A Systematic Literature Review on Cybersecurity in Autonomous Vehicles

Issa Morad[1,†], Yousef Yako[1,†]

[1]Jönköping University, School of Engineering, Computer Science and Informatics.

Abstract

This systematic literature review explores the critical cybersecurity challenges associated with autonomous vehicles (AVs), with a particular focus on message spoofing in Vehicle-to-Vehicle (V2V) communication. As AVs increasingly rely on interconnected systems for navigation, coordination, and decision-making, they become vulnerable to sophisticated cyber threats that can undermine their operational safety and reliability. Message spoofing—where false or malicious data is injected into V2V communication channels—can mislead vehicle responses, cause unsafe maneuvers, and disrupt overall traffic flow. This study examines existing detection and mitigation strategies, emphasizing the growing importance of artificial intelligence (AI) in enhancing AV cybersecurity. Through a systematic analysis of the literature, the review identifies key vulnerabilities in vehicular communication systems and highlights AI-based anomaly detection as a promising solution for identifying spoofing attacks in real time. This research underscores the necessity of developing comprehensive security frameworks to ensure the safe integration of AVs into modern transportation systems.

Keywords

Autonomous Vehicles (AVs), Cybersecurity, Vehicle-to-Vehicle (V2V) Communication, Message Spoofing, Artificial Intelligence (AI), Anomaly Detection, Systematic Literature Review (SLR)

1. Introduction

The advancement of autonomous vehicles (AVs) marks a revolutionary shift in transportation, integrating artificial intelligence (AI), sensor technologies, and Vehicle-to-Everything (V2X) communication to enhance mobility, safety, and efficiency. As these vehicles increasingly rely on digital ecosystems to navigate roads autonomously, they become highly dependent on real-time data exchange with other vehicles, infrastructure, and pedestrians. However, this interconnectivity also introduces significant cybersecurity challenges, making AVs susceptible to cyberattacks that could compromise their functionality, safety, and public trust [1].

Cybersecurity in AVs is a rapidly evolving field, with researchers and industry experts working to identify, mitigate, and prevent cyber threats targeting V2X communication. Attacks such as message spoofing, denial-of-service (DoS) incidents, and sensor manipulation pose serious risks to both AVs and civilians. Cybercriminals can exploit vulnerabilities to manipulate vehicle behavior, cause traffic disruptions, or even endanger lives [2]. The complexity of AV systems requires robust security measures to ensure data integrity, system resilience, and passenger safety. Without effective cybersecurity mechanisms, the widespread adoption of AV technology could be significantly hindered [3].

Even if the vehicle, its internal systems, and its communication with other vehicles are fully protected against cyber threats, an attacker may carry out an attack in the environment where the AV is moving. A possible attack of this kind is represented by the GPS spoofing attack, for example, real-time GPS spoofing attack detection exploiting a Bhattacharyya distance metric in the CARLA simulator [4].

The motivation behind this study stems from the increasing reliance on V2X communication in autonomous mobility and the associated cybersecurity risks. The growing number of real-world cyber incidents, such as the 2015 Jeep Cherokee hack [5], has demonstrated the vulnerabilities in modern vehicle systems. In that case, researchers remotely gained control over a vehicle's braking and acceleration, highlighting the potential dangers of unsecured automotive networks. Additionally, GPS spoofing attacks have been shown to manipulate vehicle navigation systems, leading to unsafe driving decisions [6]. These threats underscore the urgent need for improved security solutions. Furthermore,

[†]Authors are listed in alphabetical order. The authors contributed equally.

international standards such as the ISO/SAE 21434 standard [7] have emphasized the importance of developing a structured approach to automotive cybersecurity. While these regulations provide guidelines, the fast-paced evolution of AV technology means that security measures must continuously adapt to emerging threats [8].

Ensuring that communication in AVs is secure is critical to their safe operation. One major threat in this domain is message spoofing in Vehicle-to-Vehicle (V2V) communication, where malicious actors inject false data to manipulate AV behavior. Such incidents can result in traffic disruptions or even accidents by misleading the system and causing incorrect decision making [9].

Sedar et al. [10] explore anomaly detection based on AI as a promising solution for detecting and preventing real-time cyber threats. The study highlights how AI techniques can analyze vast amounts of V2X communication data to identify suspicious activity, making them a key component of future AV security architectures.

The aim of this study is to investigate how message spoofing attacks affect V2V communication, what strategies are used to detect and mitigate these threats, and explore how AI-based anomaly detection is used against spoofing in V2V communication.

The research will be conducted through a systematic review of the literature (SLR) [11]. The current state of the art on V2V message spoofing and AI-based countermeasures will be analyzed. The findings will facilitate the identification of key trends and gaps in current defense strategies. This research will contribute to the advancement of cybersecurity in autonomous vehicle ecosystems by highlighting trends and giving an overview into how AI can be applied to make V2V communication safer.

1.1. Problem statement

The cybersecurity of AVs has become a critical concern, particularly as V2V communication plays an increasingly vital role in AV coordination and decision-making. V2V communication enables real-time data exchange between vehicles, improving traffic efficiency and road safety. However, this reliance on wireless communication also introduces significant security risks that could be exploited by malicious actors [9].

One of the most pressing concerns in V2V communication is message spoofing, where attackers inject false data into the network, misleading AVs into making incorrect decisions. Such attacks can disrupt traffic flow, cause accidents, and undermine trust in autonomous driving systems. Understanding the mechanisms behind message spoofing and developing effective detection and mitigation strategies are critical to ensuring the security of AV networks [2].

AI offers a promising approach to strengthening AV cybersecurity. AI-driven models can analyze patterns in communication data to detect anomalies and identify potential cyber threats in real time [6]. This research explores the application of AI-based techniques for enhancing AV security, with a particular focus on detecting and mitigating message spoofing attacks in V2V communication.

Addressing these challenges is crucial for the safe integration of autonomous vehicles into modern transportation systems. To guide this study, the following research questions have been formulated:

1. How do message spoofing attacks compromise the security of Vehicle-to-Vehicle (V2V) communication in autonomous vehicles?
2. What strategies are used to detect and mitigate message spoofing attacks in V2V communication?
3. How is AI-based anomaly detection used in relation to cybersecurity in autonomous vehicles, particularly against spoofing in V2V communication?

1.2. Scope and limitations

This study focuses on the cybersecurity threats associated with Vehicle-to-Vehicle (V2V) communication in autonomous vehicles (AVs), with a particular emphasis on message spoofing attacks. While the broader Vehicle-to-Everything (V2X) ecosystem, including Vehicle-to-Pedestrian (V2P) communication, presents additional security concerns, this research primarily examines V2V communication due to its critical role in AV coordination and decision-making.

The scope of this research is defined by three key focus areas:

Message Spoofing in V2V Communication – Investigating how adversaries manipulate AV behavior by injecting false messages into the network, leading to unsafe driving decisions and potential traffic disruptions [2].

Detection and Mitigation Strategies for Message Spoofing – Evaluating existing security mechanisms and exploring their effectiveness in preventing malicious data manipulation [2].

AI-Based Anomaly Detection for Cybersecurity in AVs – Examining how AI techniques can enhance real-time threat detection and improve the resilience of V2V communication networks [6].

Although the study acknowledges cybersecurity threats in V2X communication more broadly, including denial-of-service (DoS) attacks [3] in V2P communication as an example, it will not be further investigated in this study because the main focus remains on the spoofing of V2V messages. The findings aim to contribute to the development of more secure AV ecosystems by offering insights into AI-driven cybersecurity solutions. By narrowing the research scope to these specific areas, this study ensures a focused and in-depth analysis within the constraints of available time and resources.

2. Background

The integration of autonomous vehicles (AVs) into modern transportation systems represents a significant technological advancement. These vehicles leverage advanced software, artificial intelligence (AI), and cyber-physical systems to enhance mobility, safety, and efficiency. A key component enabling this transformation is Vehicle-to-Everything (V2X) communication, which allows AVs to exchange real-time data with other vehicles, infrastructure, and road users. However, this increased connectivity also introduces critical cybersecurity challenges, requiring robust protection mechanisms to ensure the reliability and safety of AV networks [5, 12].

2.1. Vehicle-to-Everything (V2X) Communication and Its Importance

V2X communication is fundamental to autonomous mobility, allowing vehicles to exchange critical information such as speed, position, direction, and road conditions. The four primary modes of V2X communication—Vehicle-to-Vehicle (V2V), Vehicle-to-Pedestrian (V2P), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Network (V2N)—work together to create a connected transportation ecosystem that supports real-time decision-making and automation. Figure 1 illustrates the different V2X connectivity modes within the Internet-of-Vehicles (IoV) paradigm, demonstrating their role in traffic efficiency and safety [10].

