International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

Cyber threats in automotive environment: Literature review and mitigation strategies

João V. P. de Souza *, Carlos C. da S. Conde Jr, Marcus V. da C. Correa, Michel M. de Oliveira, Victor M. D. Albuquerque and Hualter O. Barbosa

Instituto de Pesquisas Eldorado – IPE – Avenida Mário Ypiranga, 315 - Adrianópolis, Manaus - AM, ZIP Code: 69057-070, Brasil.

International Journal of Science and Research Archive, 2026, 19(01), 263-270

Publication history: Received on 16 February 2026; revised on 30 March 2026; accepted on 02 April 2026

Article DOI: https://doi.org/10.30574/ijsra.2026.19.1.0606

Abstract

The increasing connectivity and autonomy of vehicles exposes them to a growing scenario of cyber security threats. This study analyzes recent cyberattacks and mitigation strategies for connected and autonomous vehicles (CAVs). Through a systematic analysis of papers published between 2020 and 2025, we examine threats to vehicular networks and V2X interfaces, including DoS, CAN bus injection, routing attacks in VANETs, and automotive Ethernet vulnerabilities. The results show strong progress in statistical detection, machine learning intrusion detection, physical layer authentication, secure routing, and Ethernet hardening. However, the emergence of sophisticated threats, including identity spoofing and data contamination, requires the development of more robust and adaptable security architectures. Soon, there will be a need for adaptive, intelligent, and context-aware security frameworks capable of supporting the evolving threat of landscape in modern vehicular environments.

Keywords: CAV; Vehicle; Cyber-security; Mitigation; Cyber-attacks; V2X

1. Introduction

The automotive sector is undergoing a massive transformation with connected and autonomous vehicles (CAVs) evolving to deliver better transportation efficiency, new mobility service options and enhanced safety [1]. While the advantages of CAVs are enormous, they bring new challenges in how they accelerate communication and automation. The systems that provide advanced functionalities also expose vehicles to broad cyber security threats. Different from traditional vehicles, CAVs are susceptible to remote attacks that can compromise not only user privacy but also vehicle safety and functionality [2].

Recent statistics highlight the severity of the situation. Only in 2023, there were 295 publicly reported automotive cybersecurity incidents, representing 250% when compared to 2022. Notably, 95% of these attacks were executed remotely, and 85% were long-range attacks, reflecting the growing reach and sophistication of cyber-attacks against connected vehicles. [3].

With the scope of concerns identified, it is crucial that researchers and industry stakeholders address cybersecurity vulnerabilities in CAVs sooner rather than later. A few existing defensive efforts are far from everything that needs to be done, covering a range of approaches that tend to bridge separate parts of the threat surface.

This paper aims to provide a comprehensive review of the current cybersecurity challenges facing CAVs, highlighting threats targeting vehicle network availability (CAN, V2X and Ethernet) and evaluating existing mitigation techniques

* Corresponding author: João V. P. de Souza

for these attacks. This research combines knowledge from academic and industrial sources to get more resilient and secure vehicle systems.

2. Methodology

This section describes the methodological process used to identify, select, and analyze relevant studies on cyber-attacks and mitigation strategies in connected, autonomous vehicles (CAVs) and vehicle network availability (CAN, V2X and Ethernet). The procedure follows a reproducible flow consisting of selecting scientific databases and defining the search strategy, applying inclusion and exclusion criteria, and consolidating the final set of studies.

2.1. Selection of Articles and Papers

A systematic search was conducted across four major scientific databases: IEEE Xplore, ACM Digital Library, SpringerLink, and MDPI. These repositories were selected due to their strong relevance to cybersecurity, vehicular networks, cyber-physical systems, and intrusion detection research in automotive environments.

The search covered publications from January 2020 to August 2025, aiming to capture recent advances in DoS detection, CAN-bus security, VANET routing protection, and V2I authentication mechanisms—topics aligned with the attack categories investigated in this review.

