State of the Art on CAN Protocol Vulnerabilities and Intrusion Detection Systems in Automotive Networks

Mohammed Saad DAROUICHE
Polydisciplinary Faculty of Taza
Sidi Mohamed Ben Abdellah University
Fez, Morocco
mohammedsaad.darouiche@usmba.ac.ma

El bachir TAZI
Polydisciplinary Faculty of Taza
Sidi Mohamed Ben Abdellah University
Fez, Morocco
elbachir.tazi@usmba.ac.ma

Hassan SATORI
Faculty of Sciences Dhar Mahraz
Sidi Mohamed Ben Abdellah University
Fez, Morocco
hassan.satori@usmba.ac.ma

2024 3rd International Conference on Embedded Systems and Artificial Intelligence (ESAI) | 979-8-3315-2205-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/ESAI62891.2024.10913954

***Abstract*—The Controller Area Network (CAN) protocol is a primary communication protocol in modern vehicles that enables communication among electronic control units (ECU). Nevertheless, this protocol contains numerous weaknesses that make automotive networks susceptible to various cyber dangers, including message spoofing, eavesdropping, and denial-of-service (DoS) assaults. This article provides a detailed analysis of modern Intrusion Detection Systems (IDS) created to protect CAN networks. We evaluated and contrasted the most recent IDS approaches, discussing their advantages and disadvantages. The paper points out the current research limitations and suggests potential future research directions to improve IDS performance in automotive networks. The practical implications of these discoveries suggest that employing IDS methodologies in real-world settings could greatly enhance the security of modern vehicles.**

Keywords—CAN protocol, automotive cybersecurity, Intrusion Detection System (IDS), network security, anomaly detection, cyber threats, false positives rate.

I. Introduction

The inclusion of advanced electronic systems in contemporary vehicles has transformed the automotive sector, improving both capabilities and user satisfaction. At the heart of this new development is the Controller Area Network (CAN) protocol, which enables effective communication between different Electronic Control Units (ECUs). Although the CAN protocol is widely used, it was not initially created with cybersecurity in consideration, leaving it open to different cyberattacks [1]. Securing CAN networks has become a crucial focus due to the growing use of connectivity features in vehicles [2]. The effects of cyber threats on automotive networks are substantial, with the potential to cause major financial losses and put human lives at risk in terms of safety.

In response to the rise in cyberattacks on automotive systems, Intrusion Detection Systems (IDS) tailored for CAN networks have been created [3]. IDS solutions are crucial for monitoring network activity, identifying potential breaches, and blocking attacks before they result in significant harm. This research provides a comprehensive analysis of the latest intrusion detection techniques employed in CAN networks, highlighting their advantages, disadvantages, and practical characteristics. Additionally, the article points out areas that require more investigation and suggests potential directions for future research that seeks to enhance IDS effectiveness in automotive networks.

II. Background

A. Overview of the CAN Protocol

The Controller Area Network (CAN) protocol was designed by Bosch in 1986 [4], to establish real-time communication between various ECUs in a vehicle. Unlike the usual communication protocols, CAN message is broadcasted to ECUs connected to the network. This mechanism ensures efficient data transfer, and rapid system response.

Despite its efficiency and reliability, the CAN protocol was developed without taken in consideration modern cybersecurity threats. The absence of enough safety mechanisms leaves the network vulnerable to attacks. Since CAN messages are not encrypted, attackers can easily intercept and eavesdrop on communications. Also, the lack of authentication mechanisms allows attackers to inject or alter messages on the network, potentially leading to dangerous consequences [5]. Recent updates to the CAN protocol have attempted to address some of these vulnerabilities by incorporating features such as message authentication and encryption, but the use of those solutions is still limited.

B. Security Weaknesses in CAN

The nature of the CAN protocol as it is today have made it weak against the modern attacks. Those attacks are mainly targeting vulnerabilities that can be broadly categorized into the following types:

- Message Spoofing or Injection: In a message spoofing attack, the attacker injects counterfeit messages into the CAN bus, to imitate the presence of an ECUs. The fake ECU can take control over several critical functions such as breaking, fuel injection and door lock management leading to a serious damage. The broadcast nature of CAN means that all ECUs receive the spoofed message, and without authentication, they may accept and act upon it. For example, in 2015, researchers demonstrated a spoofing attack that allowed them to remotely control a Jeep Cherokee's steering and braking systems [6].