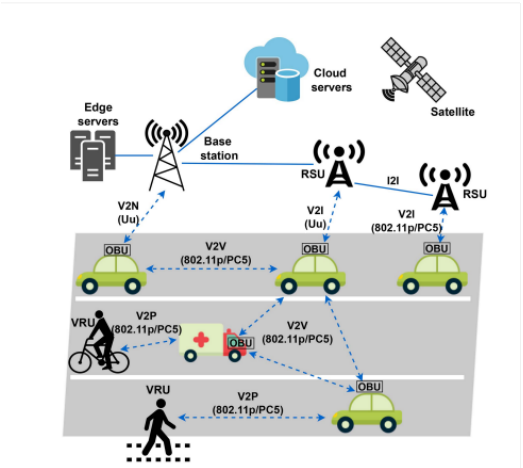

Figure 1: V2X connectivity modes composing Internet-of-Vehicles (IoV) paradigm. Via Sedar et al. [10]

Among these, V2V communication plays a crucial role in enhancing road safety by enabling vehicles to share real-time data about their movements, allowing autonomous systems to predict and respond to potential hazards. Similarly, V2P communication improves pedestrian safety by enabling AVs to detect and communicate with pedestrians through mobile devices, wearables, or roadside infrastructure, reducing accident risks in urban environments [10].

However, these systems rely on wireless communication protocols such as Dedicated Short-Range Communications (DSRC) and Cellular Vehicle-to-Everything (C-V2X), which are vulnerable to cyberattacks [5]. Securing these communication channels is essential to prevent unauthorized access, data manipulation, and potential disruptions that could compromise AV safety.

2.2. Cybersecurity Threats in V2V Communication

Vehicle-to-Vehicle (V2V) communication is essential for enhancing AV coordination. This communication introduces significant cybersecurity challenges. Vehicle decision making and overall traffic safety are compromised when AVs are exposed to malicious attacks through wireless communication. Some threats in this domain include message spoofing, replay attacks, and man-in-the-middle attacks. These threats can lead to severe safety risks [13].

2.2.1. Message Spoofing in V2V Communication

Message spoofing occurs when an attacker injects falsified messages into the V2V network. These messages deceive the AVs into making unsafe driving decisions. They can manipulate vehicle behavior by creating fake emergency warnings, altering speed, or inventing non-existent obstacles. These attacks can lead to collisions on the road and dangerous traffic disruptions [10].

2.2.2. Other Cybersecurity Concerns in V2X Communication

While this study focuses specifically on message spoofing in V2V communication, it is worth mentioning some of the different threats that exist in the V2X ecosystem:

Denial-of-Service (DoS) Attacks in V2P Communication: A DoS attack can overwhelm V2P communication channels, preventing the transmission of critical safety messages between vehicles and pedestrians. This can delay or block alerts that warn AVs about pedestrian presence, significantly increasing the risk of accidents in high-traffic urban areas [10].

Sensor Manipulation Attacks: AVs depend on sensors such as LiDAR, radar, and cameras to perceive their surroundings. Attackers can interfere with these sensor signals, causing vehicles to misinterpret their environment and make unsafe driving decisions [12].

Weaknesses in Communication Protocols: Protocols like the Controller Area Network (CAN) bus lack encryption, making them vulnerable to unauthorized access. Attackers can intercept and manipulate V2X communication data, leading to severe security breaches [5].

2.3. Real-World Cybersecurity Incidents in AVs

Real-world incidents highlight the risks posed by cybersecurity vulnerabilities in AVs. One of the most notable cases is the 2015 Jeep Cherokee hack, where researchers remotely gained control over the vehicle's braking and acceleration systems through its internet-connected infotainment system. This incident underscored the dangers of unsecured V2X communication and the urgent need for robust security mechanisms [12]. More incidents are described and discussed in chapter 5.1.

Similarly, documented GPS spoofing attacks have demonstrated how attackers can manipulate AVs navigation systems, causing vehicles to follow incorrect routes or misinterpret their surroundings. These incidents emphasize the necessity for advanced cybersecurity solutions to protect AVs from evolving cyber threats [6].

2.4. Cybersecurity Solutions in Autonomous Vehicles

As AVs continue to evolve, securing Vehicle-to-Everything (V2X) communication remains a critical challenge. The interconnected nature of AVs makes them susceptible to cyber threats, including message spoofing in Vehicle-to-Vehicle (V2V) communication and Denial-of-Service (DoS) attacks in Vehicle-to-Pedestrian (V2P) communication.

Key Cybersecurity Strategies Several security mechanisms have been proposed to address vulnerabilities in AV communication networks:

Cryptographic Security Protocols: Encryption techniques such as Public Key Infrastructure (PKI) and lightweight cryptographic algorithms help protect V2X communication from unauthorized access and data tampering while maintaining the low-latency requirements of AV systems. Secure authentication protocols, including digital signatures and message integrity verification, further prevent attackers from injecting malicious data into V2V and V2X communication channels [14].

AI-Based Intrusion Detection Systems (IDS): AI plays a crucial role in real-time threat detection by analyzing patterns in V2X data streams. AI-driven anomaly detection can identify message spoofing attempts, sensor manipulation, and abnormal network behavior, allowing for proactive cybersecurity defense [8].

Blockchain for Secure Data Transmission: Blockchain technology provides a decentralized and tamper-resistant framework for securing V2X messages. By recording communication logs in an immutable ledger, blockchain enhances data integrity and prevents unauthorized modifications, reducing the risk of message spoofing and other cyber threats [10].

Regulatory Compliance and Standardization: Adhering to international cybersecurity standards, such as ISO/SAE 21434 [7], ensures a structured approach to risk management in AV ecosystems. Strengthening regulatory frameworks and enforcing compliance across manufacturers and suppliers will be essential for enhancing security in V2X networks.

Hybrid Security Architectures: A comprehensive defense mechanism combines multiple cybersecurity techniques, such as cryptographic authentication, AI-based anomaly detection, and blockchain-secured communication. These layered protections create a robust and adaptive security framework capable of addressing evolving cyber threats in AV environments [5].

3. Method

This research will employ a systematic literature review (SLR) to analyze cybersecurity vulnerabilities in autonomous vehicles (AVs). The method selection of a systematic literature review was chosen because of different reasons. First of all, a SLR provides insights into cybersecurity concerns in AVs, revealing themes such as trust, safety, and responsibility [15]. A SLR provides structure and replicable approach to reviewing existing cybersecurity research in AVs. It also allows for the identification of vulnerabilities that are recurring and mitigation strategies across multiple studies and papers. The literature review will identify key threats in Vehicle-to-Vehicle (V2V) communication systems and examine AI-driven defense solutions.

By applying an SLR on cybersecurity for AVs, this research will contribute to an understanding of the security of V2V communication systems.

Based on the review in [16], a systematic literature review enables the identification of emerging cybersecurity threats specific to CAVs. This approach will involve analyzing peer-reviewed journal articles, case studies, and documented cybersecurity incidents, such as the 2015 Jeep hack [12], to identify recurring themes and patterns in vulnerabilities, threats, and defenses.

Previous research has shown that conducting a SLR is effective due to its structured data collection methods, comparative analysis of security threats, and identification of gaps in existing research [11, 17]. The insights gained from this work will serve as a foundation for future research and practical implementations aimed at strengthening AV cybersecurity.

3.1. Systematic Literature Review Process

The SLR will follow the known guidelines that were proposed by Kitchenham and Charters [11] and Petticrew and Roberts [18]. They outline an approach with multiple steps to follow in order to systematically identify and analyze the relevant literature. The following text will provide the key steps in the process.

In the first step we need to define clear research questions that will be answered by the SLR. The questions define the scope of the study and will ensure that the review remains focused on the relevant threats in cybersecurity within V2V communication, particularly in the context of message spoofing, and how AI can improve detection.

The research questions have been defined in the problem section chapter in the introduction of this study (1.1). The questions have been selected because they focus on specific cybersecurity threats within V2V communication and AI-driven defense solutions.

The first two questions are related to the threat of message spoofing in V2V networks that can mislead AVs with incorrect traffic information and potentially cause accidents on the roads [12].

The third question addresses AI-based anomaly detection as a solution. V2V is very complex, therefore AI techniques are being explored for their potential of detecting and mitigating the message spoofing attacks [15].

By narrowing the research to these areas, the aim of the study will be to provide an overview into AV cybersecurity by addressing V2V spoofing and AI-driven defense mechanisms.

In order to ensure the study maintains its relevancy and quality of the selected studies, there needs to be predefined inclusion and exclusion criteria that will be applied. This criteria will facilitate narrowing down the number of articles that will be reviewed.

Inclusion Criteria:

- Peer-reviewed journal articles and conference papers.
- Studies published from 2015 to 2025 to ensure up-to-date findings from the last 10 years.
- Research explicitly addressing cybersecurity in AVs, with a focus on V2V communication and message spoofing attacks.
- Studies exploring AI-driven cybersecurity solutions for detecting and mitigating threats in V2V networks.

