Synergy 2025: A Multidisciplinary Forum for Collaborative Research and Innovation
January 2025
ISBN Number: 978-93-95305-78-5

NEXT-GENERATION SECURITY FOR VEHICULAR SYSTEMS: A REVIEW OF CONTROLLER AREA NETWORK INTRUSION DETECTION

Vishal R. Deshmukh
Ph.D. Scholar
Department of CSE,
P. K. University, Shivpuri, MP, India.
deshmukh.vishal07@gmail.com
Prof. Dr. Indrabhan S. Borse
Ph.D. (Computer Engineering) Associate Professor,
Department of CSE,
P. K. University, Shivpuri, MP, India
indrabhan2000@gmaill.com

Abstract – *The rise of connected and autonomous vehicles has revolutionized modern transportation but has also exposed vehicular systems to unprecedented cybersecurity challenges. At the heart of these systems lies the Controller Area Network (CAN), a widely adopted protocol for in-vehicle communication that is increasingly targeted by cyberattacks. Intrusion Detection Systems (IDS) have emerged as a critical defense mechanism against CAN-based attacks, offering real-time monitoring and threat mitigation.This review examines the state-of-the-art advancements in IDS for CAN networks, providing a comprehensive analysis of traditional and next-generation methodologies. The study categorizes existing approaches, including signature- based, anomaly-based, and hybrid techniques, and evaluates their effectiveness in addressing contemporary attack vectors. Emerging technologies, such as machine learning, blockchain integration, and lightweight security protocols, are also explored for their potential to enhance IDS capabilities in resource-constrained vehicular environments. By identifying current challenges, research gaps, and future directions, this review aims to guide the development of robust and adaptive intrusion detection strategies, ensuring secure and resilient vehicular systems in the era of connected mobility. The study explores traditional rule-based approaches alongside modern techniques leveraging machine learning, anomaly detection, and lightweight cryptography. We categorize existing IDS frameworks based on their detection strategies, such as signature-based, anomaly- based, and hybrid approaches, while analyzing their suitability for resource-constrained vehicular environments.*

Keywords- *Controller Area Network (CAN Controller Area Network Intrusion Detection Systems (CAN IDS) .*

ISBN Number: 978-93-95305-78-5

INTRODUCTION

Introduction The rapid advancements in connected and autonomous vehicle technologies have revolutionized modern transportation systems, promising safer, more efficient, and convenient mobility. However, this connectivity also exposes vehicular systems to a range of cyber threats, posing significant risks to safety and security. Among the critical components of modern vehicles, the Controller Area Network (CAN) serves as the backbone of intra-vehicle communication, enabling seamless interaction between electronic control units (ECUs). Despite its importance, the CAN protocol was not originally designed with robust security features, making it vulnerable to cyberattacks such as spoofing, denial-of-service (DoS), and data injection. [1][2]

As the automotive industry transitions into the era of smart transportation, ensuring the security of the CAN has become a top priority. Intrusion detection systems (IDS) have emerged as a crucial defense mechanism, providing real-time monitoring and identification of malicious activities within the CAN. Over the years, researchers and practitioners have proposed various IDS techniques, ranging from traditional rule-based methods to cutting-edge machine learning algorithms. However, these solutions face challenges related to accuracy, adaptability, scalability, and resource constraints in vehicular environments. [2][3]

This review aims to provide a comprehensive examination of the current state of IDS for CAN, highlighting their methodologies, strengths, and limitations. The paper categorizes existing IDS approaches into signature-based, anomaly-based, and hybrid models, offering insights into their detection capabilities and applicability to evolving attack vectors. Furthermore, it identifies key research gaps and emerging trends, proposing directions for the development of next- generation IDS solutions that are tailored to the unique demands of vehicular systems.[4][5][6]

By consolidating existing knowledge and providing a critical analysis of contemporary approaches, this study seeks to support researchers, developers, and policymakers in enhancing the security of vehicular networks. The findings aim to contribute to the establishment of robust cybersecurity strategies, ensuring the safe deployment of intelligent transportation systems in the face of growing cyber threats.