- Eavesdropping: CAN messages are transmitted as plaintext, this mean that those messages are not encrypted, thus can be read by anyone having access to the network, allowing him to analyze and reverse engineer those messages. Eavesdropping attacks are taken advantage of this weakness and with a deep understanding of the vehicle functions via the reverse engineering, the attackers can create sophisticated attacks. A notable case involved researchers intercepting CAN messages to understand and manipulate the behavior of a Tesla Model S [7].
- Denial of Service (DoS) Attacks: A DoS attack is an attack that use flood of high priority messages that disturbs the normal communication between the ECUs. This can lead to critical failures, such as disabling safety systems or causing the vehicle to operate in an unsafe manner. In 2016, a DoS attack was demonstrated on a Nissan Leaf, where the vehicle's climate control system was disabled by flooding the CAN bus with messages [8].

C. The role of Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDS) is one of the main protection methods used to enhance the security of CAN networks. IDS can be classified into two categories: network-based IDS (NIDS) and host-based IDS (HIDS). In the automotive industry, NIDS are strongly deployed due to it network monitoring properties, that can detect the patterns representing a potential attack [9].

a) Detection Mechanisms: Several detection mechanisms are used to identify potential threats. Signature-based detection is a technique that compare the network traffic monitored in real time with a predefined database of known attacks signatures. This technique is effective against known attacks but may struggle or even ignore attacks, which are not yet cataloged in the signature database. In the other hand, anomaly-based detection refers to a baseline of the normal network behavior and flags any message that represent a deviation from this baseline. This method is more effective at detecting new and unknown attacks but may produce a higher rate of false positives.

b) Response Strategies: Apart from detecting potential attacks, IDS can take various actions to mitigate the risk. The simplest one is alerting the system and log the potential attack for future analysis, more sophisticated action can be done, such as isolating affected ECUs from the network. The more accurate the system, the faster it responds. Additionally, integrating IDS with other security measures, such as encryption and secure boot, can provide a more comprehensive security solution. This integration ensures that even if an intrusion is detected, the data remains protected, and the system can recover securely.

III. Current State of the Art

A. Overview of IDS Techniques

Several studies have been done to develop IDS for CAN network and each approach has its own strengths and limitations. The following sections provide an overview of the most employed IDS techniques.

- Signature Based Detection: Signature based IDS is a technique that refer to a baseline of known attacks and monitor the network traffic to catch any message that has a similarity to an attack present in this baseline [10]. When talking about known attacks this technique is considered highly effective. However, it is less effective against unknown and new attacks that do not match any existing signatures. So, to remain effective the signature database should be updated whenever a new attack has been discovered.
- Anomaly Based Detection: This technique is based on a baseline that represent the network normal behavior and monitor the traffic to detect any deviation. So, any deviation will be considered suspicious and can be a potential attack [11]. This approach is considered effective against new and unknown attacks, as it does not rely on predefined signatures. However, anomaly-based IDS can be tricky due to the high false positives rate, because even small deviation not related to any kind of attacks can be misinterpreted as malicious.
- Machine Learning Based Detection: IDS empowered with machine learning (ML) algorithms has become increasingly present in the recent years. Those ML models are trained on large datasets of normal and abnormal network traffics with different message patterns that distinguish between normal a malicious frame [12]. A well-trained model with a high accuracy can enhance strongly the detection efficiency of the IDS and reduce the false positives rate. However, the reliability of ML based IDS depends strongly on the dataset quality and size, also the deployment of such IDS require high performance hardware that can easily increase the development costs.

