TuJNaS

Review Article

Thamar University Journal of Natural & Applied Sciences 11(1) (2026) 15– 20

DOI: https://doi.org/10.59167/sbta1126

A Systematic Review and Meta-analysis Survey of IDS/IPS Techniques for CAN and Vehicular Networks

Younis Abdo Mohammed Nasser Al Shojaa[1]*, Khaled Al Soufy[2]

[1]Information Technology Department, Faculty of Engineering and Information Technology, Al-Qalam University, Ibb, Yemen.

[2]Electrical Engineering Department, Faculty of Engineering, Ibb University, Ibb, Yemen.

***Corresponding Author:** Younis A. M. N. Al Shojaa, Information Technology Department, Faculty of Engineering and Information Technology, Al-Qalam University, Ibb, Yemen. Email younis.alshogaa@quni.edu.ye

Received: 18 November 2025. Revised: 16 April 2026. Accepted: 18 April 2026. Published: 29 June 2026.

Abstract

As cyberattacks grow increasingly sophisticated and frequent, the need for advanced mechanisms to protect modern network systems has become more pressing, especially in sensitive environments such as automotive networks. This research presents a systematic review, complemented by a sensitivity-based quantitative trend analysis, of recent efforts to employ Machine Learning (ML) and Deep Learning (DL) techniques for intrusion detection and prevention within automotive networks, with a particular focus on the Controller Area Network (CAN) bus. The research employs a clear and reproducible methodology for identifying, screening, and evaluating relevant studies, guided by the PRISMA framework. It also presents a structured classification that groups current approaches according to model type, data sources, and evaluation strategies. Furthermore, the review provides a comparative analysis highlighting the key strengths, weaknesses, and experimental performance of various IDS/IPS techniques in automotive environments. In addition, the study includes a sensitivity-based quantitative summary of reported accuracy patterns in the literature, offering an exploratory and sensitivity-aware view of performance trends rather than a formal pooled estimate. The analysis encompassed 56 studies published between 2018 and 2025, covering diverse datasets, methodological designs, and multiple detection objectives. The findings reveal ongoing challenges, including real-time limitations, limited computational resources, and dataset variability, while also pointing to promising research avenues that could contribute to the development of more efficient AI-based intrusion detection and prevention systems for connected and autonomous vehicles.

Index Terms—CAN Bus, Vehicular Networks, In- Vehicle Communication, Intrusion Detection System, Sensitivity Analysis, Machine Learning, Deep Learning, Automotive Cybersecurity

1. Introduction

With the rapid development of modern technologies and the ever-increasing reliance of systems on networking across various sectors of life, industry, and transportation, cybersecurity has become more critical than ever. Maintaining data confidentiality, integrity, and availability is no longer a secondary option but a fundamental necessity, especially given the rise in cyberattacks and their significantly evolving methods. In this context, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) represent the first line of defense, monitoring network traffic and detecting any suspicious behavior before it develops into an actual threat. However, traditional signature-based methods often struggle to address new and sophisticated attacks, particularly in sensitive environments that demand immediate response, limited resources, and high reliability. Artificial intelligence and ML techniques have gained increasing attention due to their ability to enhance the performance of detection systems and provide higher levels of generalization and flexibility in addressing unknown threats [1-5].

This research employs a hybrid structure that combines systematic review methodology with a sensitivity-based quantitative trend analysis. The established steps of systematic reviews were followed, including comprehensive database searches, screening processes, quality assessment, and study selection within the PRISMA framework. Simultaneously, the research incorporates a broader analytical perspective, consistent with the nature of survey studies, allowing for comparison of current trends and review of advanced methods and techniques in this field.

In addition to qualitative analysis, the study includes a sensitivity-based quantitative synthesis intended to summarize reported accuracy patterns across several IDS/IPS studies under explicit simplifying assumptions. This component is not intended to provide a formal pooled effect estimate; rather, it offers an exploratory view of performance trends across the reviewed literature. This dual approach provides both analytical depth and a structured quantitative perspective, contributing to a more comprehensive understanding of detection and prevention mechanisms within vehicle networks, particularly those based on the CAN

bus.

1.1 Scope

This research focuses on intrusion detection and prevention mechanisms within vehicle communication environments, with particular attention to the control bus known as CAN. Accordingly, the study is limited to data traffic within vehicles and their associated networks, excluding enterprise or public networks.

In this context, the research reviews the most recent developments in employing artificial intelligence techniques to detect malicious activity in vehicle systems. It also addresses ML and DL methods used to improve detection speed and accuracy and enhance system resilience, while acknowledging the limitations identified in previous studies. Furthermore, the research discusses the key challenges facing the development of intelligent detection and prevention solutions in resource- constrained vehicle environments and highlights research trends that warrant further attention in the future [1, 4-7].