2.2. Inclusion and Exclusion Criteria

To ensure scientific rigor and thematic consistency, the selection of studies followed explicit eligibility conditions. Only works that addressed cyber-attacks targeting vehicles, including DoS, spoofing, message injection, routing manipulation, CAN-bus anomalies, or V2I/V2X threats, were considered. In addition to presenting a relevant attack scenario, studies needed to propose or evaluate mitigation, detection, authentication, monitoring, or risk-assessment mechanisms supported by reproducible methodologies such as algorithms, simulations, datasets, or experimental validation. Eligible publications were required to be peer-reviewed journal articles, conference papers, or book chapters, written in English and published between 2020 and 2025.

Studies were excluded when they focused on unrelated domains such as general IoT, drones, aviation, or maritime systems. Works that mentioned threats without proposing mitigation or detection strategies were also removed, as well as those lacking methodological transparency, including opinion pieces, editorials, whitepapers, or incomplete materials without full-text availability. Non-peer-reviewed documents and duplicated records across databases were likewise excluded. These conditions ensured that only relevant, technically grounded, and methodologically robust studies composed the final corpus, in accordance with reviewer recommendations.

2.3. Selection Results

The search process returned a broad initial set of studies across the four selected databases. The DoS-focused query in IEEE Xplore resulted in 41 articles, while the routing attack search in the VANETs domain produced 227 studies published between 2020 and 2025. Additional works related to CAN-bus security and V2I communication were identified across IEEE, ACM, MDPI, and Springer, forming a diverse set of potentially relevant publications. After removing duplicated records, the remaining studies were screened by title and abstract to eliminate works unrelated to automotive cybersecurity or lacking any form of mitigation strategy. The articles that passed this stage underwent a full-text review, during which each study was evaluated based on its relevance to the four categories examined in this review, the clarity of its attack model, the technical depth of its proposed solution, the reproducibility of its methodology, and its overall alignment with the objectives of this research.

Following this filtering process, a refined set of representative studies was selected. These works encompassed DoS detection and risk quantification methods, machine-learning-based CAN-bus anomaly detection, intrusion detection in heavy-duty vehicular networks, V2I authentication and anomaly detection mechanisms, and routing attack mitigation strategies in VANET environments. The final corpus forms the analytical foundation for Section 3, enabling a structured synthesis of mitigation approaches and the identification of strengths, limitations, and emerging trends in vehicular cybersecurity.

3. Findings

This section presents a comparative and critical examination of the studies analyzed, highlighting how each contributes to advancing cybersecurity in vehicles environments. By evaluating their methodologies and results, we validate the effectiveness of the authors' approaches and uncover key strengths, limitations, and opportunities.

3.1. DoS Attacks

A DoS attack (Denial of Service Attack) is defined in the literature as periodically disrupting, delaying, or discarding packets to reduce network performance. It consists of flooding (like interfering occupying the channel by third parties) and exhausting network resources, such as bandwidth and computing capacity. In the study Change Point Models for Real-Time Cyber Attack Detection in Connected Vehicle Environment [4], DoS attacks dramatically increase the number of messages to roadside equipment (RSE or roadside unit (RSU)) or on-board equipment (OBE or on-board unit (OBU)) until they are unable to process them and overall communication delays continue to increase or become unavailable.

The study [4] demonstrates that Expectation Maximization (EM) and Cumulative Summation (CUSUM) algorithms achieve high detection accuracy (≥98%), with CUSUM reaching 100%, validating their potential for real-time implementation. The disadvantage, however, lies in computational demand: EM processing time increases with vehicle density, exceeding the safety limit of 100 ms for high-load conditions. Meanwhile, the sequential nature of CUSUM ensures faster performance with less computational overhead, favoring scalability and real-time operation.

On the other hand, a more recent study [5] emphasizes the variability and propagation of risks during DoS attacks, revealing that as the intensity of the attack increases, the uncertainty (standard deviation) in risk estimates also increases. Although it lacks real-time detection capabilities, it provides a robust analytical basis for designing adaptive, risk-aware defense mechanisms. The inclusion of an ASIL-like framework positions this approach within functional safety standards, enabling the integration of cybersecurity and safety engineering, a crucial step toward regulatory and industrial adoption.

