INTERNATIONAL JOURNAL OF INFORMATION TECHNOLOGY RESEARCH STUDIES (IJITRS)
(Open Access, Double-Blind Peer Reviewed Journal)
ISSN Online: ISSN Print

The Evolution of In-Vehicle Intrusion Detection Systems through Deep Learning: A Systematic Study

Vismaya K K, Department of Computer science, Faculty of science and humanities, SRM IST Kattangulathur, Chennai, India.
P.J Arul Leena Rose, Department of Computer science, Faculty of science and humanities, SRM IST Kattangulathur, Chennai, India.

Article information
Received: 17th January 2025
Received in revised form: 5th February 2025
Accepted: 26th March 2025
Available online: 30th April 2025
Volume: 1
Issue: 1
DOI: https://doi.org/10.5281/zenodo.15309382

Abstract
The security of in-vehicle networks is jeopardized by the advancement of sophisticated automotive electronics. Historically, intrusion detection systems have been employed to safeguard these networks. Nevertheless, they cannot recognize advanced dangers; hence, recent advancements in artificial intelligence provide more refined and efficient detection systems. This systematic study emphasizes the shift from traditional methods to deep learning, examining the latest deep learning-based intrusion detection systems for in-vehicle networks. We assess the efficacy of various deep learning-based intrusion detection systems in detecting and preventing cyberattacks, including denial-of-service and spoofing, by examining their applicability, performance metrics, advantages, and disadvantages. The future of DL in in-vehicle security is also examined in our assessment, which suggests possible lines of inquiry

Keywords: - Deep Learning (DL), Intrusion Detection System (IDS), Electronic Control Unit (ECU), Controller Area Network (CAN)

I. INTRODUCTION

Cybersecurity has gained paramount significance as the automobile sector advances with connected and autonomous vehicles.

With electronic control units and sensors that communicate regularly with networks like the Controller Area Network, cars are becoming complex networks on wheels rather than merely mechanical devices. A number of cybersecurity issues have been brought to light by the increasing integration of contemporary automotive technology, such as Electronic Control Units (ECUs) and Controller-Area-Network (CAN bus).

The understanding of these concerns has heightened interest in the implementation of intrusion detection systems in automobile environments. While standard intrusion detection systems are essential, dynamic automotive environments and the ever-evolving complexity of intrusions can occasionally undermine their efficacy. To address this, deep learning-based intrusion detection systems are gaining popularity.

They are effective at detecting harmful intrusions and can quickly adjust to the changing automobile environment. With deep learning models offering promising detection skills and the ability to identify novel threats, the introduction of DL adds a new dimension to the in-vehicle IDS area. This review analyzes and synthesizes the literature on deep learning-based intrusion detection systems for in-vehicle networks.

To give a synopsis of in-vehicle network safety and to showcase the most recent developments in intrusion detection systems based on deep learning techniques, this study suggests a review. Our research revolves around

gaining a better understanding of how DL is being used to enhance cyberattack identification and avoidance in modern cars.

II. BACKGROUND

A. Importance Of Cybersecurity In Modern Vehicles

The significance of cybersecurity has increased due to the integration of advanced technologies in modern vehicles. Modern vehicles are equipped with autonomous driving capabilities, telematics, and connected technology, generating substantial volumes of data. This connectivity improves comfort and convenience by facilitating diagnostics, updates and advanced techniques that enhance the driving experience. Nonetheless, the increasing dependence on ECU and interconnectivity facilitates new threats and assaults. Unauthorized access to an automobile can control functions such as braking, steering, acceleration, and entertainment systems. Enhanced connectivity engenders potential cyberthreats, jeopardizing the safety of drivers and passengers while also undermining privacy and integrity. Researchers were able to remotely attack weaknesses in Fiat Chrysler's Uconnect system, which handles the vehicle's entertainment and navigation features, thanks to several real-world instances as the 2015 Jeep Cherokee Hack [10]. They demonstrated the possible risks of cyberattacks on automated vehicles by being able to access vital features like steering, braking, etc. The 2016 Tesla Model S hack allowed the attacker to control the braking system and unlock doors. 2018 BMW security weaknesses gave the attacker remote access to the automobile via a smartphone app, enabling them to manipulate features like unlocking doors, changing settings, and tracking the location of the vehicle..