Exclusions Criteria:

- Non-English publications.
- Non-peer-reviewed sources.
- Studies excplicitly focusing on non-cybersecurity aspects of AVs (e.g., traffic control).

A systematic search will be conducted. The following databases will be prioritized, but journals and papers from other databases will be used as long as they are relevant and match the inclusion criteria.

- IEEE Xplore
- SpringerLink
- Scopus
- Google Scholar (searching for papers)

It is also important to use the same search string in order to search for papers. The following search string will be used for this SLR:

> (”autonomous vehicle” OR ”connected vehicle” OR ”V2V communication”) AND (”cybersecurity” OR ”cyber threats” OR ”security vulnerabilities”) AND (”artificial intelligence” OR ”intrusion detection”) AND (”message spoofing”)

The studies that are selected will be analyzed based on some key parameters. These key parameters include:

Identified cybersecurity vulnerabilities – Threats in V2V communication with a particular emphasis on message spoofing attacks. This includes potential consequences of successful attacks on AV safety and decision-making.

Detection and Mitigation Strategies – Security mechanisms proposed in the literature to counteract message spoofing. This includes cryptographic solutions, anomaly detection systems, and other security frameworks.

Artificial Intelligence (AI) Applications – The role of techniques that are AI-driven and secure V2V communication. This includes both supervised and unsupervised learning methods, and real-time anomaly detection approaches.

The data that is extracted from the studies will be synthesized using a narrative synthesis approach by Popay et al. [19] in order to identify common themes, trends, and research gaps in the papers.

To ensure the reliability and relevance of the studies, a quality assessment checklist adapted from Kitchenham and Charters [11] will be used. Each study will be evaluated based on the following points:

- **QA1: Clarity of the research objectives** – The study must clearly define its research objectives, describing the specific cybersecurity challenges to be addressed and the intended contributions to the field of V2V communication security.
- **QA2: Methodological rigor** – The study should follow a well-defined research methodology, including appropriate data collection, experimental setup, or analytical approach, ensuring that the findings are based on robust and replicable methods.
- **QA3: Relevance to the research questions of this study** – The research must directly contribute to answering at least one of the research questions related to message spoofing attacks, detection and mitigation strategies, or AI-driven cybersecurity solutions in V2V communication.
- **QA4: Transparency of the findings** – The study should provide clear and detailed results, including explanations of the methodologies, data sets, and evaluation metrics, ensuring that the conclusions are well supported and reproducible.

Studies that do not meet these points will be excluded from the final synthesis.

After the final set of studies are selected, an analysis of relevant insights from the papers will be conducted. Relevant insights include and focus primarily on identifying how each paper discusses issues related to message spoofing, including their vulnerabilities, real-world implications, and specific threats according to the authors. The attention will be particularly on the proposed mitigation strategies, especially the strategies involving AI-driven anomaly detection techniques.

The key findings will be synthesized, by applying the narrative synthesis approach that is described by Popay et al. [19], to identify recurring patterns and technological gaps across the literature. The synthesis process will follow four main stages.

First, a theoretical framework will be developed to clarify how message spoofing attacks and AI-based anomaly detection function within V2V communication. This has been done in chapter 2 by identifying how spoofing compromises CV systems and how AI techniques mitigate these threats.

Second, a preliminary synthesis will be made to summarize the findings of the studies. This will be achieved through tabulated comparisons.

Third, relationships between the data will be explored to see how different factors – such as the type of systems targeted or the AI method applied – influence the outcome.

Finally, the robustness of the synthesis will be assessed by looking at the consistency and strength of evidence of the conclusions across all studies.

4. Results

This chapter presents the findings from the systematic literature review. The results explore how message spoofing compromises Vehicle-to-Vehicle (V2V) communication in autonomous vehicles, the methods used to detect and mitigate such attacks, and how artificial intelligence (AI) can be applied for anomaly detection. The selected studies have been analyzed for their contributions, methodologies, and findings in relation to these subjects. The first section combines the identification of spoofing threats with mitigation strategies, while the second section focuses specifically on AI-based approaches to anomaly detection in V2V communication.

The initial search string mentioned in the method section 3.1 produced 76 results on Google Scholar. After applying the predefined inclusion and exclusion criteria, some studies were removed and 25 studies remained. These studies were reviewed using the quality assessment checklist, and 17 papers were found to meet all criteria. In addition to this process, snowballing was used to identify further relevant literature by examining both the references cited in the papers, but also the studies that cited them. This snowballing process found 2 additional papers. Although primary databases were IEEE Xplore, SpringerLink, and Scopus, studies that were found in other databases, such as ScienceDirect, ResearchGate, and arXiv, were also included, as long as they were relevant and met the inclusion and quality assessment criteria. In the end, the total number of reviewed studies was 19.

4.1. Message Spoofing in V2V Communication: Threats and Mitigation Strategies

This section examines how message spoofing attacks compromise the security of Vehicle-to-Vehicle (V2V) communication in Connected Vehicles (CVs), and what strategies are used to detect and mitigate them. Table 1 provides an overview of studies that address spoofing threats, vulnerabilities, and mitigation strategies in CVs. It summarizes each paper's focus area, identified cybersecurity threats, research methodology, use of AI-based approaches, and key findings.

Message spoofing means that someone or something injects false or manipulated messages into a V2V network with the goal of misleading the decision-making process. Several studies demonstrate that spoofed messages can cause vehicles to do things they should not do, such as brake unnecessarily, swerve into incorrect lanes, or misinterpret traffic conditions, directly threatening road safety. According to Javagal [20], spoofing is only one of many cyber threats introduced by vehicle-to-everything (V2X) communication. When attackers target CV sensors and communication systems, the resulting misinformation can propagate through the CV's control systems, leading to faulty behavior.

CAN/LIN Spoofing: Spoofing attacks that target in-vehicle communication protocols like the Controller Area Network (CAN) and Local Interconnect Network (LIN) are studied frequently. Kalkan and Sahingoz [21] simulated spoofed RPM and gear signals and showed that repetitive patterns in these messages make them suitable for machine learning-based detection. Similar to this, El-Rewini et al. [22] emphasized the ease of manipulating LIN messages to control vehicle functions such as steering and braking. Parandkar et al. [23] extended this by proposing deep learning models like DCNN and SNN, which offer high detection accuracy, making them suitable for real-time use. Studies that address CAN and LIN spoofing consistently used ensemble machine learning or deep learning models, with detection accuracies over 95% in many cases. However, most models were tested only in simulation environments, and practical integration still remains unaddressed.

GPS Spoofing: GPS spoofing, where adversaries feed false location data to vehicle systems, was examined by Annabi et al. [24] and Gao et al. [25]. The attacks often exploit the low signal strength of GPS and can redirect CVs or interfere with the navigation. Both of the studies recommend combining AI models such as LSTM and Reinforcement Learning (RL) with blockchain-based authentication to detect false signals. Most studies that mention GPS spoofing relied on learning models like LSTM or RL, focusing on detecting anomalies in positional patterns. However, these approaches are rarely tested in real-world driving scenarios and therefore have a limited practical applicability.

Perception Layer Spoofing: Studies by Pavithra et al. [26], Gozubuyuk et al. [27], and Neupane and Sun [28] explore spoofing attacks that target perception systems like LiDAR and camera inputs. These

types of attacks can often involve manipulations that are subtle in the environment, such as modified road markings or light interference, which can mislead sensor-based object detection. To protect and mitigate these attacks, one can use secure message verification, filtering techniques, and basic encryption. However, compared to CAN and GPS spoofing, these spoofing attacks are underexplored and few AI-based models are specifically trained to detect spoofed sensory input, which highlights a gap in perception-layer defenses.

Spoofing in V2V Networked Environments: Several studies focused on spoofing attacks that disrupt broader V2V communication or VANET systems. Onur et al. [29] demonstrated spoofing detection on a mini CV platform using Random Forest (RF) with over 96% accuracy. Sharma et al. [30] applied context-adaptive beacon verification for VANETs. Ming et al. [31] simulated spoofing in a tolling scenario and highlighted the impact it had on traffic flow and the cost. Herman Muraro Gularte et al. [32] wanted to push for multi-layered defenses using IDS, blockchain, and AI. While RF and AdaBoost classifiers performed well on CAN spoofing, they showed higher false positives in broader VANET settings. This suggests that algorithm performance may vary significantly by system context and the need for better context-aware models.