Together, both studies represent complementary dimensions of vehicle cybersecurity. The change point models (EM and CUSUM) enable rapid and accurate detection of attacks, which is essential for short-term mitigation and continuity of safety functions in V2I systems. In turn, the study by [5] addresses the methodology for quantifying cyber risks, supporting strategic resilience and adaptive security architectures, contributing to informed design and compliance in accordance with the results obtained from risk qualification.

3.2. CAN bus vulnerabilities

The study *Can-sleuth: Sleuthing out the capabilities, limitations, and performance impacts of automotive intrusion detection datasets [6]* emphasizes the fragility of the CAN protocol, which has no native authentication, making it susceptible to injection attacks and message (Spoofing). To mitigate these risks, the use of supervised machine learning is proposed to identify anomalous patterns in transmissions. The model achieves high accuracy in distinguishing legitimate traffic from malicious messages, providing a non-intrusive detection layer without the need to change the existing protocol.

The work [7] expands this perspective by proposing an intelligent intrusion detection system (IIDS) for cyber-physical systems of autonomous vehicles (AV-CPS). Using transfer learning and pre-trained convolutional neural networks (such as GoogLeNet and ResNet-50), the system achieves a performance of 99.47% on the F1-score, demonstrating the effectiveness of the approach in detecting attacks launched via the CAN network. This technique stands out for allowing rapid adaptation to different vehicle and sensor contexts, in addition to reducing the need for large volumes of labeled data, a recurring limitation in deep learning-based solutions.

In *[8]*, the authors explore the challenges of applying detection methods in heavy-duty vehicle fleets, where distributed communication and data volume increase the risk of DoS attacks and packet spoofing. The article presents a hybrid model of traffic monitoring and event correlation, with an emphasis on real-time analysis to minimize response delays. The solution proposes a balance between accuracy and computational cost, highlighting the importance of scalable architectures for complex vehicular environments.

3.3. Infrastructure Attacks

When we talk about Infrastructure Attacks, Vehicle-to-Infrastructure (V2I) communications represent a significant attack surface, as they involve Road Side Units (RSUs), external sensors, smart traffic lights, and backend servers. Recent

studies highlight critical vulnerabilities in these elements and propose mitigation mechanisms based on multi-source authentication, physical layer security, and robust control.

The study van der Ploeg et al. [9] analyzes scenarios in which a compromised UAS injects false data, such as incorrect position or speed of pedestrians and cyclists, affecting automated vehicle decision algorithms. The approach proposes the detection of inconsistencies between internal and external data, allowing compromised measurements to be ignored during the sensor fusion process, which increases resilience against false data injection.

Continuing, Amin et al. [10] introduce the *Hybrid PLS-ML Authentication Scheme* for V2I Communication Networks model, which combines *Physical Layer Security (PLS)* and machine learning to validate transmissions in V2I networks. The system uses (*Time of Arrival,* ToA) metrics and channel fingerprints to authenticate entities, mitigating spoofing and impersonation attacks.

Complementarily, De Vincenzi et al. [11] present a multi-factor authentication approach that integrates cryptographic and visual channels. The method uses vehicle headlights to emit coded light patterns, which are recognized and validated by RSUs using deep neural networks. The study demonstrates high accuracy and robustness under different environmental conditions.

In turn, Ghosh et al [12] propose an attack detection and isolation scheme based on noise generators and Lyapunov functions, capable of identifying disturbances in signals coming from the infrastructure. The technique ensures system stability and robustness even under dynamic traffic and environmental variations.

Collectively, these studies reinforce a trend toward hybrid and multi-layered structures combining physical authentication, machine learning, and stable control mechanisms. These solutions extend the defense capabilities of V2X systems and complement the detection and response approaches discussed in previous sections.

3.4. Routing Attacks

In the context of Vehicular Ad Hoc Networks (VANETs) and V2X (Vehicle-to-Everything) communication, vehicles exchange distributed information such as position, speed, traffic alerts, and road conditions. For this communication to work, routing protocols decide how messages are transmitted from one node (vehicle) to another.