B. Evolution Of Automotive Electronics

Table 1 illustrates the substantial advancements in automobile electronics and communication over time, which have automated driving and our interactions with cars. In the past, cars employed simple electrical systems for things like lighting and ignition, but these days, cars use advanced electronic systems for things like infotainment, lane-keeping, GPS navigation, engine control, and braking [11]. Improved safety features and autonomous driving were made possible by the increased connectivity, which also allowed cars to communicate with one another and with external infrastructure. An expansion of the Internet of Things (IoT), the Internet of Vehicles (IoV) enables data sharing between networked vehicles, infrastructure on roads, and people on foot, with the goal of developing a sophisticated system for transportation.

Comprising an IoV network are two networks of sub-net one for communication within vehicles and one for data transfer between vehicles [12].The development of more sophisticated safety systems in vehicles has allowed for the introduction of technologies such as adaptive cruise control and collision avoidance. Conventional protocols, like as CAN, have evolved to accommodate the complexities of contemporary automobiles. The advancement of automotive Ethernet technology has enabled several benefits, such as scalability, the ability to reuse protocols at the OSI layer, and the invention of new standards.

Autonomous cars frequently employ a multi-layered security architecture to guarantee the dependability and security of their operations [14].

Table 1: Evolution of Automotive Electronics

Time Period	Main Features
1800s - 1900s	Ignition, Lighting
1930s - 1940s	Vacuum Tubes, Radio
1950s - 1960s	Transistors, Fuel Injection, Cruise Control
1970s - 1980s	Microprocessors, ABS, ESC
1990s	OBD, Multiplexing, GPS
2000s	CAN Bus, ADAS, Hybrid/Electric
2010s	Infotainment, Autonomous Driving, V2V/V2I
2020s	Refined Autonomy, EV Advancements, AI/ML

C. Intrusion Detection System

Since some traditional security mechanisms, such as particular encryption and authentication techniques, may violate CAN communication timing constraints or aren't supported by CANs, they aren't suitable for IVNs. Consequently, intrusion detection systems (IDSs) have emerged as a crucial element of contemporary Internet of Vehicles (IoV) to detect hazardous threats within vehicle networks [13]. Intrusion detection systems (IDSs), a critical element of the defense infrastructure, are typically incorporated into external networks to detect malicious attempts that bypass firewalls and authentication measures. Despite various prior endeavors to develop intrusion

detection systems (IDSs) achieving some degree of success, intrusion detection remains a complex issue. The reason for this is the abundance of network-related data, the diversity of network features, and the various cyber-attack techniques [15].

In conclusion, intrusion detection systems (IDSs) are now a crucial part of any security configuration resulting from the growing reliance of individuals, organizations, and businesses on technology and information systems, as well as the rise in attacks and their potentially dangerous effects.

III. LITERATURE REVIEW

The research by Boddu et al. [1] presents an innovative intrusion detection method for intelligent transportation systems (ITS) that utilizes vehicles to detect networks and infrastructure, hence recognizing prudent network behavior within in-vehicle networks. The system utilizes an upgraded Cuttle Fish Optimized Multiscale Convolutional Neural Network (ECFO-MCNN). The primary aim of the suggested strategy is to identify forward events originating from the central network gateways of antivirus software. The proposed IDS is assessed utilizing two benchmark datasets: the car hacker dataset for in-vehicle communications and the UNSWNB15 dataset for external network communications. Enhancing anomaly detection and intrusion prevention in in-vehicle networks augments ITS security through the utilization of ECFO-MCNN IDS. SI-LSTM is vulnerable to adversarial assaults because current G-VSPAs prioritize short-term optimization at the expense of potential dangers and spatial dependencies. In the identification of hostile traffic, ECFO-MCNN outperformed SI-LSTM and G-VSPA.

Han et al. [2] assert that deep learning-based in-vehicle intrusion detection systems (IDS) have attracted significant attention within anomaly detection technologies owing to their superior efficiency and accuracy. This research primarily investigates the complex value neural network (CVNN) for the identification of CAN IDs to safeguard the CAN network.They provided an encoder that can extract shallow features using the auto-encoder approach, as well as a random phase that rotates the complex-valued domain features to hide the true characteristics. After that, the proposed processing method retrieves useful properties using an attention strategy. By introducing anomalous data into the real car, the CAN dataset was created. In real-time, the developed intrusion detection system exhibits a high accuracy of 98%. The attack experiment specifically demonstrates that the model hardly deduces anything from the adversary. The PPM-InVIDS architecture provides elevated security measures and safeguards the Controller Area Network (CaccAN) by securing in-vehicle communications using authentication and encryption methodologies.

