International Journal of Interpreting Enigma Engineers (IJIEE)

https://ejournal.svgacademy.org/index.php/ijiee/

OPEN ACCESS

ANALYZING THE CAN PROTOCOL: VULNERABILITIES, PROTECTIVE MEASURES AND IMPROVEMENTS

Mahender Reddy Bobbala[1][0009-0003-9018-1502] and Dr. R. Kavitha[2][0000-0001-9542-3273]

Original Article

[1]Assistant Professor, Department of Information Technology, Maturi Venkata Subbarao(MVSR) Engineering college, Nadergul Hyderabad, Telangana, India

[2]Associate Professor, Department of Computer Science & Engineering, Siddhartha Institute of Engineering & Technology, Ibrahimpatnam,Rangareddy, Telangana, India

*Corresponding Author's Email: [1]mahi.bobbali@gmail.com and [2]r.kavitha@siddhartha.ac.in

Abstract

The Controller Area Network (CAN) bus, originally designed for internal communication among a limited number of Electronic Control Units (ECUs) within vehicles, faces significant security challenges due to the rapid expansion of ECUs in modern automobiles. This expansion necessitates accessibility for diagnostic purposes, yet the CAN protocol lacks fundamental security features such as encryption, authentication, and integrity checks, rendering it vulnerable to various attacks including message injection, Denial of Service (DoS), and masquerading ECUs. This paper surveys existing literature and investigates potential intrusions on the CAN bus, highlighting attacks ranging from GPS spoofing to remote sensor tampering. Various solutions are discussed, including network subdivision, encryption, authentication techniques, and intrusion detection systems (IDS). Recent research proposes IDS solutions utilizing machine learning algorithms such as Random Forest, Support Vector Machine, and Deep Neural Networks (DNN), demonstrating effectiveness in detecting known attacks. However, challenges persist in identifying unknown attacks and enhancing overall system performance. Innovative approaches, such as event-triggered detection and bloom filtering techniques, show promise in mitigating specific attack vectors but may introduce overhead or limitations in real-time response. Deep learning-based IDS systems exhibit high performance but struggle with the detection of novel attacks. Furthermore, while some solutions address specific vulnerabilities, others propose more comprehensive security measures, such as preventing remote manipulation of critical vehicle functions like steering and braking. Overall, the research emphasizes the critical need for robust security measures in automotive systems to safeguard against evolving threats to vehicle safety and integrity.

Keywords: CAN; ECUs; vehicles security; IDS; machine learning algorithms, vehicle safety

Introduction

Modern vehicles are outfitted with numerous Electronic Control Units (ECUs), sensors, actuators in vehicles like cars, responsible for managing their communication, electrical systems, thereby enhancing driving comfort and safety [1][3]. These ECUs manage various operations of the vehicle such as engine control, protect lock braking systems etc. To ensure safe driving, ECUs require a stable communication network. Renowned for its high resistance to electrical interference, ease of wiring, and ability to self-diagnose and repair errors, the CAN is well-suited for the automotive industry.

CAN is also adapted in aviation, robots and driverless vehicles. Despite CAN's resilience to electrical disturbances and inclusion of some security features, it remains susceptible to attacks. Given the increasing concern for system security, extensive research is being conducted to identify vulnerabilities in CAN and propose potential solutions. Several studies are executed on attacks on cars, with many of these attacks requiring physical access to the bus. However, the prevalence of wireless attacks is on the rise, particularly with the introduction of new wireless interfaces such as vehicle-to-vehicle and vehicle-to-infrastructure connections. It is anticipated that wireless attacks will emerge as the primary attack in future. This paper explores into the critical topic of **automated cars security**, focusing on the **CAN protocol**. It aims to illuminate the inherent vulnerabilities present in modern cars equipped with CAN, potentially exposing them to cyber-attacks.

By comprehensively analyzing the security issues, the paper seeks to empower readers with crucial knowledge. Furthermore, it examines into existing literature to present a **variety of possible solutions** that could mitigate these vulnerabilities, ultimately enhancing the security in modern vehicles.

The Section B outlines the CAN protocol and it structure. In Section C discusses the challenges, gaps and suggestion for CAN protocol. The Section D briefs the work and concludes the paper.

Controller Area Network Protocol

The CAN protocol has become a foundation protocol for vehicle communication. This robust protocol allows multiple devices, known as "nodes," to share information seamlessly across a single, twisted-pair cable. The key features of CAN are: i) Multi-master: Any node can initiate communication, promoting flexibility and adaptability. ii) Broadcast network: All nodes receive all messages, simplifying network design and reducing wiring complexity iii) High-speed data transfer: The CAN bus can transmit data at up to 1 Mbps, ensuring efficient information exchange. iv)Electromagnetic interference (EMI) immunity: Robust design protects against electrical noise, crucial in the harsh automotive environment. v)Self-diagnosis and error correction: Built-in mechanisms detect and resolve errors, enhancing system reliability and vi) Distributed architecture: Nodes handle tasks independently, simplifying maintenance and lowering overall system costs.

The CAN frame structure is depicted in Fig. 1. It has eight fields. Start of Frame (SOF – 1 bit) field indicates start of frame, arbitration (12 bits) field tells the priority of the frame, control (6 bits) field has two parts - r0,r1 (2 bits) and DLC(4 bits), r0,r1 bits used for future use and DLC is data length code, data(64 bits) field is for actual data and offset, Cyclic Redundancy Code (CRC – 16 bits) is for checking the integrity of the message, acknowledgment (ACK – 1 bit) and DEL (1 bit) is for reception of the message, End of Frame (EOF – 7 bits) indicates end of the frame and Inter Frame Space fields(3 bits) tells about the idle time.

Fig. 1 Structure of CAN fame

1 bit	12 bits	6 bits	64 bits	16 bits	2 bits		7 bits	3 bits
SOF	Arbitration	Control	Data	CRC	ACK	DEL	EOF	Inter Frame Space

The error checking methods of CAN are Start of Frame (SOF), Cyclic Redundancy Check (CRC), Acknowledgement (ACK) Bits, Bit Stuffing, End of Frame (EOF). SOF is a single dominant bit for synchronization which signals start of the frame and syncs all nodes. CRC is used for data integrity. ACK bits informs about reception of data. Bit stuffing ensures synchronization and error detection. EOF marks end of frame and aids in detection of missing bits. Error detection and collision resolution work together in CAN to guarantee data integrity and efficient communication. The CAN bus prioritizes error detection over real-time performance, as corrupted data can have more severe consequences. Other error handling mechanisms exist, such as acknowledgment frames and message timeouts, further enhancing data reliability.

Literature Review

Security wasn't a major concern for the CAN bus when it was designed. Back then, it connected a handful of Electronic Control Units (ECUs) within a vehicle, primarily for internal communication and not user interaction. As there is drastic change in automobile industry has increased usage of ECUs, so it has become mandate that it should be accessible for diagnosis [2]. While CAN has many developments such as high data transfer rates and extended addressing still it suffers from security features like encryption, authentication, integrity checks, message injection, DoS (Denial of Service) where authenticated users are not allowed to access services and messages doesn't reach the destination, masquerading ECUs.

CAN intrusion detection extensively address the issues related with CAN because of its broadcast feature. We have studied surveys on CAN from [5-6], [8-10] existing literature. In [4,7], various intrusion that could occur in the vehicles are examined. Apart from the issues in security features mentioned above other attacks could be GPS spoofing which is caused by sending false messages, location tracking, close contiguity issue like accessing through Bluetooth, key fob [15], replay attack occur in key agreement protocol, fuzzing, flooding, impersonation attack is designed by using fake identity, routing, sniffing, fabricated information attack where opponent sends false information [11-14].The most predominant attack caused is remote sensor attack on vehicles camera and sensors.