A routing attack occurs when a malicious agent manipulates the routing process in order to redirect messages to the wrong path, disrupt communication, eavesdrop or alter data in transit, and even create false traffic scenarios.

According to [13], routing in vehicular ad hoc networks (VANETs) involves several security challenges due to their dynamic and decentralized nature. The authors highlight that attacks such as denial of service (DoS) can overload the network with excessive requests, making communication between legitimate nodes difficult. Moreover, black-hole and gray-hole attacks exploit trust between nodes by advertising false routes and later dropping packets, which degrades performance and compromises data integrity.

To address the high-mobility challenges of VANETs, [14] propose the SROR (Secure and Reliable Opportunistic Routing) algorithm, which incorporates three key metrics to enhance packet forwarding and mitigate malicious behavior. First, the relative speed between vehicles is considered to ensure spatial stability and reduce transmission delay. Next, the connectivity probability is evaluated to ensure robust links, improving packet delivery with lower latency. Finally, the packet forwarding ratio is used to prevent malicious nodes (such as those performing black-hole or gray-hole attacks) from being selected as forwarders. The relay node selection is modeled as a Markov Decision Process (MDP) and solved using Deep Reinforcement Learning, whose learned policies optimize forwarding decisions against malicious vehicles.

[13] also proposes an integrated scheme for secure authentication and attack detection in VANETs that combine swarm optimization techniques with deep neural networks. Their approach merges a Cauchy mutation operator applied to Glowworm Swarm Optimization (GSO) to optimize the search for anomalous forwarding behavior patterns, with a Multilayer Maxout Network classifier responsible for identifying attack types (e.g., black-hole/gray-hole and other packet dropping/manipulation forms).

In practice, mitigation operates on two fronts: (1) **prevention** — a robust authentication module prevents unauthorized nodes (including Sybil identities) from joining the network; and (2) **detection and reaction** — the system quickly detects nodes that show suspicious behavior (e.g., low forwarding rate, inconsistent route advertisements) and triggers isolation or route reconfiguration policies to bypass malicious nodes. In VANET simulation environments, the authors

report improvements in detection rate, reduction of false positives, and enhancement of network metrics (e.g., PDR and latency), demonstrating that the combination of GSO + Cauchy mutation + Multilayer Maxout is effective in detecting and mitigating dynamic routing attacks. They also discuss common limitations, such as the classifier's training dependence and the need for validation in real-world scenarios.

3.5. Automotive Ethernet Threats

Automotive Ethernet has become a backbone for high bandwidth in-vehicle communication, and its convergence with conventional Ethernet stacks brings into the vehicle classic network threats such as spoofing, replay, man-in-the-middle (MITM), eavesdropping, and message injection. Accordingly, [11] argues that current Automotive Ethernet deployments often adopt security mechanisms in a fragmented way, leaving gaps in authentication, integrity, and confidentiality across safety critical segments. [15] similarly observes that many automotive cybersecurity frameworks still treat Ethernet largely as a performance and architecture enabler, rather than as a security sensitive substrate that must be protected end-to-end inside the vehicle.

Spoofing is identified as a central vulnerability in Automotive Ethernet because the basic MAC and IP layers do not verify the identity of the transmitting ECU once an attacker has network access. [11] highlights that, without strong source authentication and strict address management, a malicious node can impersonate legitimate ECUs or gateways and inject traffic that appears valid to downstream components. [16] propose a spoofing attack detection method for 10BASE-T1S that estimates the transmitting device from physical layer characteristics and collision avoidance behavior, showing that PHY/MAC level fingerprints can effectively distinguish genuine senders from impostors in Automotive Ethernet segments. [15] further stress that such low-level identification must be complemented by robust ECU identity and key management, so that each node on the Automotive Ethernet backbone can be strongly authenticated before participating in critical communication.