1.2 Contributions

This review offers several contributions that distinguish it from previous studies in the field. First, it employs a clear and reproducible screening methodology applied to 56 studies published between 2018 and 2025, enabling researchers to verify and build upon the findings in the future. Second, it presents an improved classification for organizing ML and DL techniques according to network type in vehicles and their application areas, thus helping to organize a fragmented research field. Third, the review goes beyond traditional descriptive comparisons by linking methodological strengths and weaknesses to practical constraints, such as real-time requirements, memory limitations, resilience to repeated attacks, and feasibility in resource-constrained systems. Fourth, it provides a comprehensive analytical framework that connects datasets, evaluation metrics, and factors related to scientific publication, offering a practical model for comparing different IDS/IPS techniques. Finally, the review highlights promising research trends focused on developing lighter, faster, and more standardized solutions to support the next generation of intelligent detection and prevention systems in vehicle environments.

2. Methodology

This study employs a hybrid methodology that aligns with the principles of systematic reviews and survey analyses, complemented by a sensitivity-based quantitative trend analysis. It followed a structured systematic literature review (SLR), which included identifying studies, screening titles and abstracts, assessing eligibility, and ultimately selecting the final studies based on the PRISMA framework. Simultaneously, the study incorporated a subject-based survey classification and comparative analysis to identify technical trends and methodological categories for intrusion detection systems in CAN and vehicular networks. A sensitivity-based quantitative analysis was conducted to summarize reported accuracy trends across the included studies under transparent simplifying assumptions.

This section provides a detailed description of each methodological step in a transparent and reproducible manner, enabling future researchers to replicate or expand the study.

2.1 Information Sources and Search Strategy

This review adopted a systematic search methodology inspired by PRISMA principles, documenting the search and screening steps, as well as the acceptance and exclusion criteria, to ensure transparency and replicability. The search process relied on specialized and widely used databases in the fields of computer engineering and cybersecurity, including the IEEE Xplore platform, which includes relevant IEEE journals and conferences (such as IEEE Access, IV Conferences, VTC, and GLOBECOM), and the ACM Digital Library, which focuses on security and networking (such as the ACM AsiaCCS conference).

The study also utilized Elsevier's ScienceDirect database, which includes journals such as *Vehicular Communications*, *Internet of Things*, and *Future Generation Computer Systems*, along with open-access platforms like *MDPI (Sensors)* and *Hindawi (Security and Communication Networks)*, and the *arXiv* repository of primary research in artificial intelligence and cybersecurity.

The logical query syntax was customized for each database using keywords reflecting the scope of the study, such as:

"intrusion detection" / IDS / IPS AND (CAN OR "in-vehicle" OR automotive OR "controller area network") AND ("machine learning" OR "deep learning")

In addition, subtypes of attacks or environments (such as DoS, spoofing, and anomaly detection) were included. The search period was limited to 2018–2025, prioritizing peer-reviewed research in cybersecurity and intelligent vehicle systems. A citation tracking mechanism (reviewing the references of listed studies and the studies that cited them) was used to ensure that no work was missed in automated searches.

The screening process was initially based on titles and abstracts, followed by full-text assessment according to predefined criteria. These procedures help ensure the study can be replicated and its findings updated in line with PRISMA 2020 recommendations [6-8].

2.2 Eligibility Criteria

2.2.1 Inclusion

The study included peer-reviewed research or authoritative manuscripts published between 2018 and 2025 related to network traffic analysis in the field of cybersecurity, which relies on artificial intelligence (ML or DL) techniques for intrusion detection and/or intrusion prevention (IDS/IPS) within computer networks, vehicles, or industrial systems. For acceptance, studies had to provide a quantitative assessment such as accuracy, precision, recall, F1 value, AUC, or other similar metrics, in addition to a description of the data used, workloads, or comparison and evaluation environments. The study areas were particularly focused on in-vehicle networks (CAN/IoV) and wireless industrial sensor networks (WSNs), given their prevalence in recent research and their reliance on common standards and designs.

2.2.2 Exclusion

Editorial reports, short messages, research commentaries, and theoretical or conceptual studies lacking empirical evaluation were excluded. Research outside the scope of networking or cybersecurity, duplicates or replaced versions, and studies containing inconsistent information that prevents reliable analysis or replication of results were also excluded. Additionally, work with insufficient evaluation details that clearly precluded re- experiments or comparisons was not prioritized.

Rationale: Research on intrusion detection systems in vehicle control systems (CAN/IoV IDS) focuses on standardized metrics and comparable evaluation environments. Similarly, studies on industrial sensor networks (WSNs) rely on standardized performance indicators in ML and DL applications. Therefore, the inclusion criteria require the submission of quantitative results and clear, reliable evaluation environments to ensure reproducibility and reusability. To preserve domain specificity, studies based on CAN-native and vehicular datasets were treated as the core evidence base of this review, whereas general benchmark datasets were retained only for contextual comparison and were interpreted separately where necessary.