ISBN Number: 978-93-95305-78-5

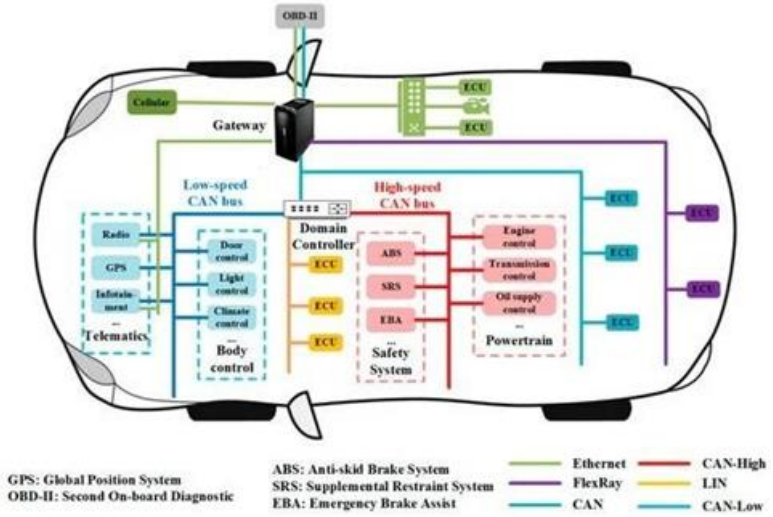

Fig. 1: Automotive Attack Surface [11]

Additionally, the review identifies critical research gaps and unresolved challenges, including issues of computational overhead, false positive rates, and adaptability to evolving attack vectors. By synthesizing current knowledge and outlining future directions, this paper aims to guide researchers, practitioners, and policymakers in their efforts to enhance vehicular network security.[11]

LITERATURE REVIEW

The increasing prevalence of cyberattacks targeting vehicular systems has driven extensive research into intrusion detection systems (IDS) for securing the Controller Area Network (CAN). This literature review examines the evolution of IDS approaches, categorizing them based on detection methodologies, technological advancements, and their applicability to vehicular environments.

1. Signature-Based IDS

Signature-based IDS approaches rely on predefined rules and patterns to detect known attack signatures. Research by Miller and Valasek (2013) highlighted vulnerabilities in CAN that could be exploited using predictable patterns, spurring the development of IDS to detect such attacks. While signature-based systems, such as the work by Muter et al. (2014), offer high accuracy for known threats, they lack adaptability to novel attack vectors, making them less effective in dynamic vehicular environments.[3][4

2. Anomaly-Based IDS

Anomaly-based systems focus on detecting deviations from normal network behavior. The work of Cho and Shin (2016) introduced a statistical anomaly detection framework for CAN traffic, leveraging timing and frequency analysis to identify irregularities. Similarly, Marchetti et al. (2017) explored entropy-based methods to detect anomalies in CAN traffic patterns. These systems are effective in identifying zero-day attacks but are prone to high false positive rates, necessitating further refinement. [5][6]

ISBN Number: 978-93-95305-78-5

3. Machine Learning-Based IDS

Recent advancements in machine learning have significantly influenced IDS development. Gmiden et al. (2019) proposed a machine learning-based IDS that uses supervised learning to classify benign and malicious traffic. Other works, such as Taylor et al. (2020), explored deep learning models, including convolutional neural networks (CNNs) and recurrent neural networks (RNNs), to enhance detection accuracy and reduce false positives. However, the computational overhead associated with these methods presents challenges for deployment in resource-constrained vehicular systems. [7][8]

4. Hybrid IDS Approaches

Hybrid IDS solutions combine multiple detection techniques to achieve a balance between accuracy and adaptability. Kang et al. (2021) introduced a hybrid IDS that integrates anomaly-based detection with machine learning classifiers, achieving improved detection rates for sophisticated attacks. Such approaches leverage the strengths of different methodologies but often face challenges in terms of complexity and scalability. [9]

5. Lightweight IDS for Resource-Constrained Systems

Given the limited computational resources in vehicular ECUs, lightweight IDS solutions have gained attention. Work by Humayed and Luo (2022) proposed a lightweight cryptographic IDS framework tailored for CAN, prioritizing low latency and minimal resource utilization. These solutions address practical implementation concerns but often trade off advanced detection capabilities. [10]

6. Trends in Emerging Technologies

Emerging trends in IDS development include the use of blockchain for secure logging, federated learning to improve detection across distributed systems, and the integration of IDS with vehicle-to-everything (V2X) communication protocols. For example, Zhou et al. (2023) explored blockchain-enhanced IDS for CAN, enabling tamper-proof event tracking and collaborative anomaly detection across vehicles.[12]

7. Research Gaps and Challenges

Despite the progress, significant challenges remain in designing IDS for vehicular systems. Issues such as high false positive rates, limited scalability, and the ability to adapt to evolving attack vectors require further investigation. Additionally, balancing detection accuracy with computational efficiency remains a critical area of focus for researchers.[13]