Replay attacks in Automotive Ethernet exploit the absence of systematic freshness guarantees, such as timestamps, nonce, or sequence numbers, in many higher layer protocols transported over Automotive Ethernet. [11] demonstrate that captured Ethernet frames can be re-injected at later times to trigger time inconsistent yet syntactically correct actions, which is particularly dangerous for controlling flows with predictable timing and content. [17] argue that effective replay protection in-vehicle networks require binding freshness indicators to cryptographic authentication, so that old messages cannot be reused without detection even if an attacker can observe and store traffic. [18] show through automated attack tree analysis that replay must be modeled explicitly as a distinct threat in the design of Automotive Ethernet based architectures, enabling systematic derivation and verification of freshness checks, temporal plausibility controls, and intrusion detection rules.

MITM attacks in Automotive Ethernet arise when an adversary is able to interpose a compromised device or software component along the communication path between ECUs, thereby gaining the capability to intercept, modify, or drop Ethernet frames. [11] note that the use of switched backbones and gateways in Automotive Ethernet makes such path-based attacks feasible whenever link layer protection and authenticated higher layer protocols are not consistently deployed across the network. [19] show that intrusion detection models derived from decision trees can capture anomalous patterns associated with MITM and manipulation of flows in Automotive Ethernet traffic, providing interpretable rules suitable for embedded deployment. [15] additionally recommend enforcing strict network segmentation and access policies, so that routing in the Ethernet backbone is constrained, and opportunities for undetected interception are minimized.

Message injection in Automotive Ethernet refers to the transmission of syntactically valid but malicious frames that inject false data, perturb control logic, or disturb communication schedules. [11] classify injection as one of the most critical threats for Automotive Ethernet because both time sensitive and best effort traffic coexist on the same backbone, making it possible for crafted packets to influence safety relevant decisions or degrade real time performance. [19] evaluate decision tree-based rule derivation for IDS in Automotive Ethernet and show that compact rule sets can accurately distinguish injected flows from legitimate traffic while meeting resource constraints of automotive ECUs. [15] emphasize that these detection mechanisms should be combined with finely tuned firewalls and policy-based filtering at Automotive Ethernet switches and gateways, enforcing predefined communication matrices for critical ECUs.

Eavesdropping on Automotive Ethernet becomes possible whenever Automotive Ethernet links, multi-drop segments, or switch ports lack encryption and strict access control, enabling passive adversaries to capture in-vehicle Ethernet traffic. [17] shows that unprotected in-vehicle communications can leak telemetry, proprietary protocols, and even security relevant information, which adversaries may later reuse in more targeted attacks. [11] recommend deploying link layer encryption and integrity protection on sensitive Automotive Ethernet paths, alongside VLAN based

segmentation and port level access control to restrict which devices can observe traffic flows. [15] also highlight the need to harden diagnostic and update channels carried over Automotive Ethernet, since unencrypted maintenance traffic can expose credentials, firmware images, or configuration data that undermine the overall security posture of the Ethernet backbone.

Across all of these attack classes, intrusion detection and continuous monitoring emerge as central components of Automotive Ethernet security. [19] show that interpretable IDS rules derived from Automotive Ethernet specific decision tree models can be embedded into ECUs to provide real-time anomaly detection with manageable computational overhead. [15] place these mechanisms within broader cybersecurity architectures that integrate secure development processes, standardized testing, and lifecycle monitoring of Automotive Ethernet networks, framing IDS as one pillar in a coordinated, multilayer defense strategy.

4. Discussion

In this topic, we will discuss the results of the mitigations, perform a comparative analysis, and present a possible solution by linking the studies addressing the challenges encountered. Emphasizes not only how these solutions perform in detecting or mitigating the attacks but also how they collectively shape a more resilient and adaptative framework for vehicular cybersecurity.

A robust security posture for V2X systems requires the integration of both types of solutions. The conclusions of the studies [4] and [5] collectively advocate for low-latency detection defense mechanisms and dynamic risk-based responses.

The studies cited on DoS attacks on vehicles also report solutions that address different phases of attacks: the study [4] provides the solution for early warning (detection), while that by [5] provides the solution for impact assessment and adaptive response (quantification).

A promising direction would involve integrating both approaches, deploying real-time CUSUM-based detectors within a risk-aware adaptive framework guided by quantitative security assessments. This strategy could result in multi-layered defense systems or defense in depth, which would use multiple security systems and controls to protect the vehicle from various types of attacks beyond DoS. They would be able to detect, assess, and adapt to DoS and other evolving cyber threats in connected vehicle environments.