2.3 Screening Workflow

Figure 1 presents the finalized PRISMA-based screening workflow used in this review.

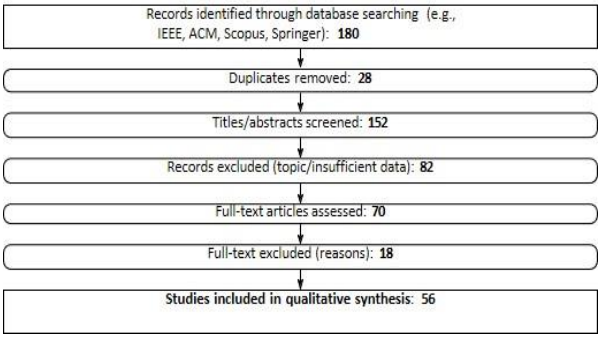

Figure 1: Final PRISMA-based screening workflow.

2.4 Data Extraction & Quality Appraisal

For each study, a set of elements was extracted, including: the datasets used, types of attacks, model family, adopted characteristics, training system, and key metrics such as accuracy, precision, recall, F1 value, and AUC, in addition to execution or response time, and computation and memory requirements. The risks of bias were also discussed from multiple perspectives, including the potential for data leakage, addressing class imbalances, the transparency of model parameter

adjustments, and the generalizability of the results across different environments. Some cited studies were authored by the present research group; however, they were retained solely because they satisfied the predefined inclusion criteria and contributed directly to the comparative scope of the review.

3. Taxonomy of AI Techniques

As seen, Figure 2 provides a multiaxis taxonomy.

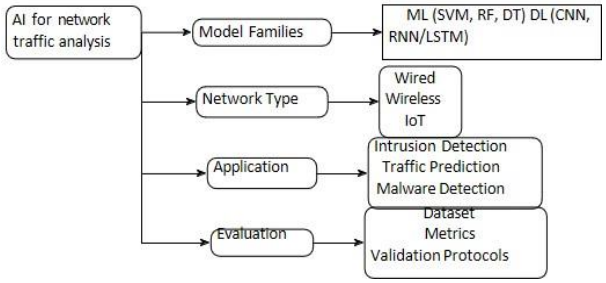

Figure 2: Mind-map taxonomy for AI in network traffic analysis.

4. Comparative Analysis

In this section, we present a concise comparative discussion of representative studies that have addressed ML, DL, and hybrid approaches for intrusion detection and prevention in CAN and vehicular network environments. For clarity and to maintain the flow of the main text, the detailed comparative tables are provided in the APPENDICES. Appendix A summarizes representative ML studies. Appendix B summarizes representative DL studies. Appendix C presents combined, hybrid, benchmarking, and overview studies.

Some representative studies have been selected to illustrate the current state of IDS/IPS research in CAN and vehicular network environments. These studies were chosen according to the predefined inclusion criteria and their relevance to the objectives of this review. Recent review studies have emphasized the rapid evolution of AI-based intrusion detection techniques in automotive systems, while comparative studies have highlighted the importance of evaluating different machine learning approaches under realistic conditions to identify their strengths and limitations [6, 9]. Accordingly, the selected studies provide a balanced and representative overview of current methodological trends, supporting a comprehensive comparison of ML-, DL-, and hybrid-based IDS/IPS techniques. These supporting tables allow easy reference while preserving the readability of the main discussion.

5. Quantitative Trend Analysis Framework

Although this research is primarily presented as a systematic review, a brief quantitative framework is included to clarify how reported accuracy values from the included IDS/IPS studies were summarized. Because many studies did not report sample sizes, confidence intervals, or variance estimates, this component should not be interpreted as a formal effect-size meta-analysis. Rather, it provides a sensitivity-based quantitative summary of reported performance trends under explicit variance assumptions.

For each study, denoted by k, the observed accuracy is represented by the coefficient $\hat{\theta}_k$.

When sample sizes are available, the variance can be calculated using the standard estimator for the Bernoulli variable as follows:

$$V_k = \frac{\hat{\vartheta}_k(1-\hat{\vartheta}_k)}{n_k} \qquad (1)$$

However, because several reviewed studies do not report n_k, a sensitivity-based variance estimation approach was adopted. This approach assumes a set of representative sample sizes:

$$n \in \{100, 500, 1000, 5000\},$$

This procedure allows for the evaluation of the resilience of the aggregated accuracy value when tested under different assumptions of statistical conditions. To examine the stability of trend-level summaries under different assumptions, fixed- and random-effect style calculations were explored as sensitivity tools rather than as formal pooled estimators.

