SECURITY ASSESSMENT OF IN-VEHICLE NETWORK INTRUSION DETECTION IN REAL-LIFE SCENARIOS

Kamronbek Yusupov[1], Md Rezanur Islam[1], Insu Oh[2], Mahdi Sahlabadi[2] and Kangbin Yim[2]

[1]Software Convergence, Soonchunhyang University, Asan-si, South Korea
[2] Department of Information Security Engineering, Soonchunhyang University, Asan-si, South Korea

ABSTRACT

This research focuses on evaluating the security of an intrusion detection system in a CAN bus-based vehicle control network. A series of studies were conducted to evaluate the performance of models proposed by previous researchers, testing their effectiveness in real-world scenarios as opposed to those on which they were trained. The article demonstrates that models trained and tested on the same dataset can only sometimes be considered adequate. An approach that included models trained only on CAN ID, payload, or full data was chosen. The research results show that such methods are ineffective enough in real-world attack scenarios because they cannot distinguish between new scenarios not presented during training. The results of testing the models in various attack scenarios are presented, and their limitations are identified. In addition, a new method is proposed explicitly for attack scenarios that may occur in the real-world use of an in-vehicle CAN communication system.

KEYWORDS

Intrusion Detection System, Controller Area Network, In-Vehicle Network, LSTM.

1. INTRODUCTION

In the automotive era, where technology is indispensable in shaping our driving experiences, ensuring security in vehicle-related technology becomes a crucial factor integral to the digital transformation of the automotive landscape. Security researchers have made a lot of progress in making these systems safer [1]-[3]. However, because technology is always changing, new problems arise, and more work needs to be done to make in-vehicle networks more resistant to new cyber threats [4]. This research comprehensively evaluates the security of an Intrusion Detection System (IDS) deployed in a Controller Area Network (CAN) bus-based vehicle control network. The evaluation is based on the features used to detect intrusion. The research consists of several meticulously carried out studies to evaluate the effectiveness of models that earlier researchers had advocated. These studies scrutinized the efficacy of the models in real-world scenarios and compared their performance with their original training environments. The findings of this investigation reveal that models that are exclusively trained and tested on the same dataset can only sporadically be deemed adequate. The approach involves models trained solely on CAN ID, payload, or entire data [5]-[8]. However, from an intruder's point of view, this approach can be improvised according to their creativity, which could make the intrusion detection system

David C. Wyld et al. (Eds): SPTM, AIS, SOENG, AMLA, NLPA, IPPR, CSIT – 2024
pp. 01-10, 2024. CS & IT - CSCP 2024 DOI: 10.5121/csit.2024.141101

underperform [1], [9]. This research highlights the need for effective intrusion detection methods to defend against this situation, as current approaches need improvement to differentiate novel situations that were not encountered during their training phases. The subsequent sections of the research paper provide a nuanced analysis of the models tested in diverse attack scenarios while elucidating their inherent limitations.

2. Related Works

Modern vehicles constantly evolve with new technologies and increased connectivity, offering improved comfort and external communication. However, these advancements also introduce vulnerabilities to vehicular systems, making it crucial to develop effective methods for preventing attacks. Various approaches and models have been explored to enhance security in the context of CAN bus IDS.

One innovative approach, presented in [5], leverages deep learning techniques, including Neural Networks (NN) and Multi-Layer Perceptron (MLP), to detect cyber-attacks on the CAN bus. This method's evaluation utilizes real-world datasets containing diverse attack types, demonstrating its effectiveness in distinguishing between normal and malicious messages, with a focus on payload analysis. However, it is worth noting that MLPs may face limitations in modelling sequential information effectively, especially when attackers manipulate the CAN ID sequence while maintaining a constant payload, as discussed in [10].