Finally, the study of Security Strategy for Autonomous Vehicle Cyber-Physical Systems argues that, in addition to detecting attacks, it is necessary to strengthen the vehicle ecosystem with predictive and proactive mechanisms. The integration of cloud computing and artificial intelligence is identified as essential for coordinating responses between vehicles and urban infrastructure. Detection based on transferred learning reduces false positives and enables an adaptive response to emerging attacks, including spoofing, data injection, and sensor manipulation.

Together, the studies about integration of cloud computing and artificial intelligence, demonstrate that vulnerabilities in vehicular networks require solutions that combine machine learning, distributed detection, and layered architecture. Strategies such as the use of *deep learning* models trained in communication data, network segmentation, and cloud integration are recurring mitigation mechanisms. Still, the authors acknowledge challenges such as computational cost, model updating, and scalability, crucial factors for the adoption of these solutions in autonomous transportation and 5G connectivity environments.

Taken together, these studies indicate that Automotive Ethernet reproduces the classic vulnerabilities of conventional Ethernet, spoofing, replay, MITM, eavesdropping, and message injection, but in an environment where real time and safety constraints significantly amplify the potential impact of successful attacks. [11], [15], and [17] all converge on the view that the fundamental security primitives required to protect Automotive Ethernet are well understood, yet their systematic, resource aware integration into in-vehicle architectures remains incomplete, particularly regarding endpoint identity, freshness, and protection of backbone links.

The most promising direction emerging from recent work is the adoption of multilayered, Automotive Ethernet aware defenses that combine strong ECU identity and key management, authenticated and encrypted communication channels, rigorous segmentation of the Ethernet backbone, and IDS specifically tuned to Automotive Ethernet traffic characteristics. [19] shows that both rule-based and deep learning-based IDS can meet automotive performance, and interpretability needs while providing effective coverage against spoofing, replay, MITM, and injection attacks in Automotive Ethernet. [18] and [15] further argue that attack tree analysis, security frameworks, and architectural

models should embed these protections from the earliest design stages, moving Automotive Ethernet from ad-hoc hardening toward a genuine security by design paradigm.

5. Conclusion

Although significant progress has been made in identifying and mitigating cybersecurity threats in connected and autonomous vehicles, there remain critical gaps between proposed theoretical solutions and their practical applicability in real-world, dynamic environments.

The studies analyzed demonstrate significant progress in detection of DoS attacks, machine learning and deep learning approaches for anomaly detection in CAN-bus, hybrid authentication schemes for V2I systems, secure routing solutions in VANETs, and layered defenses for automotive Ethernet. Collectively, these works reveal a trend toward multisource, multilayer, and context-sensitive protection strategies capable of handling the growing complexity of vehicular environments. Despite advances, several limitations remain. Many solutions still rely on limited datasets, lack comprehensive real-world validation, or require computational resources that exceed the capabilities of current automotive ECUs.

Future work should focus on the practical validation of the strategies discussed, emphasizing resilience in unpredictable operational scenarios, interoperability among solutions (e.g., CAN detectors, V2I modules, Automotive Ethernet protections), and real-time implementation feasibility, ultimately contributing to the development of safer and more reliable automotive ecosystems. Further research on Software-Defined Vehicles (SDVs) is required because software-centric vehicle architectures increase the importance of cybersecurity to protect vehicle functions, user data, and system integrity against increasingly sophisticated digital threats.

Compliance with ethical standards

Acknowledgments

This article is of a Research, Development and Innovation project carried out by the Instituto de Pesquisas Eldorado with funds provided for in Informatics Law No. 8.387/1991, in accordance with art. 21 of Decree No. 10.521/2020.

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Sun X, Yu FR, Zhang P. A survey on cyber-security of connected and autonomous vehicles (CAVs). IEEE Trans Intell Transp Syst. 2021;23:6240-6259.

[2] Gupta S, Maple C, Passerone R. An investigation of cyber-attacks and security mechanisms for connected and autonomous vehicles. IEEE Access. 2023;11:90641-90669.