B. Recent Advances and Innovations in IDS for CAN Network

Recent research in IDS for CAN network were mainly focused on improving detection accuracy, reducing false positives rate and enhancing the detection ability for the new and unknown attacks. Below are some relevant solutions that can enhance the CAN network safety:

- Entropy Based Anomaly Detection: The sequence of random CAN frames is measured to identify deviation from normal traffic patterns or frames sequence. This technique is based on the entropy analysis of the identifier field in a CAN frame, so by measuring the identifier bits sequence randomness the system can detect potential attacks such as CAN message injection or DoS attacks [13]. While comparing to Signature based IDS, the Entropy based one is more effective.
- Voltage Based IDS: This approach focusses on the monitoring of the CAN physical layer by detecting unusual changes in CAN bus characteristics such as voltage levels. Voltage based IDS can strongly limit network injection attacks due to its nature, that for sure will alter the voltage levels on the bus, this makes it difficult for the attackers to conceal such attacks [14].
- Deep Learning for IDS: Intrusion Detection System empowered with deep learning models demonstrated a promising horizon in the detection of new, unknown and sophisticated attacks by identifying

complex patterns that are rapidly increasing. Deep learning-based IDS can revolutionize the way CAN network is protected today, adding a new security level to the existing techniques that continuously learn and improve over time. In [15] the authors built an IDS that utilize a driver classification-based model combining Long Short-Term Memory (LSTM) networks and Fully Convolutional Networks (FCN). This approach integrates spatial and temporal learning with enhanced feature selection using Squeeze and Excite (SnE) layers and attention mechanisms. Evaluated on HCRL and test datasets, it achieved 99.36% and 96.36% accuracy, improving baseline performance by 4.18% and 13.99%.

IV. Challenges Facing current IDS Implementation

While IDS has significantly improved the CAN network security by providing various protection mechanisms, there still several challenges to be overcome to improve further the CAN protocol security:

- High False Positive Rates: As we have seen previously in our study, Anomaly based IDS is known for its effectiveness to detect new and unknown attacks but suffer from the high positives rate that can easily mislead the system with false alerts, leading to a reduction of the overall efficiency of the IDS.
- Resource Constraints: ECUs development rely strongly to the real time constraints that take in consideration the power consumption, memory limitation and CPU loads, plus the limited development and deployment costs allocated to the vehicle project. Therefore, IDS solutions with high complexity would be difficult to implement. This limitation implies to create lightweight and efficient IDS solutions that can meet the automotive environment constraints.
- Adaptability to Evolving Threats: Attacks are rapidly evolving, and attackers are constantly finding their way to discover and develop new attacks that overcome the actual solutions, this puts the IDS in a serious challenge and push the researchers to think and innovate new solutions, since many existing ones are designed to detect known attack patterns and may struggle to identify new, sophisticated threats. Developing IDS that can adapt to emerging threats in real time remains a critical area of research.
- Integration with Other Security Mechanisms: Indeed, IDS is alone not enough to ensure a complete security setup for the vehicle. IDS should be added up with other mechanisms such as encryption, secure boot, and hardware security modules. Ensuring seamless integration without introducing additional vulnerabilities is a complex task.

Table 1 provides a comparative analysis of IDS techniques used in CAN networks. Signature-based IDS demonstrates high detection accuracy for known attacks, with a low false-positive rate, making it ideal for scenarios with established attack patterns. Anomaly-based and machine learning-based techniques, on the other hand, offer enhanced protection against new threats but require vehicleeful tuning to mitigate high false-positive rates. Voltage and entropy-based methods, though promising, are in their early development stages and may need further refinement to ensure effective deployment in automotive systems.

TABLE 1. PERFORMANCE COMPARISON OF IDS TECHNIQUES

IDS Technique	Detection Accuracy	False Positive Rate	Computational Complexity
SIGNATURE BASED	HIGH (FOR KNOWN ATTACKS)	LOW	LOW
ANOMALY BASED	VARIABLE	HIGH	MODERATE
MACHINE LEARNING BASED	HIGH (BASED ON THE MODEL ACCURACY)	VARIABLE	HIGH
VOLTAGE BASED	HIGH	HIGH	MODERATE
ENTROPY BASED	MODERATE	MODERATE	LOW

Table 2 highlights the advantages and limitations of various IDS approaches. Signature-based IDS performs well for detecting familiar attacks but lacks the adaptability of machine learning-based IDS, which continuously learns and adjusts to new threats. Anomaly-based IDS, while valuable for unknown threat detection, faces challenges in minimizing false positives. This comparison underscores the importance of choosing an IDS technique that best aligns with automotive network requirements, balancing detection accuracy with computational efficiency.