The attacks on CAN bus are investigated and some solutions are discussed. The solutions can be categorized as network subdivision, encryption techniques, authentication approaches, and intrusion detection systems.

The security of vehicles is highly needed as CAN is prone to attacks. For example, to address the attack on network an intrusion detection system could be created as a solution. In [17], the authors proposed intrusion detection system in vehicles using the CAN bus protocol. Random Forest, Support Vector Machine, Multilayer Perceptron and Decision Tree classifiers are engaged to identify actual and malicious communications. These four algorithms could detect the know attacks but at the cost of high resource utilization. Thus the work could be extended by considering large number of data sets for identifying new and unknown attacks.

A technique called as event triggered is proposed in [18], to identify the vehicle model which could detect fuzzy and replay attacks. The proposed method has used tree based machine learning model and evaluated the accuracy and time. But the models accuracy can be improved to some more extent. The authors of [19] have proposed a method to determine the delay between request for frame and response and created IDS. With the delay, the method could conclude on normal or abnormal behavior of the communication. The proposed method has detected DoS, impersonation and fuzzy attacks but lacked in performance.

There is an effective method that was developed in [23] to overcome the device impersonation and disallowing of transmitted messages of authentic ECU. The robustness is achieved but to thirty percent in identifying malicious ECU. Recurrent Neural Network – RNN, Neural Networks and network traffic signatures are used in [20], have detected DoS, fuzzy and replay attacks. The proposed technique has resulted in high accuracy but could not identify unknown attacks.

In [16], an intrusion detection system for CAN using deep learning was proposed. The system used the combination of CNN and LSTM to identify a series of message attacks but has failed to identify the malicious nodes discharging unknown attacks. The authors of [21] proposed a brilliant system which hacks a car by disabling its steering and brake operation remotely. However, this system could be applied to existing vehicles not for the newly updated ones.

In [15] authors have developed bloom filtering technique which identifies frame modification attack. This method works on FID (frame identifier) and data fields to examine frame density. The performance of this method is very high as it provides cent percent recall rate. The deficiency of this method is that it affects the timely reply as an overhead is

included on ECU. Deep learning methods were used to find the differences between known and unknown attack. The IDS in CAN was developed in [22] using DNN. The DNN based system has exceled in its performance.

Table 1: Intrusion Detection System(IDS) for CAN bus

Key References	Attacks	Methods
Alshammari A, Zohdy M.A, Debnath D, and Corser G.[7]	DoS and the Fuzzy attacks	KNN and SVM
Almaraz-Rivera,J.G, Perez-Diaz J.A, and Cantoral-Ceballos J.A [11]	Distributed Denial of Service (DDoS) attacks	Decision Tree and the Random Forest
Groza, B.; Murvay, P.S. [15]	replay or modification attacks	Bloom filters
Narayan Khatri , Sihyung Lee ,Seung Yeob Nam, [16]	DoS attacks, Fuzzy attacks, impersonation attacks, and replay attacks	Hybrid TL model
Mee Lan Han , Byung Il Kwak , and Huy Kang Kim [18]	malicious packet attacks	decision tree classifier (DTC), a random forest classifier (RFC), and XGBoost..
Shahroz Tariq, Sangyup Lee, Huy Kang Kim, and Simon S. Woo [20]	DoS, fuzzy, and replay attacks	Recurrent Neural Networks (RNNs)
Kang, M.J.; Kang, J.W. [22]	malicious attack	deep neural network (DNN)
Wassila, Wassila Lalouani, Yi Dang, Mohamed Younis [23]	message spoofing and masquerading	voltage-based fingerprint
HM Song, J Woo, HK Kim [4]	message injection attacks	deep convolutional neural network (DCNN)

Results and Discussion

Table2:1 Comparison based on machine algorithms used and their metrics

Key References	Machine Learning Algorithms	Precision	Recall	F1	Accuracy
Hyun Min Song, Jiyoung Woo, Huy Kang Kim(2019) [4]	DCNN	0.9762	0.8681	0.9776	99%
Abdulaziz Alshammari, Mohamed A. Zohdy, Debatosh Debnath, George Corser (2018)[7]	KNN	0.999	0.965	0.935	97%
Moulahi, T.; Zidi, S.; Alabdulatif, A.; Atiquzzaman, M (2021) [17]	SVM	0.972	0.998	0.9852	97%
Han, M.L.; Kwak, B., II; Kim, H.K (2021) [18]	Decision tree	0.989	0.987	0.988	99%

In the previous section, we presented an investigation into a diverse array of intrusion detection methods within the CAN bus system, uncovering several pivotal issues that warrant attention in guiding future research endeavors aimed at enhancing Intrusion Detection Systems (IDS) for the automotive domain.

Our investigation reveals that the preference for an anomaly-based approach in CAN packet IDS stems from inherent constraints and limitations. The proprietary nature of the CAN protocol poses challenges for adopting signature or specification-based methods, which rely on semantic understanding of CAN packets and may struggle with protocol variations. Anomaly detection, leveraging learning-based techniques, emerges as a viable solution due to its capacity to adapt intelligently to the CAN environment, irrespective of protocol, vehicle model, and year.

Additionally, many of the techniques discussed above, particularly those employing machine learning-based anomaly detection, rely on supervised or semi-supervised approaches. While these methods achieve notable accuracy levels, they necessitate fully labeled data—a challenging endeavor, particularly in real-time CAN environments where data is generated rapidly. Labeling data in such scenarios requires human expertise and is highly time-consuming. Consequently, leveraging unlabeled CAN data in an unsupervised manner emerges as a preferable and more practical approach for anomaly detection.

Conclusion

This paper presents an examination of the CAN protocol and its challenges in security. A range of efforts has been put to address the issues and a variety of gaps are identified so that it helps the readers to fill the gap as a part of research.

References

1. P. Mundhenk, Security for Automotive Electrical / Electronic (E / E) Architectures. Cuvillier Verlag, 2017.
2. R. Buttigieg, M. Farrugia, and C. Meli, “Security Issues in Controller Area Networks in Automobiles,” in 18th international conference on Sciences and Techniques of Automatic Control & Computer Engineering, 2017, pp. 21–23.
3. ECU is a Three Letter Answer for all the Innovative Features in Your Car: Know How the Story Unfolded, Embitel, 2017. [Online]. Available: https://www.embitel.com/blog/embeddedblog/automotive-control-units-development-innovationsmechanical-to-electronics. [Accessed: 23-May-2018].
4. Song, H.M.; Woo, J.; Kim, H.K. In-Vehicle Network Intrusion Detection Using Deep Convolutional Neural Network. Veh. Commun. 2020, 21, 100198. [CrossRef]
5. C. Young, J. Zambreno, H. Olufowobi, and G. Bloom, “Survey of automotive controller area network intrusion detection systems,” IEEE Design Test, vol. 36, no. 6, pp. 48–55, Dec. 2019, doi: 10.1109/MDAT.2019.2899062.
6. S.-F. Lokman, A. T. Othman, and M.-H. Abu-Bakar, “Intrusion detection system for automotive controller area network (CAN) bus system: A review,” EURASIP J. Wireless Communication Network., vol. 2019, no. 1, p. 184, Jul. 2019, doi: 10.1186/s13638-019-1484-3.
7. Alshammari, A.; Zohdy, M.A.; Debnath, D.; Corser, G.; Alshammari, A.; Zohdy, M.A.; Debnath, D.; Corser, G. Classification Approach for Intrusion Detection in Vehicle Systems. Wirel. Eng. Technol. 2018, 9, 79–94
8. H. J. Jo and W. Choi, “A survey of attacks on controller area networks and corresponding countermeasures,” IEEE Trans. Intell. Transp. Syst., vol. 23, no. 7, pp. 6123–6141, Jul. 2022, doi: 10.1109/TITS.2021.3078740.
9. B. Lampe and W. Meng, “A survey of deep learning-based intrusion detection in automotive applications,” Expert Syst. Appl., vol. 221, Jul. 2023, Art. no. 119771, doi: 10.1016/j.eswa.2023.119771.
10. Buscemi, I. Turcanu, G. Castignani, A. Panchenko, T. Engel, and K. G. Shin, “A survey on controller area network reverse engineering,” IEEE Commun. Surveys Tuts., early access, Apr. 5, 2023, doi: 10.1109/COMST.2023.3264928
11. Almaraz-Rivera, J.G.; Perez-Diaz, J.A.; Cantoral-Ceballos, J.A. Transport and Application Layer DDoS Attacks Detection to IoT Devices by Using Machine Learning and Deep Learning Models. Sensors 2022, 22, 3367

12. Palanca, A.; Evenchick, E.; Maggi, F.; Zanero, S. A Stealth, Selective, Link-Layer Denial-of-Service Attack against Automotive Networks. In Proceedings of the 14th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2017, Bonn, Germany, 6–7 July 2017; Volume 10327, pp. 185–206.
13. Murvay, P.S.; Groza, B. Security Shortcomings and Countermeasures for the SAE J1939 Commercial Vehicle Bus Protocol. IEEE Trans. Veh. Technol. 2018, 67, 4325–4339.
14. 41. Gutierrez, C.N.; Kim, T.; Corte, R.D.; Avery, J.; Goldwasser, D.; Cinque, M.; Bagchi, S. Learning from the Ones That Got Away: Detecting New Forms of Phishing Attacks. IEEE Trans. Dependable Secur. Comput. 2018, 15, 988–1001.
15. Groza, B.; Murvay, P.S. Efficient Intrusion Detection with Bloom Filtering in Controller Area Networks. IEEE Trans. Inf. Forensics Secur. 2019
16. Narayan Khatri , Sihyung Lee ,Seung Yeob Nam, Transfer Learning-Based Intrusion Detection System for a Controller Area Network, IEEE Access, Vol 11,2023, Digital Object Identifier 10.1109/ACCESS.2023.3328182
17. Moulahi, T.; Zidi, S.; Alabdulatif, A.; Atiquzzaman, M. Comparative Performance Evaluation of Intrusion Detection Based on Machine Learning in In-Vehicle Controller Area Network Bus. IEEE Access 2021, 9, 99595–99605
18. Han, M.L.; Kwak, B., II; Kim, H.K. Event-Triggered Interval-Based Anomaly Detection and Attack Identification Methods for an In-Vehicle Network. IEEE Trans. Inf. Forensics Secur. 2021,
19. Lee, H.; Jeong, S.H.; Kim, H.K. OTIDS: A Novel Intrusion Detection System for in-Vehicle Network by Using Remote Frame. In Proceedings of the 2017 15th Annual Conference on Privacy, Security and Trust, PST 2017, Calgary, AB, Canada, 28–30 August 2017; Institute of Electrical and Electronics Engineers Inc.: Piscataway Township, NJ, USA, 2018; pp. 57–66.
20. Tariq, S.; Lee, S.; Kim, H.K.; Woo, S.S. Detecting In-Vehicle CAN Message Attacks Using Heuristics and RNNs. In Information and Operational Technology Security Systems; Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer: Berlin/Heidelberg, Germany, 2019; Volume 11398, pp. 39–45
21. Miller, C.; Valasek, C. Remote Exploitation of an Unaltered Passenger Vehicle. Black Hat USA 2015, 2015 (Suppl. 91), 1–91
22. Kang, M.J.; Kang, J.W. Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security. PLoS ONE 2016, 11, e0155781
23. Wassila, Wassila Lalouani, Yi Dang, Mohamed Younis, Mitigating voltage fingerprint spoofing attacks on the controller area network bus. Clust. Comput. 26(2): 1447-1460 (2023)