In the fixed-effects model, the standardized effect value is calculated using the following formula:

$$\hat{\vartheta}_{FE} = \frac{\sum_k W_k \hat{\vartheta}_k}{\sum_k W_k}, \qquad W_k = \frac{1}{V_k} \qquad (2)$$

For the random-effects model, the DerSimonianLaird estimator is used to incorporate between-study variance (τ^2):

$$\hat{\vartheta}_{FE} = \frac{\sum_k W_k^* \hat{\vartheta}_k}{\sum_k W_k^*}, \qquad W_k^* = \frac{1}{V_k + \tau^2} \qquad (3)$$

This framework is included to enhance transparency and to explain the computational logic underlying the sensitivity-based quantitative summary presented later in the paper. It is not intended as a full formal meta-analytic derivation.

6. Dataset and Evaluation Protocols

This section provides a concise overview of the datasets and evaluation protocols used in the studies included in this survey.

6.1 Datasets

The reviewed literature draws on both domain-specific vehicular datasets and general IDS benchmark datasets. CAN-specific and vehicular datasets, such as Car-Hacking, ROAD, real CAN traces, J1939-based traffic, and Internet of Vehicles (IoV) datasets, more directly reflect in-vehicle communication characteristics, message timing behavior, and attack surfaces relevant to automotive systems. These datasets are therefore the most informative for assessing IDS/IPS applicability in CAN and vehicular environments [1, 4, 10, 11].

By contrast, benchmark datasets such as KDD Cup, NSL-KDD, and CICIDS are more general-purpose intrusion detection datasets. Although they are not specific to in-vehicle communication, they remain useful for contextualizing broader model behavior, algorithmic trends, and comparative IDS performance under controlled benchmark settings. General benchmark datasets such as KDD Cup and NSL-KDD were retained only to contextualize broader IDS model behavior and were analytically distinguished from in-vehicle CAN-specific datasets.

6.2 Evaluation Protocols and Metrics

Across the reviewed studies, evaluation practices vary considerably in terms of train-test splitting strategies, attack composition, feature preprocessing, and validation protocols. Commonly reported metrics include accuracy, precision, recall, F1-score, detection rate, false alarm rate, AUC, and response time. While these metrics are useful for comparative interpretation, their meaning depends strongly on the dataset type, class balance, and experimental setup. This heterogeneity limits direct one-to-one comparison across studies and further highlights the need for more standardized evaluation frameworks in future research.

Although accuracy was used as the main quantitative indicator in the trend analysis due to its wider availability across the reviewed studies, it should not be interpreted in isolation. Its meaning must be considered alongside precision, recall, F1-score, false alarm rate, and dataset balance in order to avoid overestimating model performance under heterogeneous evaluation conditions.

7. Sensitivity-Based Quantitative Trend Analysis

To complement the qualitative review and provide a structured quantitative perspective on IDS/IPS performance in vehicle network studies, a sensitivity-based quantitative trend analysis was conducted. Reported accuracy values from representative studies were examined using transparent simplifying assumptions in order to summarize general performance tendencies across methodological categories. Given the inconsistent availability of sample sizes, confidence intervals, and variance measures in the source studies, this component should be interpreted as an exploratory quantitative summary rather than as a formal pooled meta-analysis. Table I summarizes representative studies included in this analysis, while Figure 3 provides a comparative visualization of their reported accuracy values.

This analysis is intended to reveal broad performance tendencies under sensitivity assumptions and should therefore be interpreted as trend-oriented rather than as a formal pooled meta-analytic estimate.

The quantitative summary suggests a general trend in which deep learning approaches often achieve higher reported performance, followed by hybrid approaches, while traditional machine learning methods remain attractive in lightweight and resource-constrained settings. The sensitivity analysis showed limited variation across the explored assumptions,

suggesting that the observed trend pattern remained broadly stable within the tested scenarios.

Table I. Sensitivity-Based Quantitative Summary of Representative IDS/IPS Studies

Study	Technique	Metric	Score
Al-Quayed *et al.* [12]	DT, RF, SVM	Accuracy	0.9948
Alalwany *et al.* [6]	Stacking Ensemble Learning	Accuracy	0.984
Nair *et al.* [13]	ML+DL (SVM, RF, XGBoost + CNN, RNN)	Accuracy	0.965
Rani *et al.* [14]	Comparative ML/DL architectures	Accuracy	0.970
Sharmin *et al.* [15]	Survey + Benchmarking	Accuracy	0.950
Dayyeh *et al.* [16].	Multi-stage FL IDS	Accuracy	0.960
Young *et al.* [17]	ML+DL (SVM, RF, kNN, DNN, CNN)	Accuracy	0.950
Tanksale [18]	IDS survey (ML, DL)	Accuracy	0.940
Apruzzese *et al.* [19]	IDS Evaluation Framework	Accuracy	0.955
Yang, *et al.* [20]	Hybrid Statistical + NN	Accuracy	0.990

Note: The quantitative summary is exploratory and sensitivity-based; variance-related interpretation relies on approximations because several source studies did not report sample sizes or confidence intervals.