Another unique methodology, described in [6], relies solely on CAN ID sequences to model traffic patterns. This approach employs an LSTM-based generator model to create pseudo-normal data with added noise, followed by training an anomaly detector using this data for self-supervised learning in IDS. The system significantly improves detection performance, especially against unknown attacks, by training the detector to recognize deviations from normal data patterns. Nevertheless, determining the optimal noise ratio in data generation and assessing the system's performance in complex real-world scenarios remain areas for further investigation. In the realm of IDS using semi-supervised learning, the limited availability of labelled data can challenge the detection of unknown frequency injections and attacks, particularly in dynamic data generation scenarios like in-vehicle networks. Building an IDS solely based on CAN IDs without considering time may reduce its effectiveness in detecting replay attacks or replay attacks with the same CAN ID but modified payloads. Researchers in [7] conducted a study using Federated Learning (FL) to create an IDS capable of addressing challenges from various automobile manufacturers with diverse data. They employed multiple vehicle models, each with its own dataset of CAN ID sequences, to identify common patterns while preserving data privacy. The collaborative model training using the Federated Averaging (FedAvg) algorithm achieved an accuracy of 95% in supervised techniques. However, FL models introduce complexities and dependencies on third parties.

In a recent study [8], a Binary Neural Network (BNN)-based IDS demonstrated significantly improved detection speed, achieving three times faster detection than an alternative model. It is essential to note that this speed improvement comes at the cost of accuracy, which can vary depending on the attack type. The IDS uses labelled input full frames during training containing ten CAN messages to teach the BNN model to recognize attack patterns. Once trained, the BNN model can rapidly analyse real-time CAN traffic and trigger alarms when detecting malicious activities. However, incorporating diverse features into the model may increase computational complexity, highlighting the need to balance computational efficiency and detection accuracy in IDS design.

These various approaches and methodologies contribute to the ongoing efforts to enhance the security of in-vehicle networks, particularly in the context of CAN bus communication.

3. BACKGROUND

3.1. Controller Area Network

Controller Area Network (CAN) is a well-known system for exchanging messages between electronic control [11], units in the automobile sector. It provides a dependable and effective method of communication between various car components, such as the engine, brakes, and gearbox. Due to its adaptability and simple construction, the CAN bus has become the industry standard for data [12] interchange and transfer in automotive electronics. A typical CAN data frame has several fields, as shown in Figure 1.

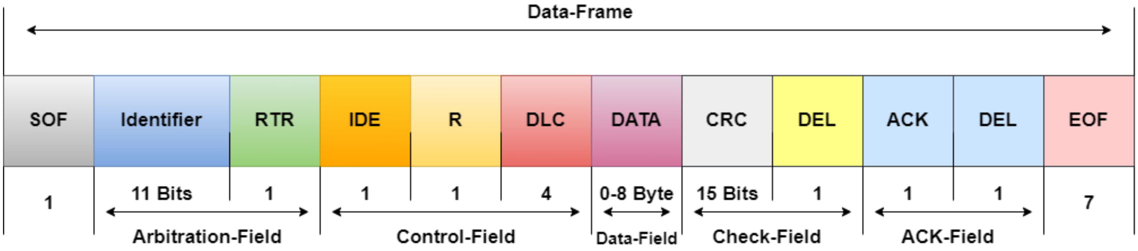


Figure 1. CAN Data-Frame

The first is the Start of the Frame (SOF), which indicates the start of message transmission. The following field is the Arbitration Field, which specifies the message's identity and establishes the data's priority and uniqueness. Furthermore, the Control Field includes bits like RTR, IDE (Identifier Extension), and DLC (Data Length Code) that provide information about the type of message being sent. The Data Field can be from 0 to 8 bytes and holds the data transmitted in the messages. Additionally, the CRC (Cyclic et al.) fields detect errors. Finally, the CAN message ends when the End of Frame (EOF) field is set to 1.