The paper a steady progression from traditional rule-based IDS to advanced machine learning and hybrid approaches. However, no single solution has yet achieved the ideal balance between accuracy, adaptability, and resource efficiency. This review highlights the need for continued innovation in IDS design to address the unique challenges posed by vehicular networks, ensuring robust security

ISBN Number: 978-93-95305-78-5

for the next generation of connected and autonomous vehicles.The security of Controller Area Networks (CAN) in modern vehicles has become a topic of critical importance due to the vulnerability of in- vehicle communication systems to cyber threats. Controller Area Network Intrusion Detection Systems (CAN IDS) have emerged as a crucial line of defense against potential intrusions. This literature review aims to analyze and synthesize the current state of research, methodologies, challenges, and future directions in the realm of CAN IDS.[14][15][16]

METHODOLOGY

This study employs a systematic review approach to analyze and synthesize existing research on intrusion detection systems (IDS) for securing the Controller Area Network (CAN) in vehicular systems. The methodology involves a structured process of data collection, classification, analysis, and synthesis to ensure comprehensive coverage of the topic and reliable insights into the state of the art.

1. Scope and Objectives

The primary objective of this review is to evaluate the current landscape of IDS for CAN, identify trends, challenges, and gaps, and propose future directions for research. The study focuses on:

- Categorizing IDS approaches (signature-based, anomaly-based, hybrid, etc.).
- Evaluating the effectiveness of IDS techniques in terms of accuracy, scalability, and adaptability.
- Identifying key research challenges and opportunities for innovation.

2. Literature Search and Data Collection

A systematic search was conducted using academic databases, including IEEE Xplore, ACM Digital Library, SpringerLink, and Scopus, to identify relevant studies. Keywords such as “CAN intrusion detection,” “vehicular security,” “automotive cybersecurity,” and “IDS for CAN” were used. The inclusion criteria were:

- Peer-reviewed articles published between 2010 and 2023.
- Studies focusing on IDS methodologies for CAN in vehicular systems.
- Articles providing quantitative evaluations of IDS performance.

Exclusion criteria included articles unrelated to vehicular systems, studies without experimental evaluations, and publications in non-English languages.

3. Classification Framework

The collected literature was classified based on the following parameters:

ISBN Number: 978-93-95305-78-5

- **Detection Methodology**: Signature-based, anomaly-based, hybrid, or machine learning.
- **Evaluation Metrics**: Accuracy, false positive rate, detection speed, and computational overhead.
- **Implementation Context**: Simulation, real- world deployment, or testbed validation.
- **Technology Used**: Machine learning models, cryptographic techniques, or emerging technologies such as blockchain.

4. Data Analysis

Each study was analyzed to extract:

- Methodology: The approach used for intrusion detection, including algorithms and frameworks.
- Performance: The reported effectiveness of the IDS in detecting intrusions under various conditions.
- Limitations: Identified challenges, such as scalability, adaptability to new attack vectors, and resource constraints.

The extracted data was systematically organized into tables and graphs to enable comparative analysis.

5. Synthesis and Interpretation

The findings from the literature were synthesized to provide insights into:

- The evolution of IDS for CAN from traditional rule-based approaches to advanced machine learning techniques.
- Emerging trends, such as lightweight cryptographic solutions and integration with V2X systems.
- Research gaps and the need for solutions addressing false positive rates, real-time detection, and resource efficiency.

6. Validation of Findings

To ensure the reliability and validity of the findings, the review was cross-verified with meta-analyses and key industry reports on vehicular security. The synthesis was structured to align with best practices in systematic reviews, including transparency and reproducibility of the methodology.

7. Proposed Framework for Future Research

Based on the review, a framework for advancing IDS for CAN is proposed, emphasizing:

- Incorporating federated learning to improve scalability and adaptability.
- Developing lightweight yet robust detection mechanisms for resource-constrained environments.

ISBN Number: 978-93-95305-78-5

- Exploring interdisciplinary approaches that integrate cryptography, machine learning, and blockchain technologies.

CONCLUSION

The Controller Area Network (CAN) is a vital communication protocol in vehicular systems, remains highly vulnerable to a variety of cyberattacks due to its lack of inherent security features. Intrusion Detection Systems (IDS) have emerged as a critical defense mechanism, enabling the detection and mitigation of malicious activities within the CAN. Its provides a comprehensive analysis of the state-of-the-art IDS approaches for CAN, categorizing them into signature- based, anomaly-based, hybrid, and machine learning- driven methodologies. While each approach offers unique advantages, challenges such as false positives, computational overhead, and limited adaptability persist, especially in resource-constrained vehicular environments. Emerging trends, including lightweight cryptographic techniques, block chain-enhanced logging, and federated learning, show promise in addressing these challenges and advancing IDS design.