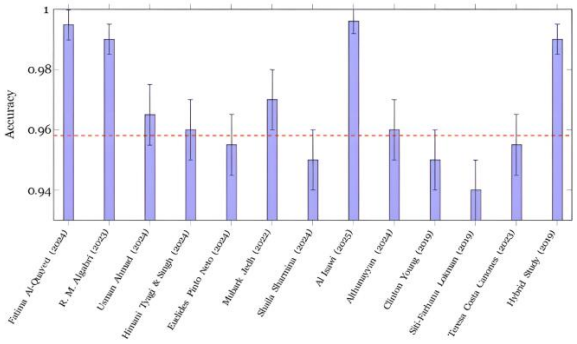

Figure 3: Comparative visualization of reported accuracy values across the included IDS/IPS studies.

7.1 Sensitivity Analysis

Due to the absence of reported sample sizes or confidence intervals in several studies, a sensitivity-based analysis was conducted to examine how reported accuracy values behave under different simplifying assumptions. To approximate variance, Bernoulli-based estimators were used under a set of hypothetical sample sizes:

$$\in\{100,\ 500,\ 1000,\ 5000\}.$$

Rather than producing formal pooled estimates, this analysis was designed to evaluate the stability of observed performance patterns under varying assumptions. The results showed limited variation across the explored scenarios, indicating that the general trend of reported performance remained broadly stable within the tested conditions.

This behavior suggests that the relative ordering of methodological approaches (e.g., DL, hybrid, and ML) is consistent across different sensitivity assumptions. However, these findings should be interpreted as indicative trends rather than statistically precise aggregate estimates, given the absence of consistent variance and sample-size information in the original studies.

7.2 Interpretation

The results suggest that deep learning techniques generally achieve higher reported performance in intrusion detection tasks, primarily due to their ability to capture complex temporal and structural patterns in vehicular network data. Hybrid approaches combining ML and DL also demonstrate strong performance, although they typically require higher computational resources.

Traditional machine learning methods remain effective in lightweight and resource-constrained environments, offering a practical trade-off between accuracy and efficiency. Overall, the findings highlight the importance of balancing detection performance with computational cost and deployment feasibility in CAN-based and vehicular systems.

These observations should be interpreted as general performance trends derived under sensitivity assumptions, rather than as definitive pooled performance estimates [1, 2, 21-23].

8. Critical Discussion

8.1 Reasons for the Success or Failure of Different Methods

The studies reviewed demonstrate that the performance of AI-based intrusion detection systems depends heavily on the type of model used, the characteristics of the data, and the operational constraints of the deployment environment. Traditional machine learning methods, particularly Random Forest (RF) and Support Vector Machine (SVM), remain widely adopted in intrusion detection for vehicular networks due to their robust classification capabilities and relatively low computational requirements. The reviewed studies indicate that RF models achieve reliable performance in detecting known attack patterns through ensemble learning, whereas their effectiveness may decrease when confronted with previously unseen or evolving attacks. In contrast, SVM-based models are capable of learning complex decision boundaries and can identify certain novel attack patterns; however, several studies have reported higher false-positive rates under heterogeneous traffic conditions, which may limit their applicability in real-world vehicular environments [1, 8, 11, 21].

To overcome these limitations, many recent studies have proposed hybrid architectures that integrate multiple machine learning algorithms or combine ML with deep learning techniques. Such approaches generally improve detection accuracy, robustness, and generalization capability, although these gains are often achieved at the expense of increased model complexity and computational overhead, which may reduce their suitability for real-time deployment in resource-constrained vehicular systems [8, 11, 21, 23].

To address these limitations, several studies have proposed hybrid approaches that combine multiple ML algorithms or integrate ML with deep learning (DL) techniques. These models often improve detection accuracy and robustness; however, they introduce additional complexity in model design and require higher computational resources, which can negatively impact their suitability for real-time applications.

In the domain of deep learning, convolutional neural networks (CNNs) demonstrate strong performance in capturing local patterns in CAN traffic and extracting low-level signal features, making them well-suited for complex intrusion detection scenarios. However, their effectiveness depends heavily on the availability of large, well-labeled datasets, and they require careful hyperparameter tuning to avoid overfitting. Recurrent neural networks (RNNs) and long short-term memory (LSTM) models are particularly effective in modeling temporal dependencies in sequential CAN messages. Despite their advantages, their relatively slow training and inference processes limit their applicability in time-critical environments.

Ensemble DL methods further enhance detection performance and improve resilience against diverse attack types, but they significantly increase computational and memory requirements. This makes their deployment challenging in resource-constrained environments such as in-vehicle networks and IoT-based vehicular systems.

8.2 External Validity and Reproducibility

The reviewed studies reveal clear challenges related to external validity and reproducibility. A considerable number of studies rely on synthetic, imbalanced, or domain-specific datasets that may not fully represent real-world vehicular traffic conditions. This increases the risk of overfitting and limits the generalizability of the reported results. Additionally, inconsistencies in data preprocessing, segmentation, and feature engineering may lead to unintended data leakage, which can artificially inflate performance metrics. Furthermore, some studies employ validation strategies that do not reflect real deployment scenarios, such as random cross-validation without considering temporal dependencies or data source separation. These practices reduce the reliability of performance claims and hinder fair comparison across different approaches [8, 24, 25].. To improve external validity, future research should adopt more rigorous evaluation protocols, such as time-aware data splitting, source-based

validation, and explicit reporting of preprocessing pipelines. Reporting inference time on target hardware and conducting ablation studies to quantify the impact of each component would further enhance reproducibility and transparency.

8.3 Practical Deployment Considerations

While many IDS/IPS approaches achieve high performance in controlled experimental settings, their deployment in real-world vehicular environments introduces additional challenges. Computational efficiency remains a critical concern, as many high-performing DL models require substantial processing power and memory resources, making them unsuitable for embedded systems such as electronic control units (ECUs).

To enable practical deployment, techniques such as model compression, pruning, and quantization are essential to reduce model size and inference cost without significantly degrading performance. Inference latency is another key factor, as intrusion detection systems must operate under strict real-time constraints. Models with high latency or those requiring batch processing may fail to meet these requirements.

Practical deployment of IDS/IPS solutions in vehicular environments remains challenging due to compatibility requirements with existing automotive communication protocols and system architectures [26, 27]. In addition, the absence of standardized evaluation frameworks and testing methodologies makes objective comparison between different approaches difficult and hinders their wider industrial adoption [28]. Furthermore, practical deployment requires addressing computational efficiency, privacy preservation, and low-latency processing, particularly in resource-constrained vehicular systems and edge-based environments[22, 29-31]. These findings collectively indicate that achieving practical and scalable deployment requires balancing detection performance with implementation feasibility.

Finally, scalability and cost considerations play an important role in deployment decisions. Cloud-based solutions offer high scalability but may introduce latency, privacy, and security concerns. Edge-based solutions reduce latency but require lightweight and efficient models capable of operating under limited resources. Achieving an optimal balance between detection accuracy, computational cost, latency, and deployment feasibility remains a central challenge in this field.

9. Challenges and Open Issues

Despite significant advancements in intrusion detection and protection technologies, several challenges still hinder the effective security of CAN networks [1, 5, 26, 27].

9.1 Resource Limitations

Many electronic control units (ECUs) have limited computing power and memory capabilities, making it difficult to implement resource-intensive security mechanisms.

9.2 Real-Time Requirements

Systems in vehicles rely on real-time communication, and introducing additional security protocols can increase latency, complicating implementation.

9.3 Lack of Standardized Standards

There are no widely agreed-upon security standards for CAN networks, which limit the ability to develop consistent and reliable protection solutions across different systems.

10. Limitations

Although this review provides a comprehensive overview of the latest developments in IDS/IPS techniques for CAN networks, several limitations should be acknowledged. First, many of the included studies did not report sample sizes or variance measures in a sufficiently consistent manner. As a result, the quantitative component of this review could not be conducted as a formal effect-size meta-analysis. Instead, a sensitivity-based quantitative trend analysis was used to explore reported performance patterns under explicit simplifying assumptions. Second, substantial heterogeneity exists across the reviewed studies in terms of datasets, feature representations, attack scenarios, evaluation metrics, and experimental protocols. This variability limits strict cross-study comparability and requires cautious interpretation of any quantitative summary. Third, some included studies rely on benchmark datasets that are not specific to in-vehicle communication environments. Although these studies were retained for contextual comparison, they should not be interpreted as equivalent to evidence derived from CAN-native or vehicular datasets. Accordingly, the quantitative findings presented in this review should be interpreted as broad trend indicators rather than definitive pooled estimates.