3.2. CAN Vulnerabilities

Denial of Service. A Denial of Service (DoS) [13] attack is a hostile action intended to interfere with a system's regular functioning, create problems, and restrict access to it. DoS attacks directed at the CAN bus aim to obstruct the normal operation of the system by preventing the transmission of valid messages. Successful DoS attacks can have disastrous effects, such as unexpected engine shutdowns or brake failures, which could result in accidents. In our situation, injections were performed with a time interval ranging from 0.3 to 0.5 milliseconds, while the attack was carried out using a dataset with the CAN ID 0x000 supplied. The attack's goal was to overwhelm the CAN system by flooding the CAN bus with many messages, forcing the system to become unresponsive.

Fuzz. Fuzzing [13] is a sort of cyberattack used to test or discover system flaws and give attackers potential entry points. The goal of this attack is to transmit a large number of random and inaccurate messages [14] to see how the system reacts to such irregular data. The fuzzing attack in our dataset was carried out by sending random CAN IDs and data at intervals of 0.3 to 0.5 milliseconds. The purpose of this deliberate injection of erratic and inconsistent data was to confuse and interfere with the system's regular operation. The attack's goal was to hinder the system's functionality and cause confusion throughout its operations.

Replay. Replay attacks [14] are a sort of cyberattack in which attackers intercept valid communications sent by other ECUs, record them, and then replay or resend them to the system at a later time. These messages replace regular messages, which causes the system to recognize them as genuine and carry out their directives. For instance, a hacker may examine and record communications that are used to control the braking system or other car operations. The attacker can then transmit these recorded messages to the system with the purpose of tricking it by often utilizing the original message IDs. A replay attack was included in our dataset and was conducted with intervals of 0.3 to 0.5 milliseconds, just like the fuzz and dos attacks. This assault was carried out around 300 times.

3.3. Neural Network

Long Short-Term Memory (LSTM) [15] is a sort of recurrent neural network that successfully handles the difficulty of addressing long-term dependencies in sequential input. By including memory cells and the three crucial parts of input gates, forget gates, and output gates, it solves the gradient decay issue in conventional RNNs. By combining these elements into each memory cell, the LSTM model is able to preserve and use pertinent data from earlier time steps while tossing out irrelevant material. As a result, the LSTM model is better able to capture complicated temporal patterns in sequential data, which makes it suitable for handling complex information when used in the context of the CAN system.

4. EXPERIMENTAL METHOD

The datasets were collected from a real vehicle, such as KIA SOUL [16]. The datasets include three types of attacks: DoS, Fuzz, Replay, and Attack Free. Each dataset consists of 14 columns: Time Offset, CAN ID, Time Gap, DLC, Payload (Payload 1 to Payload 8), and Label. These columns provide various information about the functional operation. For example, Time Offset represents time and is used to track the interval between messages, and CAN ID is a CAN system identifier that identifies the priority of messages and the sender. Time Gap represents the time interval between two CAN messages. The DLC column indicates the number of bytes in the Payload. Payload columns contain the actual data exchanged in the CAN communication system. Columns Payload 1 through Payload 8 contain individual data that is combined into the Payload column. The last column, Label, contains the labels "T" (Attack) and "R" (Regular), which allows distinguishing between attacked and under-attacked data. After selecting a specific dataset, all data were cleaned and brought into one format. The data was then combined and divided into two sets for training and testing. For three types of experiments, a specific set of columns was selected for training and testing. The first set included only the CAN ID and Label columns; the second included the Payload and Label columns separately; and the third included the entire dataset with all columns. After preparing the datasets, LabelEncoder [17] and MeanNormalization [18] were applied. LabelEncoder was used to convert categorical data to a usable format, improving convergence stability and model training efficiency. Mean normalization was performed using the formula x_normalized = (x - μ) / σ is the standard deviation. The permutation method [18] was then used to improve the generalization ability of the model by providing it with a variety of training examples. This method involves randomly changing the order or distribution of training examples, producing a variety of training data. With this technique, you can reduce the likelihood of overfitting the model because it is trained on a wider range of input scenarios. After data preprocessing was completed, an LSTM model was built that classifies the data using the Binary Cross technique. Three distinct model types were created in the current study and trained using various methods, such as CAN ID, Payload, and the full dataset. The research was based on testing these models on a CAN system under an identical assault scenario, where they effectively identified abnormalities.