Markus et al. [3] introduced CANet IDS, an unsupervised intense learning technique for CAN buses. It performs better than earlier approaches and can effectively handle unknown assaults and identify manipulation. An LSTM subnetwork is meant to capture temporal dependencies and improve the model's sensitivity to message sequences, ensuring strong intrusion detection capabilities. Effective information fusion and feature extraction are made possible by the integration of joint latent vectors with fully connected layers. By making sure the model is not unduly sensitive to the precise sequential order message IDs, the architecture is intended to offer flexibility in managing fluctuations in sequences of data commonly encountered in actual Controller Area Network (CAN) data. CANet has a high true negative rate—typically above 0.99—for detecting CAN bus incursions. Hossain et al. [4] presented an intrusion system for CAN bus networks based on LSTM. To train and evaluate the algorithm, they first collected threat-free data from their car, then gathered more data following the assaults. They were able to create their own dataset as a result. According to the results, they were able to detect DoS, Fuzzing, and spoofing attacks with an overall accuracy of 99.995%. The Survival Analysis for Automotive IDS dataset, developed by the Hacking and Countermeasures Research Lab in Korea, was also used to examine the LSTM model. The LSTM model outperformed the Survival Analysis approach in terms of detection rate. Only three attack types—denial-of-service (DoS), fuzzing, and spoofing—were studied.

Inoue et al. [5] proposed an Intrusion Detection System utilizing the Deep CNN Inception-ResNet architecture to mitigate CAN bus assaults. They attained a detection rate of 0.99 and an impressive accuracy of 99.9% for effective threat identification by validating the IDS with authentic automotive datasets. They created an in-vehicle network assaults dataset that included DoS, Fuzzing, and spoofing attacks since the majority of research are unable to classify fuzzy attacks. The suggested CNN-based intrusion detection system accurately recognized Fuzzing attempts. The principal limitation of this work is that the framework is just evaluated on datasets from three specific car models (Toyota, Subaru, and Suzuki), and it has not been tested on other car models or types of CAN bus traffic, hence constraining the model's generalizability.

Yang et al. [6] used two distinct datasets, 1 and 2, to propose a single GAN for intrusion detection in in-vehicles. The model outperforms the comparable works by 1-3 percent in terms of accuracy and precision. They were able to optimize the training process, resulting in excellent accuracy and a shorter training convergence time, by using various settings for datasets. The study's concentration on particular attack types, such as fuzzy, DoS,

gear, and RPM attacks, restricts the model's potential to be used broadly. Additionally, they don't address the drawbacks of using GAN-based IDS in practical situations.

Ullah et al. [7] proposed the use of long short-term memory (LSTM) and gated recurrent unit (GRU) for a hybrid intrusion detection system, utilizing SMOTE to balance the dataset. Two datasets were utilized to evaluate the effectiveness of the proposed method: one for automotive hacking and another for a composite DDoS dataset that included CSE-CIC-IDS 2018, CIC DoS, and CI-CIDS 2017. The testing findings indicate that the proposed method achieves an accuracy of 99.5% for DDoS attacks and 99.9% for automobile hacks.

The study has a few limitations, including that it does not compare the model's efficacy with other state-of-the-art IDS that are currently in use. Additionally, the publication mentions using SMOTE to balance the datasets but does not explain limitation of using SMOTE.

Song et al. suggested an intrusion detection system (IDS) utilizing a deep convolutional neural network (DCNN) [8]. The DCNN autonomously studies network traffic rhythms and identifies malicious activity without the necessity for manually crafted features.They were able to achieve a high detection rate while removing unnecessary complexity from the ReSNet model's design. The detection method was applied to real-world automobile datasets. The suggested DCNN-based IDS performs better than LSTM, ANN, SVM, kNN, NM, and decision trees in detecting message injection threats in automobiles. Future research attempts to improve DCNN for unknown attack types since the study falls short in detecting unlearned attack kinds.For vehicle security, Longari et al. [9] introduced CANnolo, an unsupervised IDS that uses LSTM-auto encoders and performs better than state-of-the-art anomaly detection methods for CAN. CANnolo demonstrated notable AUC improvements in data-field based anomalies and demonstrated expertise in detecting sequence-based abnormalities with high AUC values. Despite its efficacy, the study possesses some limitations, primarily its intricacy and protracted computation. Future research endeavors to create a more lightweight system for enhanced functionality.