TABLE 2. ADVANTAGES AND LIMITATIONS OF IDS TECHNIQUES

IDS Techniques	Key Advantages	Key Limitations
SIGNATURE-BASED	EFFECTIVE FOR KNOWN ATTACK PATTERNS	STRUGGLES WITH ZERO-DAY ATTACKS
ANOMALY-BASED	DETECTS UNKNOWN ATTACKS	HIGHER FALSE POSITIVES
MACHINE LEARNING-BASED	ADAPTABLE TO NEW THREATS	REQUIRES SUBSTANTIAL TRAINING DATA
ENTROPY-BASED	DETECTS MESSAGE ANOMALIES	MAY MISS SUBTLE ATTACKS
VOLTAGE-BASED	EFFECTIVE AT PHYSICAL-LAYER ATTACK DETECTION	SENSITIVE TO PHYSICAL VARIATIONS, REQUIRING CALIBRATION

V. Research Gaps and Future Directions

The literature review in this article provides a comprehensive analysis of the vulnerabilities inherent in the CAN protocol and evaluates existing IDS approaches designed to address these issues. It identifies critical shortcomings in current IDS methods, such as high false positive rates, difficulty in adapting to evolving threats, and challenges in integrating IDS with other security measures. Furthermore, the review highlights opportunities for future research, including the development of lightweight, resource-efficient IDS, real-time adaptive algorithms, and standardized benchmarks for comparing IDS performance:

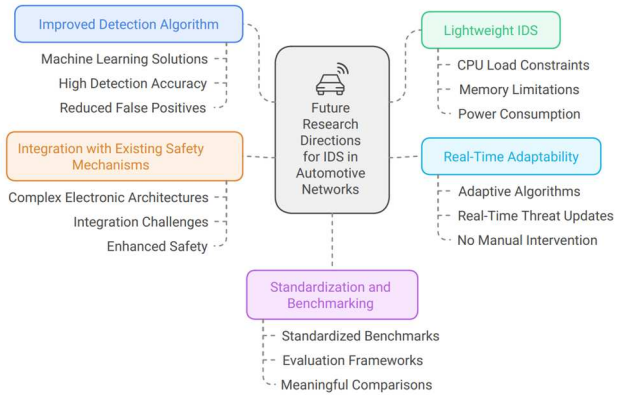

Fig. 1. Future Research Directions for Intrusion Detection Systems (IDS) in Automotive Networks.

A. Improved Detection Algorithm

Now with the presence of machine learning based solutions combined with IDS that showed a promising result, has opened an all area of research that can explore further solution based on machine and deep learning models that may offer high detection accuracy with a reduction of false positives rate.

B. Lightweight IDS

Research should focus on developing lightweight IDS that can meet the automotive environment constraints, which indeed is a challenging task due to the requirements related to CPU load, memory limitation and power consumption.

C. Real Time Adaptability

The need of an adaptive IDS that can track the constant evolution of attacks in real time is becoming crucial to maintain an efficient protection system. Future research should investigate adaptive algorithms that can update their detection models in response to emerging threats without requiring manual intervention.

D. Integration with existing safety mechanisms

As mentioned previously, IDS solutions should be added up with other safety mechanism already integrated in the vehicle, and knowing the complexity that electronic and electric architectures has reached today due to the sophisticated features present in today's vehicles has made this integration quite challenging. This led us to say that research in the future that will improve that aspect will be very useful and beneficial.

E. Standardization and Benchmarking

The lack of standardized evaluation metrics for IDS in automotive networks has made it difficult to compare the effectiveness of different solutions. Future research should focus on developing standardized benchmarks and evaluation frameworks that can facilitate meaningful comparisons between IDS technologies.