Table 1. Assessing Trained Features CAN ID.

Index	CAN ID Original Dataset			CAN ID Improvised Dataset		
	Precision	Recall	F1-score	Precision	Recall	F1-score
Attack Free	0.99	0.98	0.99	0.74	0.99	0.85
Attack	0.99	0.99	0.99	0.99	0.79	0.88
Overall Accuracy	0.99			0.87		

Table 2. Assessing Trained Features Payload

Index	Payload Original Dataset			Payload Improvised Dataset		
	Precision	Recall	F1-score	Precision	Recall	F1-score
Attack Free	0.96	0.99	0.98	0.75	0.93	0.83
Attack	1.00	0.98	0.99	0.91	0.68	0.78
Overall Accuracy	0.98			0.81		

Table 3. Assessing Trained Features all columns (Full data)

Index	Full Original Dataset			Full Improvised Dataset		
	Precision	Recall	F1-score	Precision	Recall	F1-score
Attack Free	1.00	0.99	0.99	0.91	0.92	0.90
Attack	0.99	1.00	0.99	0.92	0.90	0.90
Overall Accuracy	0.99			0.90		

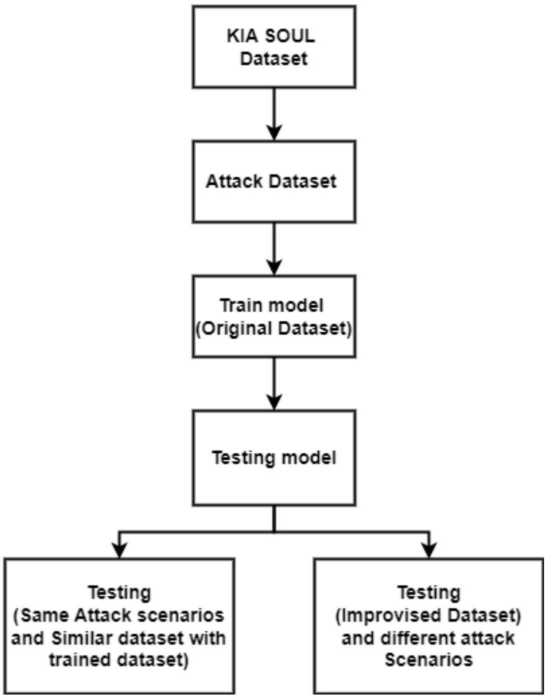

KIA SOUL Dataset
Attack Dataset
Train model (Original Dataset)
Testing model
Testing (Same Attack scenarios and Similar dataset with trained dataset)
Testing (Improvised Dataset) and different attack Scenarios

Figure 2. Experimental Flow

The models were trained just on one assault scenario; thus, even if they performed well in this assignment, they cannot identify other kinds of threats. Several tests were run as part of the scientific investigation to assess the models' efficacy. As seen in Figure 2, all three models were trained using the same assault scenario before testing the finished products in other attack situations.

5. Experimental Performance

The purpose of this experiment was to evaluate the effectiveness of certain methods trained using specific columns in IDS for CAN security, as previously presented by other researchers. These methods, which have been demonstrated in prior work, are being assessed for their real-world applicability. A comparative analysis was conducted on methods proposed by other researchers, such as training a model using only CAN ID or Payload. The researchers claimed that their models were successful in detecting attacks by focusing on the CAN ID or the data in the Payload columns. In this study, an analysis was carried out, and the results indicate that the model performs well on the dataset used in training, with testing accuracy on this attack scenario reaching 99%.