Table 2: Literature Survey

Author	Methods Used	Dataset	Advantages	Limitations
Bo Song et al. proposed an intrusion detection system ddu et al. [1]	ECFO-MCNN	Car hacking, UNSW-NB15	Enhances ITS security, improves anomaly detection	Lacks focus on long-term optimization, vulnerable to attacks
Han et al. [2]	Complex value neural network (CVNN)	CAN dataset	High real-time detection accuracy (98%)	Requires substantial computational resources and is deficient in real-world event prediction.
Markus et al. [3]	CANet, LSTM	CAN bus dataset	High true negative rate (>0.99)	Struggles with gradual network state changes
Hossain et al. [4]	LSTM	Custom dataset, Korea Hacking and Countermeasures Research Lab dataset	High accuracy (99.995%) for DoS, fuzzing, spoofing	Only evaluated three attack types
Inoue et al. [5]	Deep CNN Inception-ResNet	Real car datasets	High accuracy (99.9%)	Limited to specific car models, resource constraints not addressed
Yang et al. [6]	GAN	Custom datasets	High precision and accuracy	Focused on specific attacks, lacks real-world discussion
Ullah et al. [7]	GRU, LSTM, SMOTE	Car-hacking dataset, combined DDoS dataset	High accuracy (99.5-99.9%)	Lack of comparison with state-of-art IDS
Song et al. [8]	Deep convolutional neural network (DCNN)	Real vehicle datasets	High detection rate, avoids unwanted complexity	Lacks detection of unlearned attack types
Longari et al. [9]	CANnolo (LSTM-auto encoders)	CAN bus dataset	High AUC values for anomalies	Slow computation, complexity

The literature review is summarized in Table 2. which also provides a comprehensive overview of the many deep learning-based IDS models proposed by different researchers, emphasizing the methods used, datasets used, key advantages, and disadvantages of each investigation. The objective of this comparative analysis is to offer perspectives on the status of the intrusion detection system for autonomous networks.

IV. DISCUSSION AND FUTURE WORK

The analyzed literature reveals substantial progress in intrusion detection systems (IDS) designed for intelligent transportation systems (ITS). Diverse designs and methods, such as ECFO-MCNN, CVNN, and GANs, have been utilized, each offering distinct contributions to the difficulties of in-vehicle and external network security. For instance, ECFO-MCNN shows superior performance in detecting hostile traffic compared to traditional methods like SI-LSTM and G-VSPA, indicating its potential to enhance ITS security. Similarly, CVNN with its random phase feature rotation and attention mechanisms achieves an impressive accuracy of 98% There are still numerous challenges to be solved. Real-time in real-time intrusion detection, showcasing the effectiveness of feature engineering in securing Controller Area Networks (CAN).

LSTM-based methodologies, such as those put forth by Hossain et al., Ullah et al., and Longari et al., have exhibited remarkable precision in identifying diverse assault types. Nonetheless, these solutions encounter constraints, including implementation sophistication and a concentration on a limited spectrum of attack types.

Markus et al.'s CANet IDS and Song et al.'s DCNN-based IDS highlight the significance of unsupervised and automated feature extraction methods in improving the scalability and adaptability of IDS. Nevertheless, these studies often rely on limited datasets, which hampers the generalizability of the proposed solutions.

GAN-based models and hybrid approaches such as LSTM-GRU have shown promise in improving detection accuracy and reducing training time. However, these strategies provide their own issues, including vulnerability to adversarial attacks and computational overhead. Additionally, methods like SMOTE, used for dataset balancing, require careful evaluation to ensure that they do not introduce biases or degrade the model's performance. Across the reviewed works, a common limitation is the restricted scope of attack types considered and the lack of testing on diverse real-world datasets. The challenge of detecting previously unseen or sophisticated attack types remains largely unaddressed, highlighting a critical gap in the existing research.

Future work includes real-time detection using unsupervised learning and explores adversarial and unsupervised methods for identifying zero-day attacks. Also developing Lighter systems and to study correlations to address the slow computation issues are other future research direction. Furthermore, it is essential to create comprehensible intrusion prevention systems and to devise models that are exclusively trained on conventional CAN communications.

V. CONCLUSION

In summary, robust security measures such as Intrusion Detection Systems (IDS) are essential owing to the heightened complexity of in-vehicle networks resulting from the transition from mechanical systems to Electrical Control Units (ECUs). A variety of deep learning models, including Long Short-Term Memory (LSTM) networks, Recurrent Neural Networks (RNN), Convolutional Neural Networks (CNN), and hybrid models, have demonstrated significant potential in enhancing network security. Previous investigations have demonstrated increased accurate detection, minimal false positive rates, and the capacity to manage complicated data.