General or Multi-Layered Spoofing Approaches: Some studies proposed spoofing mitigation strategies that were broader and spanned multiple systems. Rathore et al. [33] recommended combining cryptography with AI in a multi-layered security framework. Limbasiya et al. [34] reported 98.9% accuracy using challenge-response authentication and radio frequency fingerprinting. Ali et al. [35] and Ahmad et al. [36] recommended lightweight cryptographic schemes together with AI. Bharati et al. [37] and Researcher [38] highlighted threat modeling and continuous monitoring through IDS. All of these studies have a consensus on the importance of layered defenses and hybrid methods. The challenge is in the integration and the need for unified evaluation metrics persist in order to compare different algorithms and models with each other.

Summary: Across all groups, message spoofing is recognized as a widespread and threat that has a very high impact in V2V communication. CAN and GPS spoofing are the most frequently addressed, often using ensemble AI models. Perception-layer spoofing is significantly underexplored, despite its potential for serious consequences. Moreover, most detection systems remain untested in real-world environments, and there is a lack of standard metrics to compare performance across studies.

To better illustrate the relationship between spoofing threats and mitigation approaches, including the role of AI, Figure 2 presents a conceptual flowchart. It visualizes the process of how spoofed messages are detected in real time using AI-based anomaly detection models such as Random Forest and LSTM.

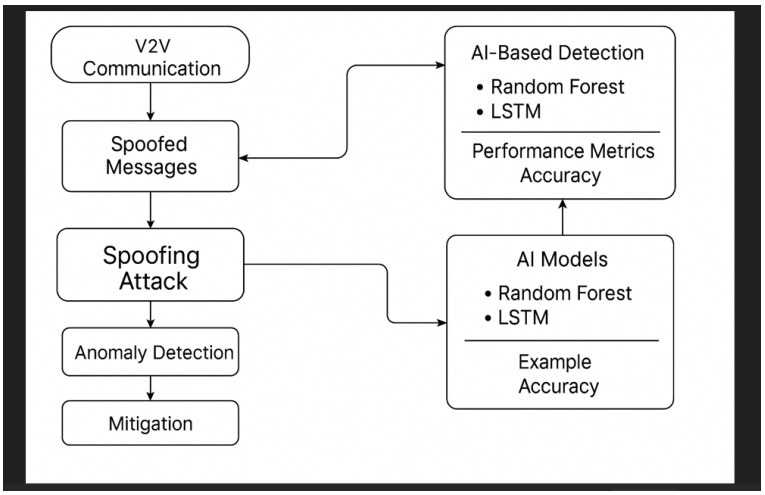

Figure 2: Overview of spoofing threats in V2V communication and AI-based mitigation strategies, including anomaly detection models used for real-time detection and response.

Table 1: Overview of Research Papers That Discuss Spoofing

Paper	Focus Area	Cybersecurity Threat	Methodology	AI-based Approach	Key Findings
Javagal [20] (2023)	General V2X threats	Message spoofing	Theoretical analysis	No	Spoofing attacks disrupt AV control layers via sensor/communication layers.
Onur et al. [29] (2024)	Mini autonomous vehicle testing	Message spoofing	Experimental (real-world vehicle)	Random Forest	Spoofed messages detectable with 96%+ accuracy.
Rathore et al. [33] (2022)	In-vehicle communication security	Internal spoofing	Protocol-level vulnerability review	Combined cryptography + AI	AI and crypto jointly needed for spoofing defense.
El-Rewini et al. [22] (2020)	LIN protocol vulnerabilities	Message spoofing in LIN	Architecture exploitation	Intrusion detection + fallback	LIN spoofing can disable functions, detection essential.
Kalkan and Sahingoz [21] (2020)	CAN bus intrusion detection	CAN spoofing	Signal manipulation experiment	Ensemble models	Predictable spoofing makes detection feasible.
Parandkar et al. [23] (2024)	In-vehicle network neuromorphic IDS	CAN message spoofing	Simulation	Deep CNNs + SNNs	High detection rate, energy-efficient.
Annabi et al. [24] (2024)	Sensor spoofing (GPS/LiDAR)	GPS, LiDAR spoofing	Literature review	LSTM + blockchain	Combined techniques improve positioning spoofing resilience.
Gao et al. [25] (2022)	GPS spoofing in AVs	GPS spoofing	Threat modeling	Reinforcement learning	AI improves GPS spoofing detection and adaptation.
Neupane and Sun [28] (2025)	Sensor attacks	LiDAR/camera spoofing	Threat analysis	Filtering + encryption	Secures perception layers in AVs.
Pavithra et al. [26] (2023)	Perceptual spoofing	Physical spoofing	Scenario analysis	Not specified	Minor changes (e.g. markings) can spoof AV sensors.
Gozubuyuk et al. [27] (2023)	Lightweight security in AVs	Message spoofing	System model testing	Not specified	Lightweight crypto + authentication help mitigate spoofing.
Ming et al. [31] (2018)	VANET tolling simulation	Spoofing/malicious messages	Simulation-based tolling model	Not used	Spoofing impacts cost/distance/time significantly.
Herman Muraro Gularte et al. [32] (2024)	IDS for V2X	Message spoofing	Systematic review	IDS + Blockchain	Multi-layered approach to spoofing prevention.
Sharma et al. [30] (2017)	VANET security	Beacon spoofing	Context-aware filtering	AI-optimized filters	CABV reduces resource load and increases detection.
Limbasiya et al. [34] (2022)	Authentication in VANET	Message spoofing	Radio fingerprinting + challenge-response	Not specified	98.9% detection accuracy with hybrid method.
Ali et al. [35] (2025)	Lightweight crypto for AVs	Message spoofing	Cryptographic review	AI-enhanced protocols	Stronger security with AI and ECC.
Ahmad et al. [36] (2024)	Blockchain in CAV security	Message spoofing	Literature synthesis	ML + Blockchain	Enhances data integrity and spoofing detection.
Bharati et al. [37] (2020)	Layered security modeling	System-wide spoofing	Threat modeling	Not specified	Multi-layer spoofing mitigation is vital.
Researcher [38] (2025)	IDS in automotive protocols	CAN/LIN spoofing	Protocol analysis	AI-based anomaly detection	AI IDS can continuously learn new spoofing patterns.

4.2. AI-Based Anomaly Detection

This section explores how AI-based anomaly detection is used to enhance cybersecurity in autonomous vehicles, particularly in detecting and preventing message spoofing in V2V communication. Table 2 provides an overview of the studies that apply AI-based anomaly detection methods in CVs. The table summarizes the techniques used, systems targeted, effectiveness, simulation environments, advantages and limitations, and whether they are capable of operating in real-time scenarios.

Figure 3, 4, 5, and 6 show charts that provide an overview of the reviewed studies. The figures help illustrate the scope of the reviewed literature, highlight common research focuses, and reveal research gaps.

CAN Bus and In-Vehicle Network Detection: AI techniques are often applied to detect spoofing in Controller Area Network (CAN) and other in-vehicle communication systems. Kalkan and Sahingoz [21] tested ensemble classifiers including Random Forest, AdaBoost, and Neural Networks. They achieved almost perfect accuracy in detecting spoofed RPM and gear signals. The work shows that spoofed CAN traffic often follows a pattern that is detectable which makes it suitable for algorithmic detection. Parandkar et al. [23] expanded on this by proposing energy-efficient deep learning models. This included Deep Convolutional Neural Networks (DCNNs) and Spiking Neural Networks (SNNs) that are capable of maintaining high accuracy while also being lightweight enough for real-time vehicle integration. Similar to this, Researcher [38] introduced adaptive intrusion detection systems (IDS) that can monitor CAN traffic in order to detect spoofed messages based on their behavioral anomalies and continuously learning new patterns of attack over time. Studies in this group show that ensemble and deep learning models are effective at detecting spoofing in CAN systems with high accuracy. However, the deployment of these models is often limited to controlled simulation settings. Their practical real-world testing remains limited.

GPS and Positioning System Detection: AI models that are advanced have also been proposed for spoofing detection in GPS and other positioning systems. Gao et al. [25] applied Long Short-Term Memory (LSTM) networks to identify GPS signal patterns that were not regular, together with Reinforcement Learning (RL) for adaptive response strategies in dynamic spoofing conditions. These models have their advantages in adaptability and long-term learning. This enables vehicle systems to respond to evolving spoofing attacks. Most studies that address GPS spoofing rely on sequential AI models like LSTM and RL. They are well suited to GPS data. However, these approaches are rarely used and tested in real-world driving conditions. The challenges still remain in scaling them for real-time, low-latency CV systems.

VANET and V2V Communication-Level Detection: AI-based spoofing detection has also been applied to general and broader V2V communication environments such as Vehicular Ad Hoc Networks (VANETs). Sharma et al. [30] developed a context-adaptive beacon verification (CABV) technique that uses AI filters to detect spoofed messages by using contextual features from the communication environment. By taking this approach, it minimizes computational overhead and enhances detection precision. Onur et al. [29] demonstrated through real-world experiments with a mini CV platform the effectiveness of Random Forest classifiers in detecting spoofed packets in live scenarios. The models, however, displayed more false positives and that suggests the need for improvement. While these AI approaches in VANETs show strong potential, the inconsistencies in detection performance across the environments still remain. For example, while Random Forest achieved high accuracy in CAN-based detection, their performance in VANET environments was more variable.