Our experimental setup makes use of a Kia Soul car in the context of DoS assaults. The most important finding is that may ID 018 has the greatest priority, meaning that any CAN ID below 018 may be used as a point of entry to start a DoS assault injection. As for the payload, purposeful random changes highlight how they affect the effectiveness of the IDS. These variants are meant to illustrate, from the attacker's point of view, the possible consequences of creative data injection, underscoring the need of taking into account a variety of payload situations in order to improve IDS reliability. When it comes to fuzzing assaults, a method called random selection of CAN IDs is used, which includes combining high and low priority IDs. Although attackers may display a variety of patterns, traditional supervised approaches usually train models on a small collection of injection cases. By highlighting this disparity, the research hopes to emphasize how important it is to take any changes in assault patterns into consideration when training models. In addition, the effects of payload alteration are investigated for both replay and fuzzing situations. Attackers' varied strategies and their possible effects on system security are shown by introducing random modifications to payload values across different CAN IDs, from minor tweaks to more substantial ones.

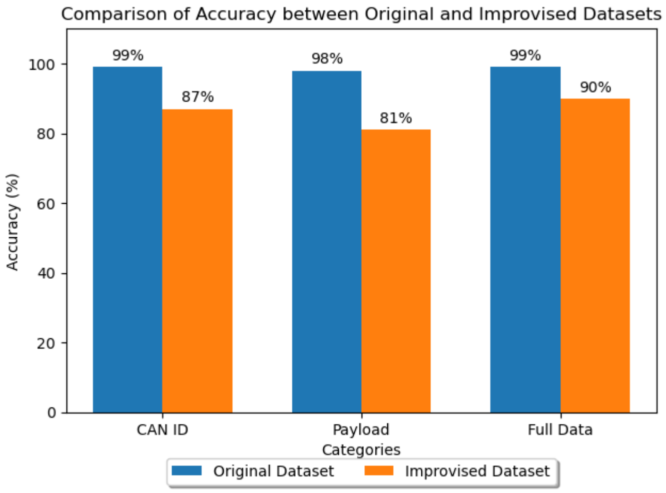


Figure 3. Confusion Matrix for Original Dataset

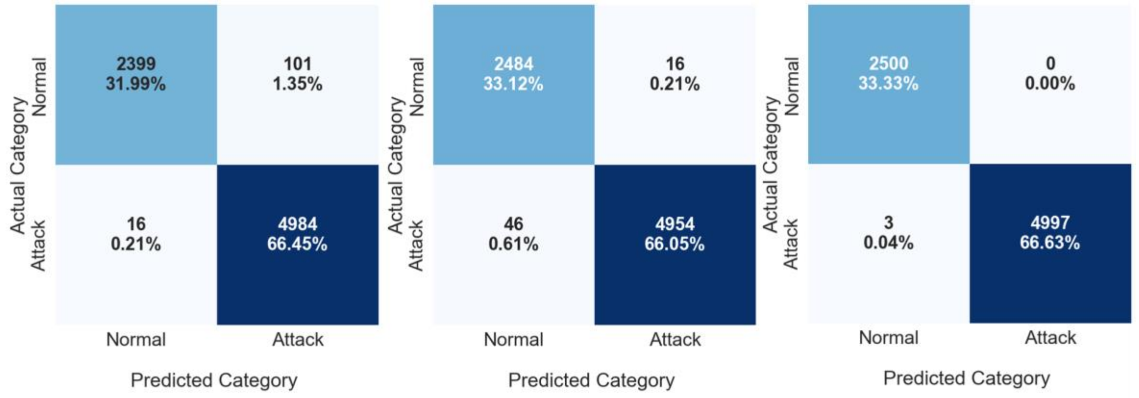
The improvised datasets were created as follows:

DoS Attack Modifications: In the original version, the attack value was set to 0x000. However, for the improvised version, four-digit values were generated, considering that real CAN IDs in KIA SOUL cars typically start with 0x0018. For the DoS CAN ID, 0x015, 0x008, 0x017, 0x002, and 0x003 were selected as the attack IDs.

Payload Modifications (DoS): The values in the Payload 1, Payload 2, Payload 3, and Payload 4 columns were modified. Specifically, for rows where the CAN ID matched 0x002, 0x015, 0x008, 0x017, or 0x003, the values in these columns were changed to 0xFF.