REFERENCES

[1] R. S. K. Boddu, R. R. Chandan, M. Thamizharasi, R. Shaikh, A. A. Goyal, P. P. Gupta, and S. K. Gupta, "Using deep learning to address the security issue in intelligent transportation systems," *Journal of Autonomous Intelligence*, vol. 7, no. 4, 2024. [Online]. Available: https://doi.org/10.32629/jai.v7i4.1220

[2] M. Han, P. Cheng, and S. Ma, "PPM-InVIDS: Privacy protection model for in-vehicle intrusion detection system based complex-valued neural network," *Vehicular Communications*, vol. 31, 2021. [Online]. Available: https://doi.org/10.1016/j.vehcom.2021.100374

[3] M. Hanselmann, T. Strauss, K. Dormann, and H. Ulmer, "CANet: An unsupervised intrusion detection system for high dimensional CAN bus data," *IEEE Access*, 2019. [Online]. Available: https://doi.org/10.1109/ACCESS.2020.2982544

[4] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall, and Y. Kadobayashi, "An effective in-vehicle CAN bus intrusion detection system using CNN deep learning approach," in *Proc. IEEE Global Communications Conference (GLOBECOM)*, 2020. [Online]. Available: https://doi.org/10.1109/GLOBECOM42002.2020.9322395

[5] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall, and Y. Kadobayashi, "An effective in-vehicle CAN bus intrusion detection system using CNN deep learning approach," in *Proc. IEEE Global Communications Conference (GLOBECOM)*, 2020. [Online]. Available: https://doi.org/10.1109/GLOBECOM42002.2020.9322395

[6] Y. Yang, G. Xie, J. Wang, J. Zhou, Z. Xia, and R. Li, "Intrusion detection for in-vehicle network by using single GAN in connected vehicles," *Journal of Circuits, Systems and Computers*, vol. 30, no. 1, 2021. [Online]. Available: https://doi.org/10.1142/S0218126621500079

[7] S. Ullah, M. A. Khan, J. Ahmad, S. S. Jamal, Z. E. Huma, M. T. Hassan, N. Pitropakis, A. Arshad, and W. J. Buchanan, "HDL-IDS: A hybrid deep learning architecture for intrusion detection in the Internet of Vehicles," *Sensors*, vol. 22, no. 4, 2022. [Online]. Available: https://doi.org/10.3390/s22041340

[8] H. M. Song, J. Woo, and H. K. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," *Vehicular Communications*, vol. 21, 2020. [Online]. Available: https://doi.org/10.1016/j.vehcom.2019.100198

[9] S. Longari, D. Humberto, N. Valcarcel, M. Zago, M. Carminati, and S. Zanero, "CANnolo: An anomaly detection system based on LSTM autoencoders for Controller Area Network," *IEEE Trans. Network and Service Management*, 2020. [Online]. Available: http://dx.doi.org/10.1109/TNSM.2020.3038991

[10] H. Bangui and B. Buhnova, "Recent advances in machine-learning driven intrusion detection in transportation: Survey," *Procedia Computer Science*, vol. 184, pp. 877–886, 2021. [Online]. Available: https://doi.org/10.1016/j.procs.2021.04.014

[11] P. Agbaje, A. Anjum, A. Mitra, S. Hounsinou, E. Nwafor, and H. Olufowobi, "Privacy-preserving intrusion detection system for Internet of Vehicles using split learning," in *Proc. 10th IEEE/ACM Int. Conf. Big Data Computing, Applications and Technologies (BDCAT)*, Dec. 2023. [Online]. Available: https://doi.org/10.1145/3632366.3632388

[12] W. Wu, R. Li, G. Xie, J. An, Y. Bai, J. Zhou, and K. Li, "A survey of intrusion detection for in-vehicle networks," *IEEE Trans. Intelligent Transportation Systems*, vol. 21, no. 3, pp. 919–933, 2020. [Online]. Available: https://doi.org/10.1109/TITS.2019.2908074

[13] R. S. Vitalkar, "A review on intrusion detection system in vehicular ad-hoc network using deep learning method," *Int. J. for Research in Applied Science and Engineering Technology (IJRASET)*, vol. 8, no. 5, pp. 1591–1595, 2020. [Online]. Available: https://doi.org/10.22214/ijraset.2020.5258

[14] H. Ji, Y. Wang, H. Qin, Y. Wang, and H. Li, "Comparative performance evaluation of intrusion detection methods for in-vehicle networks," *IEEE Access*, vol. 6, pp. 37523–37532, 2018. [Online]. Available: https://doi.org/10.1109/ACCESS.2018.2848106

[15] A. Khalil, H. Farman, M. M. Nasralla, B. Jan, and J. Ahmad, "Artificial intelligence-based intrusion detection system for V2V communication in vehicular ad-hoc networks," *Ain Shams Engineering Journal*, vol. 15, no. 4, 2024. [Online]. Available: https://doi.org/10.1016/j.asej.2023.102616