[3] Upstream Security. 2024 global automotive cybersecurity report [Internet]. 2024 [cited 2025 Apr]. Available from: https://info.upstream.auto/hubfs/Security_Report/Security_Report_2024/Upstream_2024_Global_Automotive_Cybersecurity_Report.pdf

[4] Comert G, Rahman M, Islam M, Chowdhury M. Change point models for real-time cyber attack detection in connected vehicle environment. IEEE Trans Intell Transp Syst. 2022;23(8):12328-12342.

[5] Pethő Z, Kazár TM, Szalay Z, Török Á. Quantifying cyber risks: the impact of DoS attacks on vehicle safety in V2X networks. IEEE Trans Intell Transp Syst. 2024;25:18591-18600.

[6] Kidmose B, Kidmose A, Meng W. CAN-sleuth: sleuthing out the capabilities, limitations, and performance impacts of automotive intrusion detection datasets. Int J Inf Secur. 2025;24(5):193.

[7] Alsulami AA, Abu Al-Haija Q, Alturki B, Alqahtani A, Alsini R. Security strategy for autonomous vehicle cyber-physical systems using transfer learning. J Cloud Comput. 2023;12:181.

[8] Potvin MJ, Leblanc SP. Detecting malicious anomalies in heavy-duty vehicular networks using long short-term memory models. Sensors (Basel). 2025;25(14):4430.

[9] van der Ploeg C, Smit R, Siagkris-Lekkos A, Benders F, Silvas E. Anomaly detection from cyber threats via infrastructure to automated vehicle. In: Proceedings of the 2021 European Control Conference (ECC); 2021 Jun 29-Jul 2; Delft, Netherlands. IEEE; 2021. p. 1788-1794.

[10] Amin H, Kaldari J, Mohamed N, Aman W, Al-Kuwari S. Hybrid PLS-ML authentication scheme for V2I communication networks. In: Proceedings of the 2023 International Symposium on Networks, Computers and Communications (ISNCC); 2023; Doha, Qatar. p. 1-6.

[11] De Vincenzi M, Sun S, Zhang CBC, Garcia M, Ding S, Bodei C, Matteucci I, Sarma SE, Suo D. Vehicular communication security: multi-channel and multi-factor authentication. IEEE Trans Veh Technol. 2026;75(2):1779-1792.

[12] Ghosh S, Saha N, Roy T. A cyberattack detection-isolation algorithm for CAV under changing driving environment. IEEE Trans Intell Transp Syst. 2024;25(12):19646-19657.

[13] Shankar J, Nagaraja SR. Secure authentication and attack detection in VANET using Cauchy mutation operator-Glowworm swarm optimization with multilayer maxout network. In: Proceedings of the 3rd International Conference on Data Science and Information System (ICDSIS); 2025. p. 1-6.

[14] Xu H, Wang Y. SROR: a secure and reliable opportunistic routing for VANETs. Vehicles. 2024;6(4):1730-1751.

[15] Kifor CV, Popescu A. Automotive cybersecurity: a survey on frameworks, standards, and testing and monitoring technologies. Sensors (Basel). 2024;24(18):6139.

[16] Iehira K, Inoue H. Spoofing attack detection method by estimating transmitting device on 10BASE-T1S. In: Proceedings of the 2024 IEEE 29th Asia Pacific Conference on Communications (APCC); 2024 Nov 5-7; Bali, Indonesia. IEEE; 2024. p. 511-514.

[17] Khatri N, Shrestha R, Nam SY. Security issues with in-vehicle networks, and enhanced countermeasures based on blockchain. Electronics. 2021;10(8):893.

[18] Chlup S, Christl K, Schmittner C, Shaaban AM, Schauer S, Latzenhofer M. THREATGET: towards automated attack tree analysis for automotive cybersecurity. Information. 2023;14(1):14.

[19] Gail F, Rieke R, Fenzl F, Krauß C. Evaluation of decision tree-based rule derivation for intrusion detection in automotive Ethernet. In: Proceedings of the IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom); 2023; Exeter, United Kingdom. p. 1392-1399.