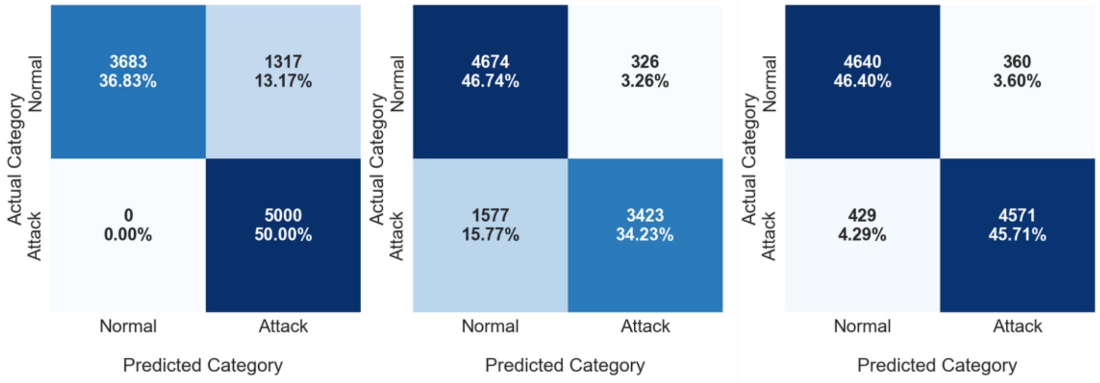
Fuzzing Attack Modifications: Initially, CAN IDs 0x2A0, 0x081, 0x260, and 0x1F1 were chosen for the Fuzz attack. However, in the improvised version, these CAN IDs were altered to different values, such as 0x1A0, 0x080, 0x250, and 0x009.

Payload Modifications (Fuzzing and Replay): For the Payload column, values in the Payload 1 column were set to 0x00 for rows where the CAN ID was 0x017. Additionally, if the CAN ID was 0x165 and the value in the Payload 1 column was 0xFF. Furthermore, for rows with CAN IDs 0x370 and 0x440, the values in the Payload 5 column were set to 0xFF.



(a) CAN ID (b) Payload (c) Full data

Figure 4. Confusion Matrix for Original Dataset



(a) CAN ID (b) Payload (c) Full data

Figure 5. Confusion Matrix for Improvised Dataset

These adjustments were made to create an improvised dataset for testing the models. For the improvised data, the values on which the model was trained using the original dataset were changed. The results showed that models trained on one attack scenario performed differently with the improvised data shown in Figures 2, 3, 4, and 5. For example, a model trained on CAN ID achieved 99% accuracy on test data, but its performance dropped to 87% on improvised data. In the second experiment, the accuracy for Payload test data was 98% shown in Table 1, but on improvised data, the accuracy reached only 81% shown in Table 2. In the third experiment, models trained using all columns achieved 99% on the test data, but their accuracy dropped to 90% when tested with improvised data shown in Table 3. These results indicate that models trained solely on specific columns and the methods proposed earlier are not considered effective. To enhance the effectiveness of an IDS, considering time-gap features between two packets with CAN ID sequences is recommended. This approach offers several advantages. Utilizing the entire dataset could lead to a more complex model that is computationally less efficient. Focusing on time-gap features allows for a simplified model while still capturing critical information. Also, to make the model work in different situations and help the data become more general, it's a good idea to investigate techniques like converting the data into the frequency domain or other useful methods [1], [9]. These techniques can enhance the IDS's ability to detect intrusions under different scenarios and conditions, making it more versatile and practical.

