Big Data (Big Data), IEEE, 2017, pp. 4522–4528.

[154] T. Limbasiya, K. Z. Teng, S. Chattopadhyay, J. Zhou, A systematic survey of attack detection and prevention in connected and autonomous vehicles, Vehicular Communications (2022) 100515.

[155] Z. Yang, J. Ying, J. Shen, Y. Feng, Q. A. Chen, Z. M. Mao, H. X. Liu, Anomaly detection against gps spoofing attacks on connected and autonomous vehicles using learning from demonstration, IEEE Transactions on Intelligent Transportation Systems (2023).

[156] M. Pham, K. Xiong, A survey on security attacks and defense techniques for connected and autonomous vehicles, Computers & Security 109 (2021) 102269.

[157] A. Tomlinson, J. Bryans, S. A. Shaikh, Using a one-class compound classifier to detect in-vehicle network attacks, in: Proceedings of the Genetic and Evolutionary Computation Conference Companion, 2018, pp. 1926–1929.

[158] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, G. Epiphaniou, An optimized fuzzy deep learning model for data classification based on nsga-ii, Neurocomputing 522 (2023) 116–128.

[159] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, Y. Chen, Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions, Accident Analysis & Prevention 148 (2020) 105837.

[160] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, S. Capkun, On the requirements for successful GPS spoofing attacks, in: Proceedings of the 18th ACM conference on Computer and communications security, 2011, pp. 75–86.

[161] B. Manale, T. Mazri, Intrusion detection method for gps based on deep learning for autonomous vehicle, International Journal of Electronic Security and Digital Forensics 14 (2022) 37–52.

[162] B. Biggio, B. Nelson, P. Laskov, Poisoning attacks against support vector machines, arXiv preprint arXiv:1206.6389 (2012).

[163] B. Biggio, I. Corona, D. Maiorca, B. Nelson, N. Šrndić, P. Laskov, G. Giacinto, F. Roli, Evasion attacks against machine learning at test time, in: Joint European conference on machine learning and knowledge discovery in databases, Springer, 2013, pp. 387–402.

[164] X. Liu, H. Yang, Z. Liu, L. Song, H. Li, Y. Chen, Dpatch: An adversarial patch attack on object detectors, arXiv preprint arXiv:1806.02299 (2018).

[165] J. Lu, H. Sibai, E. Fabry, D. Forsyth, No need to worry about adversarial examples in object detection in autonomous vehicles, arXiv preprint arXiv:1707.03501 (2017).

[166] K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, C. Xiao, A. Prakash, T. Kohno, D. Song, Robust physical-world attacks on deep learning visual classification, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2018, pp. 1625–1634.

[167] K. B. Kelarestaghi, M. Foruhandeh, K. Heaslip, R. Gerdes, Intelligent transportation system security: impact-oriented risk assessment of in-vehicle networks, IEEE Intelligent Transportation Systems Magazine (2019) 1–1.

[168] Y. Cao, C. Xiao, B. Cyr, Y. Zhou, W. Park, S. Rampazzi, Q. A. Chen, K. Fu, Z. M. Mao, Adversarial sensor attack on lidar-based perception in autonomous driving, in: Proceedings of the 2019 ACM SIGSAC conference on computer and communications security, 2019, pp. 2267–2281.

[169] H. Shin, D. Kim, Y. Kwon, Y. Kim, Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications, in: International Conference on Cryptographic Hardware and Embedded Systems, Springer, 2017, pp. 445–467.

[170] C. Sitawarin, A. N. Bhagoji, A. Mosenia, M. Chiang, P. Mittal, Darts: Deceiving autonomous cars with toxic signs, arXiv preprint arXiv:1802.06430 (2018).

[171] J. Kos, I. Fischer, D. Song, Adversarial examples for generative models, in: 2018 IEEE security and privacy workshops (spw), IEEE, 2018, pp. 36–42.

[172] S.-M. Moosavi-Dezfooli, A. Fawzi, O. Fawzi, P. Frossard, Universal adversarial perturbations, in: Proceedings of the IEEE conference on computer vision and pattern recognition, 2017, pp. 1765–1773.

[173] M.-I. Nicolae, M. Sinn, M. N. Tran, B. Buesser, A. Rawat, M. Wistuba, V. Zantedeschi, N. Baracaldo, B. Chen, H. Ludwig, et al., Adversarial robustness toolbox v1. 0.0, arXiv preprint arXiv:1807.01069 (2018).

[174] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking, Computers & Security 88 (2020) 101629.

[175] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, M. Hammoudeh, H. Karimipour, G. Srivastava, Block hunter: Federated learning for cyber threat hunting in blockchain-based iiot networks, IEEE Transactions on Industrial Informatics 18 (2022) 8356–8366.

[176] M. Luo, A. C. Myers, G. E. Suh, Stealthy tracking of autonomous vehicles with cache side channels, in: 29th {USENIX} Security Symposium ({USENIX} Security 20), 2020, pp. 859–876.

[177] F. Nelles, A. Yazdinejad, A. Dehghantanha, R. M. Parizi, G. Srivastava, A federated learning approach for multi-stage threat analysis in advanced persistent threat campaigns, arXiv preprint arXiv:2406.13186 (2024).

[178] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, K.-K. R. Choo, Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles, IEEE Transactions on Vehicular Technology (2020).

[179] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, G. Srivastava, H. Karimipour, Secure intelligent fuzzy blockchain framework: Effective threat detection in iot networks, Computers in Industry 144 (2023) 103801.

[180] H. Nazari, A. Yazdinejad, A. Dehghantanha, F. Zarrinkalam, G. Srivastava, P3gnn: A privacy-preserving provenance graph-based model for apt detection in software defined networking, arXiv preprint arXiv:2406.12003 (2024).

[181] S. Garg, K. Kaur, G. Kaddoum, S. H. Ahmed, D. N. K. Jayakody, SDN-based secure and privacy-preserving scheme for vehicular networks: A 5G perspective, IEEE Transactions on Vehicular Technology 68 (2019) 8421–8434.

[182] S. Chen, J. Hu, Y. Shi, Y. Peng, J. Fang, R. Zhao, L. Zhao, Vehicle-to-everything (V2X) services supported by LTE-based systems and 5G, IEEE Communications Standards Magazine 1 (2017) 70–76.

[183] M. Hashemi, C. E. Koksal, N. B. Shroff, Out-of-band millimeter wave beamforming and communications to achieve low latency and high energy efficiency in 5G systems, IEEE Transactions on Communications 66 (2017) 875–888.

[184] R. Yu, J. Ding, X. Huang, M.-T. Zhou, S. Gjessing, Y. Zhang, Optimal resource sharing in 5G-enabled vehicular networks: A matrix game approach, IEEE Transactions on Vehicular Technology 65 (2016) 7844–7856.

[185] S. A. A. Shah, E. Ahmed, M. Imran, S. Zeadally, 5G for vehicular communications, IEEE Communications Magazine 56 (2018) 111–117.

[186] R. Molina-Masegosa, J. Gozalvez, LTE-V for sidelink 5G V2X vehicular communications: A new 5G technology for short-range vehicle-to-everything communications, IEEE Vehicular Technology Magazine 12 (2017) 30–39.

[187] S. Makar, A. Dehghantanha, F. Zarrinkalam, G. Srivastava, A. Yazdinejad, Systemization of knowledge (sok)-cross impact of transfer learning in cybersecurity: Offensive, defensive and threat intelligence perspectives, arXiv preprint arXiv:2309.05889 (2023).

[188] R. Quinonez, J. Giraldo, L. Salazar, E. Bauman, A. Cardenas, Z. Lin, {SAVIOR}: Securing autonomous vehicles with robust physical invariants, in: 29th {USENIX} Security Symposium ({USENIX} Security 20), 2020, pp. 895–912.

[189] A. Pütz, A. Zlocki, J. Bock, L. Eckstein, System validation of highly automated vehicles with a database of relevant traffic scenarios, situations 1 (2017) 19–22.

[190] R. B. Banerjee, Development of a simulation-based platform for autonomous vehicle algorithm validation, Ph.D. thesis, Massachusetts Institute of Technology, 2019.

[191] C. Oham, S. S. Kanhere, R. Jurdak, S. Jha, A blockchain based liability attribution framework for autonomous vehicles, arXiv preprint arXiv:1802.05050 (2018).

[192] S. Iqbal, A. Haque, M. Zulkernine, Towards a security architecture for protecting connected vehicles from malware, in: 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), 2019, pp. 1–5. doi:`10.1109/VTCSpring.2019.8746516`.

[193] D. Zelle, R. Rieke, C. Plappert, C. Krauß, D. Levshun, A. Chechulin, Sepad–security evaluation platform for autonomous driving, in: 2020 28th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), IEEE, 2020, pp. 413–420.

[194] F. Rosique, P. J. Navarro, C. Fernández, A. Padilla, A systematic review of perception system and simulators for autonomous vehicles research, Sensors 19 (2019) 648.

[195] P. Jing, H. Hu, F. Zhan, Y. Chen, Y. Shi, Agent-based simulation of autonomous vehicles: A systematic literature review, IEEE Access 8 (2020) 79089–79103.

[196] Q. Chao, H. Bi, W. Li, T. Mao, Z. Wang, M. C. Lin, Z. Deng, A survey on visual traffic simulation: Models, evaluations, and applications in autonomous driving, in: Computer Graphics Forum, volume 39, Wiley Online Library, 2020, pp. 287–308.

[197] W. Huang, K. Wang, Y. Lv, F. Zhu, Autonomous vehicles testing methods review, in: 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), IEEE, 2016, pp. 163–168.

[198] G. D'Antonio, M. De Maddis, J. S. Bedolla, P. Chiabert, F. Lombardi, Analytical models for the evaluation of deep-lane autonomous vehicle storage and retrieval system performance, The International Journal of Advanced Manufacturing Technology 94 (2018) 1811–1824.

[199] J. Ivanchev, T. Braud, D. Eckhoff, D. Zehe, A. Knoll, A. Sangiovanni-Vincentelli, On the need for novel tools and models for mixed traffic analysis, in: 26th ITS World Congress, Singapore, 2019.

[200] A. Ghiasi, X. Li, J. Ma, A mixed traffic speed harmonization model with connected autonomous vehicles, Transportation Research Part C: Emerging Technologies 104 (2019) 210–233.

[201] P. Bhavsar, P. Das, M. Paugh, K. Dey, M. Chowdhury, Risk analysis of autonomous vehicles in mixed traffic streams, Transportation Research Record 2625 (2017) 51–61.

[202] J. Cui, B. Zhang, Vera: A simplified security risk analysis method for autonomous vehicles, IEEE Transactions on Vehicular Technology 69 (2020) 10494–10505. doi:`10.1109/TVT.2020.3009165`.

[203] Z. Zhao, Y. Chen, Z. Hu, Minimum delay routing for connected and autonomous vehicles communications, in: 2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), 2020, pp. 1–5. doi:`10.1109/CSNDSP49049.2020.9249520`.

[204] X. Ji, W. Xu, C. Zhang, T. Yun, G. Zhang, X. Wang, Y. Wang, B. Liu, Keep forwarding path freshest in vanet via applying reinforcement learning, in: 2019 IEEE First International Workshop on Network Meets Intelligent Computations (NMIC), 2019, pp. 13–18. doi:`10.1109/NMIC.2019.00008`.

[205] R. A. Nazib, S. Moh, Reinforcement learning-based routing protocols for vehicular ad hoc networks: A comparative survey, IEEE Access 9 (2021) 27552–27587. doi:`10.1109/ACCESS.2021.3058388`.

[206] B. Häfner, J. Jiru, K. Roscher, J. Ott, G. A. Schmitt, Y. Sevilmis, Cvip: A protocol for complex interactions among connected vehicles, in: 2020 IEEE Intelligent Vehicles Symposium (IV), 2020, pp. 510–515. doi:`10.1109/IV47402.2020.9304556`.

[207] M. A. Panhwar, S. A. Khuhro, T. Mazhar, D. ZhongLiang, M. Bilal, N. Qadir, Li-net: towards a smart li-fi vehicle network, Indian Journal of Science and Technology 13 (2020) 1–9.

[208] J. I. Janjua, T. A. Khan, M. S. Khan, M. Nadeem, Li-fi communications in smart cities for truly connected vehicles, in: 2021 2nd International Conference On Smart Cities, Automation & Intelligent Computing Systems (ICON-SONICS), IEEE, 2021, pp. 1–6.

[209] B. Ying, A. Nayak, Anonymous and lightweight authentication for secure vehicular networks, IEEE Transactions on Vehicular Technology 66 (2017) 10626–10636. doi:`10.1109/TVT.2017.2744182`.

[210] C.-M. Chen, B. Xiang, Y. Liu, K.-H. Wang, A secure authentication protocol for internet of vehicles, IEEE Access 7 (2019) 12047–12057. doi:`10.1109/ACCESS.2019.2891105`.

[211] M. Tsao, K. Yang, K. Gopalakrishnan, M. Pavone, Private and decentralized location sharing for congestion-aware routing, arXiv preprint arXiv:2202.13305 (2022).

[212] N. Phan, X. Wu, H. Hu, D. Dou, Adaptive laplace mechanism: Differential privacy preservation in deep learning, in: 2017 IEEE international conference on data mining (ICDM), IEEE, 2017, pp. 385–394.

[213] R. Gupta, S. Tanwar, N. Kumar, B-iomv: Blockchain-based onion routing protocol for d2d communication in an iomv environment beyond 5g, Vehicular Communications 33 (2022) 100401.

[214] M. Shariq, K. Singh, P. K. Maurya, A. Ahmadian, D. Taniar, Anonsurp: an anonymous and secure ultralightweight rfid protocol for deployment in internet of vehicles systems, The Journal of Supercomputing (2022) 1–26.

[215] L. Alouache, N. Nguyen, R. Chelouah, M. Aliouat, HSDN-GRA: a Hybrid SDN-based Geographic Routing Protocol with Multi-agent Approach, International Journal of Communication Systems (2020). doi:`10.1002/dac.4521`.

[216] S. Harrabi, W. Chainbi, K. Ghedira, A multi-agent proactive routing protocol for vehicular ad-hoc networks, in: The 2014 International Symposium on Networks, Computers and Communications, IEEE, 2014, pp. 1–6.

[217] S. Harrabi, I. B. Jaffar, K. Ghedira, Novel optimized routing scheme for VANETs, Procedia Computer Science 98 (2016) 32–39.

[218] A. Chattopadhyay, K.-Y. Lam, Y. Tavva, Autonomous vehicle: Security by design, IEEE Transactions on Intelligent Transportation Systems (2020).

[219] P. Škorput, S. Mandžuka, S. Bermanec, H. Vojvodić, Cybersecurity of autonomous and connected vehicles, in: International Conference "New Technologies, Development and Applications", Springer, 2020, pp. 547–553.

[220] S. Chuprov, I. Viksnin, I. Kim, L. Reznikand, I. Khokhlov, Reputation and trust models with data quality metrics for improving autonomous vehicles traffic security and safety, in: 2020 IEEE Systems Security Symposium (SSS), IEEE, 2020, pp. 1–8.

[221] M. Ito, Supporting process design in the autonomous era with new standards and guidelines, in: European Conference on Software Process Improvement, Springer, 2020, pp. 525–535.

[222] V. K. Kukkala, S. Pasricha, T. Bradley, Sedan: Security-aware design of time-critical automotive networks, IEEE Transactions on Vehicular Technology 69 (2020) 9017–9030.

[223] A. Jakaria, Formal Techniques for Automated Design of Adaptive Networked Systems Based on Security and Resiliency Requirements, Ph.D. thesis, Tennessee Technological University, 2020.

[224] T. Dirsehan, C. Can, Examination of trust and sustainability concerns in autonomous vehicle adoption, Technology in Society (2020) 101361.

[225] J. Guo, Q. Yang, S. Fu, R. Boyles, S. Turner, K. Clarke, Towards trustworthy perception information sharing on connected and autonomous vehicles, in: 2020 International Conference on Connected and Autonomous Driving (MetroCAD), IEEE, 2020, pp. 85–90.

[226] U. Javaid, M. N. Aman, B. Sikdar, A scalable protocol for driving trust management in internet of vehicles with blockchain, IEEE Internet of Things Journal (2020).

[227] M. Chowdhury, A. Gawande, L. Wang, Secure information sharing among autonomous vehicles in NDN, in: 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), IEEE, 2017, pp. 15–26.

[228] D. DiMase, Z. A. Collier, J. Chandy, B. S. Cohen, G. D'Anna, H. Dunlap, J. Hallman, J. Mandelbaum, J. Ritchie, L. Vessels, A holistic approach to cyber physical systems security and resilience, in: 2020 IEEE Systems Security Symposium (SSS), IEEE, 2020, pp. 1–8.

[229] X. Ge, Ultra-reliable low-latency communications in autonomous vehicular networks, IEEE Transactions on Vehicular Technology 68 (2019) 5005–5016.

[230] X. Liu, Y. Liu, Y. Chen, L. Wang, Z. Lu, Reinforcement learning in v2i communication assisted autonomous driving, in: IEEE International Conference on Communications (ICC), IEEE, 2020, pp. 1–6.

[231] T. Sharma, A. K. Sharma, et al., Heterogeneous-internet of vehicles (Het-IoV) in twenty-first century: a comprehensive study, in: Handbook of Computer Networks and Cyber Security, Springer, 2020, pp. 555–584.

[232] S. Gautham, A. Rajagopala, A. V. Jayakumar, C. Deloglos, E. Karincic, C. Elks, Heterogeneous runtime verification of safety critical cyber physical systems, arXiv preprint arXiv:2009.09533 (2020).

[233] R. Shrestha, S. Y. Nam, R. Bajracharya, S. Kim, Evolution of V2X communication and integration of blockchain for security enhancements, Electronics 9 (2020) 1338.

[234] D. Püllen, N. A. Anagnostopoulos, T. Arul, S. Katzenbeisser, Security and safety co-engineering of the flexray bus in vehicular networks, in: Proceedings of the International Conference on Omni-Layer Intelligent Systems, 2019, pp. 31–37.

[235] A. Yazdinejad, A. Dehghantanha, G. Srivastava, Ap2fl: auditable privacy-preserving federated learning framework for electronics in healthcare, IEEE Transactions on Consumer Electronics (2023).

[236] D. Namakshenas, A. Yazdinejad, A. Dehghantanha, G. Srivastava, Federated quantum-based privacy-preserving threat detection model for consumer internet of things, IEEE Transactions on Consumer Electronics (2024).

[237] A. Yazdinejad, A. Dehghantanha, G. Srivastava, H. Karimipour, R. M. Parizi, Hybrid privacy preserving federated learning against irregular users in next-generation internet of things, Journal of Systems Architecture (2024) 103088.