REFERENCES

[1] *Vishal R. Deshmukh , Prof. Dr. Indrabhan S. Borse , "Enhancing Security in Vehicular Networks: A Study of Controller Area Network Intrusion Detection Systems", Vol. 9, No. 2, 2024, PP. 82-85, International Journal of Innovations in Engineering and Science, www.ijies.net*

[2] *Checkoway, Stephen, et al. "Comprehensive experimental analyses of automotive attack surfaces." In Proceedings of the USENIX Security Symposium, vol. 12, pp. 6-8. 2011.*

[3] *Miller, C., & Valasek, C. (2013). Adventures in automotive networks and control units. DEF CON.*

[4] *Muter, M., & Asaj, N. (2014). Entropy-based anomaly detection for in-vehicle networks. IEEE Intelligent Vehicles Symposium (IV), 1110–1115.*

[5] *Cho, K.-T., & Shin, K. G. (2016). Fingerprinting electronic control units for vehicle intrusion detection.* USENIX Security Symposium.

[6] *Marchetti, M., & Stabili, D. (2017). Anomaly detection of CAN bus messages through analysis of ID sequences.* IEEE Transactions on Intelligent Transportation Systems, *18(5), 1238–1248.*

[7] *Gmiden, M., Boudriga, N., & Bouaziz, T. (2019). A CAN bus intrusion detection architecture for connected vehicles.* IEEE Vehicular Technology Conference (VTC).

[8] *Taylor, A., Leblanc, S., & Japkowicz, N. (2020). Anomaly detection in automotive CAN bus*

ISBN Number: 978-93-95305-78-5

data with deep learning. IEEE Vehicular Networking Conference (VNC).

[9] *Kang, M., Kim, S., & Cho, J. (2021). Hybrid intrusion detection system for CAN bus security in connected cars.* IEEE Transactions on Vehicular Technology, *70(3), 2346–2356.*

[10] *Humayed, A., & Luo, B. (2022). Lightweight cryptographic-based intrusion detection system for in-vehicle networks.* ACM Transactions on Cyber-Physical Systems.

[11] *Zhou, H., Wang, C., & Zhang, Y. (2023). Blockchain-enhanced intrusion detection for connected vehicles: A decentralized approach.* IEEE Internet of Things Journal.

[12] *Haichun Zhang, XuMeng, XiongZhangandZhenglin Liu, "CANsec: APractical in-Vehicle Controller Area Network Security Evaluation Tool", Sensors 2020, 20, 4900; doi:10.3390/s20174900 www.mdpi.com/journal/sensors*

[13] *Koscher, Karl, et al. "Experimental security analysis of a modern automobile." In Security and Privacy (SP), 2010 IEEE Symposium on, pp. 447-462. IEEE, 2010.*

[14] *Zhao, Lichao, et al. "In-vehicle network security: Vulnerabilities, challenges, and research directions." IEEE Transactions on Intelligent Transportation Systems 17.12 (2016): 3436-3452.*

[15] *Abomhara, Mohamed, and Asif Irshad Khan Køien. "Security of the internet of things: Vulnerabilities, attacks, and countermeasures." IEEE Access 5 (2017): 115-124.*

[16] *Zimba, Johannes, et al. "Anomaly detection for in-vehicle networks using machine learning." 2019 IEEE 16th Annual Consumer Communications & Networking Conference (CCNC), 2019, pp. 1-6.*

[17] *Park, Soo-Hyung, et al. "Deep learning-based intrusion detection system in in-vehicle network." Electronics 9.10 (2020): 1622.*

[18] *Rössler, Johannes, et al. "Towards an intrusion detection system for in-vehicle networks based on ECU communication behavior." 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2018, pp. 1-5.*

[19] *Liu, Zhipeng, et al. "A survey on security aspects for vehicular ad hoc networks." IEEE Transactions on Intelligent Transportation Systems 22.1 (2021): 95-108.*

[20] *Wang, Xingyu, et al. "A hybrid intrusion detection system for in- vehicle network security." 2022 IEEE 24th International Conference on Intelligent Transportation Systems (ITSC), 2022, pp. 1-6.*

[21] *Gupta, Anjali, et al. "Federated learning-based intrusion detection for connected vehicles." IEEE Transactions on Vehicular Technology 72.4 (2023): 3565-3577.*