6. CONCLUSION

In conclusion, the outcomes of this experiment have unveiled certain limitations and constraints in the training methods employed for a CAN-based IDS. Through a comparative investigation of various approaches based on feature inputs, encompassing models trained solely on CAN ID or Payload data as well as those incorporating all available parameters, notable differences in performance emerged. These results make it clear that models trained only on certain features and the suggested methods have flaws that make them less useful in real-life attack situations, which makes sense in real-life situations. While these models excel at classifying attacks within controlled test datasets, their performance experiences a significant decline when tested against improvised datasets. This shows how important it is to make IDS systems that are more reliable and can adapt to changing attack scenarios in the real world, not just the controlled conditions of normal testing. The agnostic nature of the injection procedure has meant that data generability has often been ignored in research efforts aimed at protecting in-vehicle networks. Finding appropriate characteristics or investigating data generability must be given top priority in order to close this gap.

ACKNOWLEDGEMENTS

This work was supported in part by the National Research Foundation of Korea (NRF) Grant funded by the Korean Government [Ministry of Science and ICT (MSIT)] under Grant 2021R1A4A2001810; in part by the Institute for Information and Communications Technology Planning and Evaluation (IITP) Grant funded by the Korean Government (MSIT), Convergence Security Core Talent Training Business (Soonchunhyang University), under Grant 2022-0-01197; and in part by Soonchunhyang University Research Fund.

REFERENCES

[1] M. R. Islam, I. Oh, and K. Yim, “Universal intrusion detection system on in-vehicle network,” in International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Springer, 2023, pp. 78–85.

[2] P. Wei, B. Wang, X. Dai, L. Li, and F. He, “A novel intrusion detection model for the can bus packet of in-vehicle network based on attention mechanism and autoencoder,” Digital Communications and Networks, vol. 9, no. 1, pp. 14–21, 2023.

[3] Z. Yu, Y. Liu, G. Xie, R. Li, S. Liu, and L. T. Yang, “Tce-ids: Time interval conditional entropy-based intrusion detection system for automotive controller area networks,” IEEE Transactions on Industrial Informatics, vol. 19, no. 2, pp. 1185–1195, 2022.

[4] Z. Cai, A. Wang, W. Zhang, M. Gruffke, and H. Schweppe, “0-days & mitigations: Roadways to exploit and secure connected bmw cars,” Black Hat USA, vol. 2019, no. 39, p. 6, 2019.

[5] F. Amato, L. Coppolino, F. Mercaldo, F. Moscato, R. Nardone, and A. Santone, “Can-bus attack detection with deep learning,” IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 8, pp. 5081–5090, 2021.

[6] H. M. Song and H. K. Kim, “Self-supervised anomaly detection for in-vehicle network using noised pseudo normal data,” IEEE Transactions on Vehicular Technology, vol. 70, no. 2, pp. 1098–1108, 2021.

[7] T.-N. Hoang, M. R. Islam, K. Yim, and D. Kim, “Canperfl: Improve in-vehicle intrusion detection performance by sharing knowledge,” Applied Sciences, vol. 13, no. 11, p. 6369, 2023.

[8] L. Zhang, X. Yan, and D. Ma, “A binarized neural network approach to accelerate in-vehicle network intrusion detection,” IEEE Access, vol. 10, pp. 123 505–123 520, 2022.

[9] M. R. Islam, M. Sahlabadi, K. Kim, Y. Kim, and K. Yim, “Cf-aids: Comprehensive frequency-agnostic intrusion detection system on in-vehicle network,” IEEE Access, 2023.

[10] Z. Lin, A. Jain, C. Wang, G. Fanti, and V. Sekar, “Using gans for sharing networked time series data: Challenges, initial promise, and open questions,” in Proceedings of the ACM Internet Measurement Conference, 2020, pp. 464–483.

[11] M. Farsi, K. Ratcliff, and M. Barbosa, “An overview of controller area network,” Computing & Control Engineering Journal, vol. 10, no. 3, pp. 113–120, 1999.

[12] Y. Koh, S. Kim, Y. Kim, I. Oh, and K. Yim, “Efficient can dataset collection method for accurate security threat analysis on vehicle internal network,” in International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Springer, 2022, pp. 97–107.