VI. Conclusion

The increasing connectivity of modern vehicles has underscored the need for robust security measures to protect automotive networks from cyber threats. The CAN protocol, while integral to vehicle communication, suffers from several vulnerabilities that expose it to various attacks. Intrusion Detection Systems (IDS) represent a critical defense mechanism for safeguarding these networks. This paper has reviewed the current state of IDS technologies for CAN networks, identified key research gaps, and proposed future directions for improving the effectiveness of IDS in automotive security. As the automotive industry continues to evolve, ongoing research in this area will be essential to ensuring the safety and security of connected vehicles.

References

[1] K. Koscher et al., "Experimental Security Analysis of a Modern Automobile," 2010 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2010, pp. 447-462.

[2] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," *Proc. 20th USENIX Security Symp.*, San Francisco, CA, USA, Aug. 2011. [Online].Available: https://www.usenix.org/conference/usenix-security-11/comprehensive-experimental-analyses-automotive-attack-surfaces.

[3] T. Hoppe, S. Kiltz, and J. Dittmann, "Applying intrusion detection to automotive IT: early insights and remaining challenges," J. Inform. Assur. Secur., vol. 4, no. 6, pp. 226–235, 2009.

[4] Bosch, R. (1991). "CAN Specification Version 2.0." Robert Bosch GmbH, Stuttgart, Germany.

[5] C. P. Andel, T. R. Yampolskiy, and J. T. McDonald, "In-vehicle networks: Attacks, vulnerabilities, and proposed solutions," in Proc. 10th Annu. Cyber Inf. Secur. Res. Conf., Oak Ridge, 2015, p. 1.

[6] Miller, C., & Valasek, C. (2015). Remote Exploitation of an Unaltered Passenger Vehicle. Presented at Black Hat USA2015.Retrievedfromhttps://www.blackhat.com/docs/us-15/materials/us-15-Miller-Remote-Exploitation-Of-An-Unaltered-Passenger-Vehicle.pdf

[7] NIE, Sen, LIU, Ling, et DU, Yuefeng. Free-fall: Hacking tesla from wireless to can bus. *Briefing, Black Hat USA*, 2017, vol. 25, no 1, p. 16.

[8] T. Hunt, "Controlling Vehicle Features of Nissan," Troy Hunt's Blog, Feb. 2016. [Online]. Available: https://www.troyhunt.com/controlling-vehicle-features-of-nissan/[Accessed: Nov. 17, 2024].

[9] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," J. Netw. Comput. Appl., vol. 84, pp. 25–37, 2017.

[10] S. Jin, J.-G. Chung, and Y. Xu, "Signature-Based Intrusion Detection System (IDS) for In-Vehicle CAN Bus Network," in Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), 2021, pp. 1–5.

[11] M. L. Han, B. I. Kwak, and H. K. Kim, "Anomaly intrusion detection method for vehicular networks based

on survival analysis," Vehicular Communications, vol. 14, pp. 52–63, 2018.

[12] M. Hanselmann, T. Strauss, K. Dormann, and H. Ulmer, "CANet: An Unsupervised Intrusion Detection System for High Dimensional CAN Bus Data," IEEE Access, vol. 8, pp. 58194–58205, 2020.

[13] Q. Wang, Z. Lu, and G. Qu, "An Entropy Analysis-Based Intrusion Detection System for Controller Area Network in Vehicles," 2018. [Online]. Available: https://doi.org/10.48550/arXiv.1808.04046.

[14] Choi, Wonsuk & Joo, Kyungho & Jo, Hyo & Park, Moon & Lee, Dong. (2018). VoltageIDS: Low-Level Communication Characteristics for Automotive Intrusion Detection System. IEEE Transactions on Information Forensics and Security. PP. 1-1.

[15] J. A. Khan, D. -W. Lim and Y. -S. Kim, "A Deep Learning-Based IDS for Automotive Theft Detection for In-Vehicle CAN Bus," in IEEE Access, vol. 11, pp. 112814-112829, 2023