Summary: The literature that has been reviewed shows that AI-based anomaly detection is a powerful tool for identifying spoofed messages across various components of CV systems. Ensemble learning methods and deep neural networks consistently show high detection accuracy in CAN-based spoofing scenarios. Sequential models like LSTM and RL are preferred for GPS-based attacks. Context-aware models offer more efficient spoofing mitigation in VANET settings. Despite these advances, most models are only validated and tested in simulation environments and only a few studies explore the integration of these techniques into full CV control systems.

Table 2: Overview of Research Papers That Apply AI-Anomaly Detection

Paper	**AI Technique**	**Targeted Threat**	**Effectiveness**	**Simulation Environment**	**Advantages / Limitations**	**Real-Time Capable?**
Onur et al. [29] (2024)	Random Forest	Message Spoofing	96.1% detection rate, 93.6% for legitimate traffic	Real-world mini autonomous vehicle	Easy to implement, but needs improvement in detecting attack packets	Yes
Kalkan and Sahingoz [21] (2020)	Random Forest, AdaBoost, Neural Networks	Spoofed RPM and gear signals in CAN bus	100% accuracy, precision, recall, and F1-score	Simulated CAN traffic	High accuracy but tested only in simulations	Yes
Parandkar et al. [23] (2024)	DCNN, SNN	Spoofing in CAN and LIN protocols	>90% accuracy with low energy consumption	Not specified	Energy-efficient and scalable, but complex to train	Yes
Gao et al. [25] (2023)	LSTM, Reinforcement Learning (RL)	GPS spoofing and adaptive response	Effective for learning abnormal patterns and dynamic adjustments	Likely synthetic GPS datasets or simulation	Adaptive and robust but may need large training data	Potentially
Sharma et al. [30] (2017)	Context-Adaptive Signature Verification	VANET message spoofing	Up to 86.5% computational overhead saved, 76% spoofed beacon detection	SUMO + OMNeT++ with Veins middleware	Context-aware and lightweight; may miss outliers	Yes
Researcher [38] (2025)	AI-Based Intrusion Detection System	Behavioral spoofing in CAN traffic	Message authentication has 85% effectiveness against spoofing, while IDS shows 70%	Experimental network testbed	Continuously learns and adapts; may require high computation	Yes

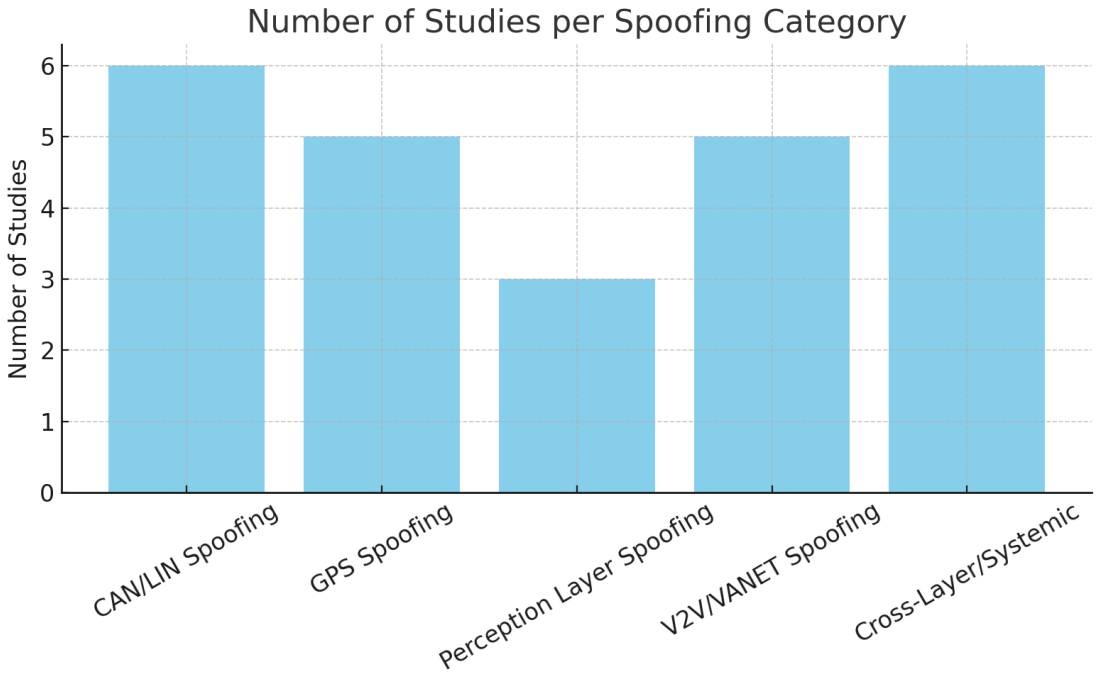

Figure 3: This bar chart shows how many reviewed studies focused on each category of spoofing threat.

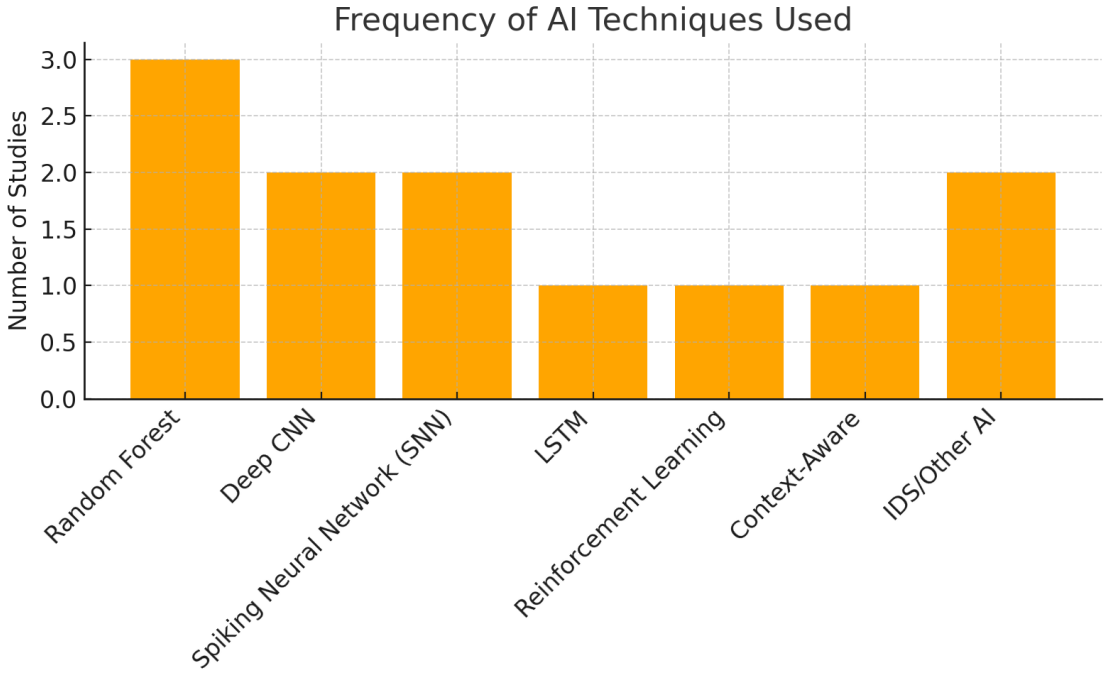

Figure 4: This bar chart displays the frequency of different AI methods applied across the reviewed studies.

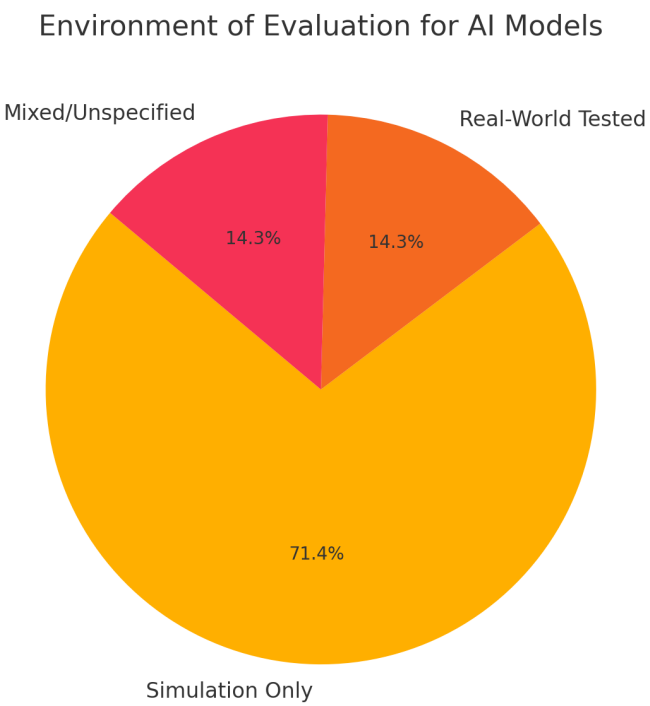

Figure 5: This pie chart shows whether the AI models were tested in simulation environments, real-world settings, or a mix of both.

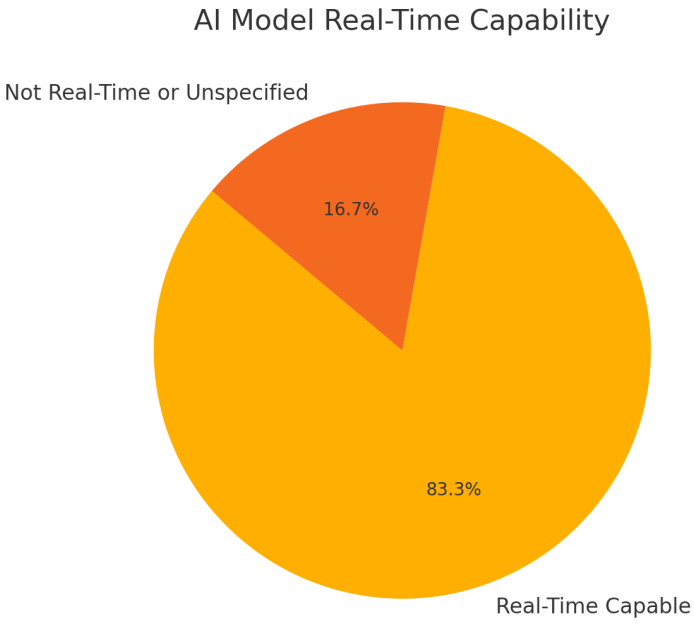

Figure 6: This pie chart illustrates the proportion of AI models that were described as real-time capable versus those that were not or whose capabilities were unspecified.

5. Discussion

This study explored the cybersecurity landscape in autonomous vehicles (AVs), focusing specifically on message spoofing in Vehicle-to-Vehicle (V2V) communication and the potential of AI-based anomaly detection mechanisms to mitigate such threats. The results from the systematic literature review (SLR) reveal a consensus on the increasing sophistication of cyberattacks targeting V2V communication and the urgent need for more robust, adaptive, and intelligent security frameworks.

5.1. Message Spoofing Threats in V2V Communication

Message spoofing emerged as a critical threat that can severely compromise the safety and decision-making capabilities of AVs. As many studies emphasized, spoofed messages can lead to false alerts, misdirected responses, and even collisions, especially in dense urban environments where communication latency and trust are paramount. Research such as that by Herman Muraro Gularte et al. [32] and El-Rewini et al. [22] illustrated how both inter-vehicle and intra-vehicle systems—like LIN and CAN buses—are vulnerable to injected falsified data, stressing the need for advanced message authentication mechanisms and fallback safety protocols.

There are various examples of real-world incidents that include spoofing threats. For example, Tesla vehicles have shown themselves being susceptible to GPS spoofing attacks [24]. These attacks emphasize the need for robust communication security inside AVs. It is true that the technology of AVs have advanced rapidly, with milestones like Google's 140,000-mile autonomous driving by 2010, VisLab's intercontinental journey in 2013, and Tesla's 2016 commercial launch of intelligent cruise control [39]. However, security protections have not always been keeping up. According to Qayyum et al. [39], this gap is evident in real-world incidents, such as Tesla's 2016 autopilot failure where it could not distinguish a white truck from the bright sky, Google's collision with a bus, and Uber's fatal pedestrian accident in 2018. These incidents that were caused by cybersecurity weaknesses demonstrate that the systems in AVs remain sensitive to cyber threats. By strengthening AI-based spoofing detection, we are potentially going to save lives in the future from fatal accidents.

The findings suggest that certain systems within AVs, particularly those that involve communication protocols such as the CAN bus and positioning systems like GPS, appear to be more vulnerable to spoofing attacks than other systems. Studies like Kalkan and Sahingoz [21] and Parandkar et al. [23] have demonstrated how spoofed messages on the CAN have the ability to easily manipulate critical vehicle functions such as RPM or gear signals. Other studies, such as Gao et al. [25] and Annabi et al. [24], emphasize how low-power GPS signals are susceptible to spoofing. These vulnerabilities are concerning because they target the low-level communication and navigation systems in the vehicle which could directly influence the core vehicle control.

Moreover, spoofing attacks were found across multiple layers of AVs. The literature, however, focuses more on the network and communication layers, such as CAN, V2V, and GPS. The perception layer, which includes sensors like LiDAR and radar, is mentioned in some studies, such as Gozubuyuk et al. [27] and Neupane and Sun [28], but the attack types remain underexplored despite their potential to mislead object detection and environmental awareness systems. This means that there is an imbalance and it suggests that detection efforts we have today may not be fully aligned with all critical threat surfaces.

5.2. Effectiveness of AI-Based Anomaly Detection

The findings also highlight how artificial intelligence, particularly through machine learning and deep learning models, plays a transformative role in detecting spoofing attempts. Techniques such as anomaly detection, context-aware filtering, and supervised classification models were applied across various studies to successfully distinguish between legitimate and malicious messages. For instance, Onur et al. [29] demonstrated how random forest models could detect spoofed packets with high accuracy, while Sharma et al. [30] proposed context-adaptive beacon verification (CABV) to minimize computational overhead in detection.

Traditional machine learning models, such as Random Forest and AdaBoost, have shown high detection accuracy in identifying spoofed messages [29, 21]. However, in real-time their performance shows that complex traffic scenarios remain less explored. Deep Convolutional Neural Networks (DCNNs) and Spiking Neural Networks (SNNs), which are deep learning approaches, offer better adaptability which makes them promising for real-world deployment [23]. Their limitations lie in their need for more computational resources and longer training periods. Context-adaptive signature verification approaches [30] present solutions that are lightweight and suitable for VANETs, which are networks that make it possible for nearby vehicles to communicate, but these approaches might struggle with detecting sophisticated spoofing attacks. Overall, while ensemble learning models offer ease of training together with robustness, deep and reinforcement learning techniques appear better suited for future-proofing the security in AVs against evolving spoofing threats, because they can learn complex patterns and dynamically adjust strategies based on interactions. Lastly, although results in simulations are promising, the real problems arrive in the real-world where we must consider network delays, sensor errors, varying environmental conditions, computational limitations of vehicle hardware, and the sheer complexity and unpredictability of live traffic scenarios.

5.3. Real-World Relevance and Limitations

Despite these advancements, the review also identified certain limitations. Many AI models face challenges related to training data quality, real-time performance, and susceptibility to adversarial attacks. Moreover, not all approaches integrated AI seamlessly with lightweight authentication, which is crucial in vehicular networks where latency and computational resources are constrained. Studies such as Ahmad et al. [36] and Ali et al. [35] proposed combining AI with blockchain or elliptic curve cryptography to enhance security while preserving performance, yet practical implementation of such hybrid systems remains in early stages.

The studies also suggest a lack of unified frameworks that integrate security from the sensor level up to the application layer. For instance, while GPS spoofing is often addressed in isolation, LiDAR and CAN-based spoofing receive comparatively less attention despite being equally critical. Moreover, the simulation-based nature of many evaluations (e.g., Ming et al. [31]) highlights the gap between theoretical proposals and real-world testing, suggesting a future need for collaborative efforts with industry stakeholders for empirical validation.

The systematic literature review (SLR) provided a structured analysis of message spoofing threats and AI-based mitigation strategies in V2V communication. However, certain limitations must be acknowledged. First, the review looked at studies published in the last 10 years (2015-2025). This may have excluded older research or very recent breakthroughs that would have been useful for this study. Secondly, only peer-reviewed journal articles that were written in English and from specific databases were considered. By doing this, we may have overlooked relevant findings from non-English publications from other databases. Third, most of the studies that were reviewed were based on simulations rather than real-world experiments, which may have limited the generalizability of the results to real driving environments. Fourth, the world of AI and cybersecurity is fast-evolving, meaning that newer methods or threats may have emerged after the literature search was completed. Fifth, although specific databases were selected, papers that were relevant and met the quality assessment criteria were discovered in other sources. A larger and more desirable number of papers may have been found if these additional databases were included from the start. Sixth, the absence of a shared evaluation metric system for quantitatively measuring the methods in the papers meant that demonstrating fair quantitative results proved very difficult. Finally, subjective judgment during paper selection and reading could introduce minor biases, even though there were predefined inclusion and exclusion criteria.

5.4. Validity and Reliability

To ensure the validity and reliability of this systematic literature review, rigorous methodologies were applied throughout the study. The review followed well-established guidelines, particularly

those proposed by Kitchenham and Charters [11], which include clearly defined research questions, transparent inclusion and exclusion criteria, and structured search strategies across multiple academic databases such as IEEE Xplore, SpringerLink, Scopus, and Google Scholar. These measures enhanced the construct validity of the review by ensuring that the selected studies were relevant to the research focus on message spoofing in V2V communication and AI-driven mitigation strategies.

Reliability was further supported through a standardized data extraction process and the use of a quality assessment checklist, evaluating each study's clarity, methodology, relevance, and transparency. Only peer-reviewed and English-language studies published between 2015 and 2025 were included, which helped maintain consistency in the sources analyzed.

However, the review is subject to certain limitations. Most notably, the exclusion of non-English publications and gray literature may have limited the scope of potentially relevant findings. Additionally, because the majority of the included studies were simulation-based, there is a limitation in external validity, meaning that the findings may not be directly generalizable to real-world conditions. Furthermore, although the selection criteria were predefined, some degree of subjectivity was unavoidable in interpreting study relevance and quality, which could introduce minor biases.

Despite these limitations, the systematic and replicable nature of the review process strengthens the internal reliability and provides a dependable foundation for further research into the cybersecurity of AV systems.

5.5. Future Work

In the future, research should focus on combining AI-based anomaly detection with cryptographic authentication techniques to create more secure spoofing detection systems for V2V communication. The detection accuracy and message integrity can be strengthened by integrating cryptographic methods such as message authentication codes with intrusion detection.

Additionally, security frameworks that combine AI with blockchain offer promising potential for decentralization and resistance to tampering. Blockchain can help create immutable logs of communication that make it more difficult for spoofed messages to go undetected.

Another direction for future work is the need to bridge the gap between theory and practice, it is very important to test spoofing detection solutions in real-world environments under diverse conditions, including rush hours, weather variations, and sensor noise.

There are many underrepresented spoofing attack types that need to be addressed in future work. GPS and CAN message spoofing are frequently studied, but attacks targeting LiDAR, radar, and ultrasonic sensors in the perception layer are less examined. If these attack vectors are more understood and analyzed, it can help to build comprehensive defense mechanisms.

At present, there is a lack of consistent benchmarks when it comes to evaluation metrics for spoofing detection. This can make it difficult to assess the real-world performance of competing models and different security solutions. There is a need for the research community to adopt shared evaluation metrics and standardized datasets for spoofing detection. By establishing evaluation frameworks that are based on precision, false positive rates, real-time capability, and more, it would enable clearer benchmarking and accelerate progress in the field.

Finally, future work could look at the integration of energy-efficient AI models. There is a need to balance detection performance with computational load in order to make AI-based spoofing detection applicable in commercial autonomous systems.

6. Conclusions

This study has systematically examined the cybersecurity challenges inherent in autonomous vehicles (AVs), with a specific focus on message spoofing within Vehicle-to-Vehicle (V2V) communication. As AV technology advances, the reliance on V2V communication for real-time data exchange among vehicles, infrastructure, and road users has become critical for enhancing safety and efficiency. However, this

interconnectivity exposes AVs to significant cybersecurity vulnerabilities, particularly through message spoofing, which can lead to incorrect decision-making and jeopardize passenger safety.

The findings of this literature review underscore the urgent need for robust cybersecurity mechanisms to protect AV systems from these threats. Notably, the application of artificial intelligence (AI) presents a promising avenue for improving security measures. AI-driven techniques, particularly those employing machine learning and deep learning, have demonstrated their potential in detecting and mitigating spoofing attacks by identifying anomalies in communication patterns.

Despite these advancements, several challenges persist, including issues of scalability, real-world applicability, and the need for comprehensive security frameworks. The study highlights the necessity of integrating multi-layered security strategies that combine cryptographic methods, AI-based anomaly detection, and fallback protocols to create a resilient defense against spoofing threats.

Furthermore, the review emphasizes the importance of empirical research to validate AI solutions in real-world scenarios. Future investigations should aim to bridge the gap between theoretical models and practical implementations, ensuring that AV systems are equipped to withstand evolving cyber threats.

In conclusion, while significant progress has been made in addressing cybersecurity for AVs, ongoing research and collaboration among industry stakeholders, regulatory bodies, and the academic community are essential for developing secure and reliable autonomous vehicle ecosystems. By prioritizing these efforts, we can enhance public trust and facilitate the safe integration of AV technology into our transportation systems.

References

[1] S. Kim, R. Shrestha, Automotive Cyber Security: Introduction, Challenges, and Standardization, Springer Singapore Pte. Limited, Singapore, 2020. doi:https://doi.org/10.1007/978-981-15-8053-6.

[2] S. Dasgupta, A. Ahmed, M. Rahman, T. N. Bandi, Unveiling the Stealthy Threat: Analyzing Slow Drift GPS Spoofing Attacks for Autonomous Vehicles in Urban Environments and Enabling the Resilience, 2024. URL: http://arxiv.org/abs/2401.01394. doi:10.48550/arXiv.2401.01394, arXiv:2401.01394.

[3] T. Stübler, A. Amodei, D. Capriglione, G. Tomasso, N. Bonnotte, S. Mohammed, An investigation of denial of service attacks on autonomous driving software and hardware in operation, in: 2024 IEEE 20th International Conference on Automation Science and Engineering (CASE), 2024, pp. 3051–3056. doi:10.1109/CASE59546.2024.10711339.

[4] C. Vitale, N. Piperigkos, C. Laoudias, G. Ellinas, J. Casademont, J. Escrig, A. Kloukiniotis, A. S. Lalos, K. Moustakas, R. Diaz Rodriguez, D. Baños, G. Roqueta Crusats, P. Kapsalas, K.-P. Hofmann, P. S. Khodashenas, CARAMEL: results on a secure architecture for connected and autonomous vehicles detecting GPS spoofing attacks, EURASIP Journal on Wireless Communications and Networking 2021 (2021) 115. URL: https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-021-01971-x. doi:10.1186/s13638-021-01971-x.

[5] 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. URL: https://www.sciencedirect.com/science/article/pii/S0001457520316572. doi:https://doi.org/10.1016/j.aap.2020.105837.

[6] M. M. Abrar, A. Youssef, R. Islam, S. Satam, B. S. Latibari, S. Hariri, S. Shao, S. Salehi, P. Satam, GPS-IDS: An Anomaly-based GPS Spoofing Attack Detection Framework for Autonomous Vehicles, 2024. URL: http://arxiv.org/abs/2405.08359. doi:10.48550/arXiv.2405.08359, arXiv:2405.08359.

[7] J. Henle, S. Otten, E. Sax, Systems engineering approach for compliant over-the-air update development, in: 2024 IEEE International Conference on Recent Advances in Systems Science and Engineering (RASSE), 2024, pp. 1–9. doi:10.1109/RASSE64357.2024.10773922.

[8] D. Grimm, A. Lautenbach, M. Almgren, T. Olovsson, E. Sax, Gap analysis of iso/sae 21434 –

improving the automotive cybersecurity engineering life cycle, in: 2023 IEEE 26th International Conference on Intelligent Transportation Systems (ITSC), 2023, pp. 1904–1911. doi:10.1109/ITSC57777.2023.10422100.

[9] Z.-R. Tzoannos, D. Kosmanos, A. Xenakis, C. Chaikalis, The impact of spoofing attacks in connected autonomous vehicles under traffic congestion conditions, Telecom 5 (2024) 747–759. URL: https://www.mdpi.com/2673-4001/5/3/37. doi:10.3390/telecom5030037.

[10] R. Sedar, C. Kalalas, F. Vázquez-Gallego, L. Alonso, J. Alonso-Zarate, A comprehensive survey of v2x cybersecurity mechanisms and future research paths, IEEE Open Journal of the Communications Society 4 (2023) 325–391. doi:10.1109/OJCOMS.2023.3239115.

[11] B. Kitchenham, S. Charters, Guidelines for performing systematic literature reviews in software engineering, EBSE Technical Report (2007). URL: https://legacyfileshare.elsevier.com/promis_misc/525444systematicreviewsguide.pdf.

[12] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, H. K. Kim, Cybersecurity for autonomous vehicles: Review of attacks and defense, Computers Security 103 (2021) 102150. URL: https://www.sciencedirect.com/science/article/pii/S0167404820304235. doi:https://doi.org/10.1016/j.cose.2020.102150.

[13] A. Yousseef, S. Satam, B. S. Latibari, J. Pacheco, S. Salehi, S. Hariri, P. Satam, Autonomous vehicle security: A deep dive into threat modeling, 2024. URL: https://arxiv.org/abs/2412.15348. arXiv:2412.15348.

[14] A. Giaccaglini, Implementing secured messages for V2X communication, laurea, Politecnico di Torino, 2024. URL: https://webthesis.biblio.polito.it/33907/.

[15] N. Liu, A. Nikitas, S. Parkinson, Exploring expert perceptions about the cyber security and privacy of connected and autonomous vehicles: A thematic analysis approach, Transportation Research Part F: Traffic Psychology and Behaviour 75 (2020) 66–86. URL: https://www.sciencedirect.com/science/article/pii/S1369847820305386. doi:https://doi.org/10.1016/j.trf.2020.09.019.

[16] M. Pandey, Seetharaman, A review of factors impacting cybersecurity in connected and autonomous vehicles (cavs), in: 2022 8th International Conference on Control, Decision and Information Technologies (CoDIT), volume 1, 2022, pp. 1218–1224. doi:10.1109/CoDIT55151.2022.9804071.

[17] K. Petersen, S. Vakkalanka, L. Kuzniarz, Guidelines for conducting systematic mapping studies in software engineering: An update, Information and Software Technology 64 (2015) 1–18. URL: https://www.sciencedirect.com/science/article/pii/S0950584915000646. doi:https://doi.org/10.1016/j.infsof.2015.03.007.

[18] M. Petticrew, H. Roberts, Systematic Reviews in the Social Sciences: A Practical Guide, Blackwell Publishing, 2006. doi:10.1002/9780470754887.

[19] J. Popay, H. Roberts, A. Sowden, M. Petticrew, Guidance on the conduct of narrative synthesis in systematic reviews, ESRC Methods Programme (2006). URL: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=ed8b23836338f6fdea0cc55e161b0fc5805f9e27.

[20] S. D. Javagal, Cybersecurity for vehicles: Challenges and mitigation strategies, INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND TECHNOLOGY (IJCET) 14 (2023). URL: https://lib-index.com/index.php/IJCET/article/view/IJCET_14_03_005.

[21] S. C. Kalkan, O. K. Sahingoz, In-vehicle intrusion detection system on controller area network with machine learning models, in: 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2020, pp. 1–6. doi:10.1109/ICCCNT49239.2020.9225442.

[22] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, P. Ranganathan, Cybersecurity challenges in vehicular communications, Vehicular Communications 23 (2020) 100214. URL: https://www.sciencedirect.com/science/article/pii/S221420961930261X. doi:https://doi.org/10.1016/j.vehcom.2019.100214.

[23] P. Parandkar, S. D, P. V. Joshi, S. K. M., Intrusion detection in in-vehicle networks using neuro computing, SSRN Electronic Journal (2024). URL: https://www.ssrn.com/abstract=4917843. doi:10.2139/ssrn.4917843.

[24] M. Annabi, A. Zeroual, N. Messai, Towards zero trust security in connected vehicles: A compre-

hensive survey, Computers Security 145 (2024) 104018. URL: https://www.sciencedirect.com/science/article/pii/S0167404824003237. doi:https://doi.org/10.1016/j.cose.2024.104018.

[25] C. Gao, G. Wang, W. Shi, Z. Wang, Y. Chen, Autonomous driving security: State of the art and challenges, IEEE Internet of Things Journal 9 (2022) 7572–7595. doi:10.1109/JIOT.2021.3130054.

[26] R. Pavithra, V. K. Kaliappan, S. Rajendar, Security Algorithm for Intelligent Transport System in Cyber-Physical Systems Perceptive: Attacks, Vulnerabilities, and Countermeasures, SN Computer Science 4 (2023) 544. URL: https://link.springer.com/10.1007/s42979-023-01897-9. doi:10.1007/s42979-023-01897-9.

[27] B. Gozubuyuk, W. Bailey, D. Everson, Z. Dong, L. Cheng, M. D. Pesé, An overview of security in connected and autonomous vehicles, in: 2023 International Conference on Artificial Intelligence of Things and Systems (AIoTSys), 2023, pp. 206–213. doi:10.1109/AIoTSys58602.2023.00052.

[28] S. R. Neupane, W. Sun, Advanced data classification framework for enhancing cyber security in autonomous vehicles, Automation 6 (2025). URL: https://www.mdpi.com/2673-4052/6/1/5. doi:10.3390/automation6010005.

[29] F. Onur, S. Gönen, M. A. Barışkan, C. Kubat, M. Tunay, E. N. Yılmaz, Machine learning-based identification of cybersecurity threats affecting autonomous vehicle systems, Computers Industrial Engineering 190 (2024) 110088. URL: https://www.sciencedirect.com/science/article/pii/S0360835224002092. doi:https://doi.org/10.1016/j.cie.2024.110088.

[30] P. Sharma, H. Liu, H. Wang, S. Zhang, Securing wireless communications of connected vehicles with artificial intelligence, in: 2017 IEEE International Symposium on Technologies for Homeland Security (HST), 2017, pp. 1–7. doi:10.1109/THS.2017.7943477.

[31] L. Ming, G. Zhao, M. Huang, X. Kuang, J. Zhang, H. Cao, F. Xu, A general testing framework based on veins for securing vanet applications, in: 2018 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computing, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), 2018, pp. 2068–2073. doi:10.1109/SmartWorld.2018.00347.

[32] K. Herman Muraro Gularte, J. Alfredo Ruiz Vargas, J. Paulo Javidi da Costa, A. Santos da Silva, G. Almeida Santos, Y. Wang, C. Alfons Müller, C. Lipps, R. Timóteo de Sousa Júnior, W. de Britto Vidal Filho, P. Slusallek, H. Dieter Schotten, Safeguarding the v2x pathways: Exploring the cybersecurity landscape through systematic review, IEEE Access 12 (2024) 72871–72895. doi:10.1109/ACCESS.2024.3402946.

[33] R. S. Rathore, C. Hewage, O. Kaiwartya, J. Lloret, In-vehicle communication cyber security: Challenges and solutions, Sensors 22 (2022). URL: https://www.mdpi.com/1424-8220/22/17/6679. doi:10.3390/s22176679.

[34] T. Limbasiya, K. Z. Teng, S. Chattopadhyay, J. Zhou, A systematic survey of attack detection and prevention in connected and autonomous vehicles, Vehicular Communications 37 (2022) 100515. URL: https://www.sciencedirect.com/science/article/pii/S2214209622000626. doi:https://doi.org/10.1016/j.vehcom.2022.100515.

[35] H. I. Ali, H. Kurunathan, M. H. Eldefrawy, F. Gruian, M. Jonsson, Navigating the challenges and opportunities of securing internet of autonomous vehicles with lightweight authentication, IEEE Access 13 (2025) 24207–24222. doi:10.1109/ACCESS.2025.3537800.

[36] J. Ahmad, M. U. Zia, I. H. Naqvi, J. N. Chattha, F. A. Butt, T. Huang, W. Xiang, Machine learning and blockchain technologies for cybersecurity in connected vehicles, WIREs Data Mining and Knowledge Discovery 14 (2024) e1515. URL: https://wires.onlinelibrary.wiley.com/doi/abs/10.1002/widm.1515. doi:https://doi.org/10.1002/widm.1515. arXiv:https://wires.onlinelibrary.wiley.com/doi/pdf/10.1002/widm.1515.

[37] S. Bharati, P. Podder, M. R. H. Mondal, M. R. A. Robel, Threats and countermeasures of cyber security in direct and remote vehicle communication systems, 2020. URL: https://arxiv.org/abs/2006.08723. arXiv:2006.08723.

[38] Researcher, CYBERSECURITY IN AUTOMOTIVE NETWORKS: MITIGATING THREATS IN CAN, LIN AND AUTOMOTIVE ETHERNET SYSTEMS (2025). URL: https://zenodo.org/doi/10.5281/zenodo.14892660. doi:10.5281/ZENODO.14892660.

[39] 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. doi:10.1109/COMST.2020.2975048.

A. Appendix A

This is the start of the appendix.

A.1. Project Time Plan

Week	Task Description
1–2	Completion of thesis registration, assignment of supervisor and examiner.
3	Initial meeting with the supervisor to discuss the thesis scope and expectations.
4–6	Define research questions, scope, and objectives. Develop the methodology for the systematic literature review (SLR), including search strategy, inclusion/exclusion criteria, and quality assessment measures. Begin writing the background chapter.
6–8	Receive and incorporate feedback from the supervisor. Refine methodology and background sections.
9–16	Conduct database searches (IEEE Xplore, SpringerLink, Scopus, Google Scholar). Screen and select relevant papers based on predefined criteria. Extract and synthesize data.
17–19	Analyze findings, finalize results, and draft the discussion chapter.
20	Write and refine the conclusion and abstract. Present the thesis.
21–22	Perform final proofreading, formatting, and submit the thesis.

Table 3
Project Time Plan