11. Future Research Trends

Based on the review and analysis, several promising research paths for the future can be suggested:

- **Developing Lightweight Security Solutions:** Future research should focus on designing effective security mechanisms that are compatible with the limited constraints of electronic control units within vehicles.
- **Testing and Validation in Real-World Environments:** Evaluation in real-world environments is a crucial step to ensure that detection and protection systems can operate effectively under varying and practical operating conditions.
- **Integrating ML Technologies:** The use of ML contributes to improving the ability to detect anomalous attacks while simultaneously reducing false alarm rates.
- **Prioritizing Research Areas:** It is important to direct research efforts according to priority and expected impact, focusing on the most prominent challenges facing vehicle cybersecurity.

12. Conclusion

This review has provided a comprehensive overview of current solutions for intrusion detection and prevention systems in CAN networks, employing a methodology that combines systematic review with a sensitivity-based quantitative trend analysis. This approach integrates structured evidence analysis with a broad analytical comparison of IDS/IPS methods implemented in these networks. The quantitative findings reported in this review should be interpreted as broad trend indicators that support comparative insight, rather than as definitive pooled performance estimates. Despite significant progress in this field, challenges remain in securing critical in-vehicle communication systems. Therefore, future research should focus on developing lightweight and highly efficient security solutions capable of addressing the growing cyber threats targeting modern vehicles.

Data Availability

The datasets used and analyzed during the current study are available from the corresponding author upon reasonable request.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Conflict of Interest

The authors declare that there are no conflicts of interest.

References

[1] Kalkan, S.C., Sahingoz, O.K. (2020) In-vehicle intrusion detection system on controller area network with machine learning models. *In Proceedings of the 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT 2020)*, *IEEE*, Kharagpur, India, 1-3 July, 2020, pp. 1-6.

[2] Alfardus, A., Rawat, D.B. (2021) Intrusion detection system for can bus in-vehicle network based on machine learning algorithms. *In Proceedings of the 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, *IEEE*, 1-4 December, 2021, pp. 0944-0949.

[3] Al-Janabi, M., Ismail, M.A., Ali, A.H. (2021) Intrusion Detection Systems, Issues, Challenges, and Needs, *The International Journal of Computational Intelligence Systems* **14**: 560-571.

[4] Panigrahi, R., Borah, S., Bhoi, A.K., Ijaz, M.F., Pramanik, M., Jhaveri, R.H., Chowdhary, C.L. (2021) Performance assessment of supervised classifiers for designing intrusion detection systems: a comprehensive review and recommendations for future research, *Mathematics* **9**: 690.

[5] Micale, D., Costantino, G., Matteucci, I., Fenzl, F., Rieke, R., Patanè, G. (2022) Cahoot: a context-aware vehicular intrusion detection system. *In Proceedings of the 2022 IEEE international conference on trust,*

security and privacy in computing and communications (TrustCom), *IEEE*, Wuhan, China, pp. 1211-1218.

[6] Alalwany, E., Mahgoub, I. (2022) Classification of normal and malicious traffic based on an ensemble of machine learning for a vehicle can-network, *Sensors* **22**: 9195.

[7] Rajapaksha, S., Kalutarage, H., Al-Kadri, M.O., Petrovski, A., Madzudzo, G., Cheah, M. (2023) Ai-based intrusion detection systems for in-vehicle networks: A survey, *ACM Computing Surveys* **55**: 1-40.

[8] Nagarajan, J., Mansourian, P., Shahid, M.A., Jaekel, A., Saini, I., Zhang, N., Kneppers, M. (2023) Machine Learning based intrusion detection systems for connected autonomous vehicles: A survey, *Peer-to-Peer Networking and Applications* **16**: 2153-2185.

[9] Kumar, A., Das, T.K. (2023) CAVIDS: Real time intrusion detection system for connected autonomous vehicles using logical analysis of data, *Vehicular Communications* **43**: 100652.

[10] Alalwany, E., Mahgoub, I. (2024) An effective ensemble learning-based real-time intrusion detection scheme for an in-vehicle network, *Electronics* **13**: 919.

[11] Shahriar, M.H., Xiao, Y., Moriano, P., Lou, W., Hou, Y.T. (2023) CANShield: Deep-learning-based intrusion detection framework for controller area networks at the signal level, *IEEE Internet of Things Journal* **10**: 22111-22127.

[12] Al-Quayed, F., Ahmad, Z., Humayun, M. (2024) A situation based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of industry 4.0, *IEEE Access* **12**: 34800-34819.

[13] Nair, R. (2023) Unraveling the Decision-making Process Interpretable Deep Learning IDS for Transportation Network Security, *Journal of Cybersecurity & Information Management* **12**.

[14] Rani, D., Kaushal, N.C. (2020) Supervised machine learning based network intrusion detection system for Internet of Things. *In Proceedings of the 2020 11th International conference on computing, communication and networking technologies (ICCCNT)*, *IEEE*, pp. 1-7.

[15] Sharmin, S., Mansor, H., Abdul Kadir, A.F., Aziz, N.A. (2024) Benchmarking frameworks and comparative studies of Controller Area Network (CAN) intrusion detection systems: A review, *Journal of Computer Security* **32**: 477-507.

[16] Dayyeh, R., AlSawareah, W., Kasasbeh, B., Qaddoura, R., Kamal, S. (2023) Comparative Analysis of Decision Trees, Random Forest, and k-Nearest Neighbors in Predictive Analytics for Orange Telecom's Customer Complaint Data. *In Proceedings of the 2023 2nd International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI)*, *IEEE*, Zarqa, Jordan, pp. 1-6.

[17] Young, C., Olufowobi, H., Bloom, G., Zambreno, J. (2019) Automotive intrusion detection based on constant can message frequencies across vehicle driving modes. *In Proceedings of the 2019 ACM Workshop on Automotive Cybersecurity (AutoSec 2019)*, *Association for Computing Machinery (ACM)*, Richardson, Texas, USA, March 27, 2019, pp. 9-14.

[18] Tanksale, V. (2024) Intrusion detection system for controller area network, *Cybersecurity* **7**: 4.

[19] Apruzzese, G., Laskov, P., Schneider, J. (2023) Sok: Pragmatic assessment of machine learning for network intrusion detection. *In Proceedings of the 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*, *IEEE*, Delft, Netherlands, 3-7 July, 2023, pp. 592-614.

[20] Kocher, G., Kumar, G. (2022) A hybrid deep learning approach for effective intrusion detection systems using spatial-temporal features, *Adv. Eng. Sci.* **54**: 1503-1519.

[21] Ahmed, N., Hassan, F., Aurangzeb, K., Magsi, A.H., Alhussein, M. (2024) Advanced machine learning approach for DoS attack resilience in internet of vehicles security, *Heliyon* **10**: e28844.

[22] Alemerien, K., Al-Suhemat, S., Almahadin, M. (2024) Towards optimized machine-learning-driven intrusion detection for Internet of Things applications, *International Journal of Information Technology* **16**: 4981-4994.

[23] Kousar, A., Ahmed, S., Altamimi, A., Khan, Z.A. (2024) A Novel Light-Weight Machine Learning Classifier for Intrusion Detection in Controller Area Network in Smart Cars, *Smart Cities* **7**: 3289-3314.

[24] El-Gayar, M.M., Alrslani, F.A., El-Sappagh, S. (2024) Smart collaborative intrusion detection system for securing vehicular networks using ensemble machine learning model, *Information* **15**: 583.

[25] Musa, U.I., Musa, A.I., Galadima, Y.I., Kantunsung, R.O., Gupta, S., Dua, S. (2024) Machine Learning-Based Cybersecurity Optimization in Internet of Things-Enabled Autonomous Vehicles. *In Proceedings of the 2024 1st International Conference on Innovative Engineering Sciences and Technological Research (ICIESTR)*, *IEEE*, Muscat, Oman, 14-15 May, 2024, pp. 1-6.

[26] Rajapaksha, S., Madzudzo, G., Kalutarage, H., Petrovski, A., Al-Kadri, M.O. (2024) CAN-MIRGU: a comprehensive CAN bus attack dataset from moving vehicles for intrusion detection system evaluation. *In Proceedings of the 2nd Symposium on Vehicle Security and Privacy (VehicleSec 2024)*, San Diego, California, USA, February 26 to March 1, 2024, pp. 43.

[27] Wasicek, A., Pesé, M.D., Weimerskirch, A., Burakova, Y., Singh, K. (2017) Context-aware intrusion detection in automotive control systems. *In Proceedings of the 5th ESCAR USA Conference (Embedded Security in Cars)*, Ypsilanti, Michigan, USA, 21-22 June, 2017, pp. 21-22.

[28] Ossen, S. (2025) Enabling Low-Latency High-Throughput Real-Time Stream Processing Using Smart Network Compute Elements. *Department of Computer Science*, Ph.D. Thesis, Indiana University, Bloomington, Indiana, USA.

[29] Liu, H., Lang, B., Liu, M., Yan, H. (2019) CNN and RNN based payload classification methods for attack detection, *Knowledge-Based Systems* **163**: 332-341.

[30] Faker, O., Dogdu, E. (2019) Intrusion detection using big data and deep learning techniques. *In Proceedings of the 2019 ACM Southeast Conference (ACMSE 2019)*, Kennesaw, Georgia, USA, 18-20 April, 2019, pp. 86-93.

[31] Kumar, A., Sharma, I. (2023) CNN-based approach for IoT intrusion attack detection. *In Proceedings of the 2023 International conference on sustainable computing and data communication systems (ICSCDS)*, *IEEE*, Erode, India, 23-25 March, 2023, pp. 492-496.