[13] H. Lee, S. H. Jeong, and H. K. Kim, “Otids: A novel intrusion detection system for in-vehicle network by using remote frame,” in 2017 15th Annual Conference on Privacy, Security and Trust (PST), IEEE, 2017, pp. 57–5709.

[14] H. Kang, B. I. Kwak, Y. H. Lee, H. Lee, H. Lee, and H. K. Kim, “Car hacking and defense competition on in-vehicle network,” in Workshop on Automotive and Autonomous Vehicle Security (AutoSec), vol. 2021, 2021, p. 25.

[15] Y. Yu, X. Si, C. Hu, and J. Zhang, “A review of recurrent neural networks: Lstm cells and network architectures,” Neural computation, vol. 31, no. 7, pp. 1235–1270, 2019.

[16] A. or Organization, Hacking and countermeasure research lab, https: / /ocslab.hksecurity.net/, Accessed on January 24, 2024, Year of access.

[17] M. S. Yadav and R. Kalpana, “Data preprocessing for intrusion detection system using encoding and normalization approaches,” in 2019 11th International Conference on Advanced Computing (ICoAC), IEEE, 2019, pp. 265–269.

[18] Y. Kamronbek, I. M. Rezanur, I. Oh, and K. Yim, “Time series mean normalization for enhanced feature extraction in in-vehicle network intrusion detection system,” in International Conference on Broadband and Wireless Computing, Communication and Applications, Springer, 2023, pp. 302–311.

AUTHORS

Kamronbek Yusupov received his B.S. in 2023, from the Department of Information Security Engineering at Soonchunhyang University in Asan, South Korea. Currently, he is studying a Master`s degree in Software Convergence at Soonchunhyang University in South Korea. His research interests encompass deep learning, anomaly detection, and malware detection, reflecting his commitment to investigating advanced solutions and leveraging state-of-the-art technologies in these domains.

Md. Rezanur Islam received the B.Sc. degree in electrical and electronic engineering from the University of Asia Pacific, Bangladesh, in 2016, and the M.Sc. degree in mobility convergence from Soonchunhyang University, South Korea, in 2023, where he is currently pursuing the Ph.D. degree in software convergence. His research interests include deep learning, anomaly detection, and malware detection, reflecting the commitment to investigating advanced solutions, and leveraging state-of-the-art technologies in these domains.

Insu Oh received his B.S. in 2018, M.S. in 2020, and Ph.D. in 2023, all from the Department of Information Security Engineering at Soonchunhyang University in Asan, South Korea. Currently, he is conducting postdoctoral research at Soonchunhyang University in South Korea. His research interests include vulnerability analysis, mobile baseband security, automotive security, and V2X security.

Mahdi Sahlabadi received the Ph.D. degree in industrial computing from the National University of Malaysia. His academic journey includes research positions with the Japan Advanced Institute of Science and Technology (JAIST), Singapore Management University (SMU), the Sharif University of Tehran (SUT), University Kebangsaan Malaysia (UKM), and Soonchunhyang University (SCH), South Korea. His research interests include process mining, software architecture, cybersecurity, and quality assurance.

Kangbin Yim received the B.S., M.S., and Ph.D. degrees from the Department of Electronics Engineering, Ajou University, Suwon, South Korea, in 1992, 1994, and 2001 respectively. He is currently a Professor with the Department of Information Security Engineering, Soonchunhyang University. His research interests include vulnerability assessment, code obfuscation, mal-ware analysis, leakage prevention, secure platform architecture, and mobile security. He has worked on more than 60 research projects and published more than 100 research papers related to these topics. He has served as an Executive Board Member for the Korea Institute of Information Security and Cryptology, the Korean Society for Internet Information, and The Institute of Electronics Engineers of Korea. He has also served as a committee chair for international conferences and workshops and has acted as a Guest Editor for journals, such as Journal of Information Technology, Journal of Management Information Systems, Journal of Current Pharmaceutical Sciences, Journal of Internet Services and Information Security, and Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications.