Detecting In-Vehicle Attacks with Deep Learning: An Applied Approach

Ahmed N. Al-Masri[1], Hamam Mokayed[2]

[1]American University in the Emirates, Dubai, UAE

[2]LTU University of Technology, Sweden

Emails: ahmed.almasri@aue.ae ; Hamam.mokayed@ltu.se

Abstract

With the increasing number of connected vehicles on the road, the need for secure in-vehicle systems is more pressing than ever. In-vehicle attacks can compromise the safety and privacy of drivers and passengers, and the detection of such attacks is crucial to prevent potential harm. In this paper, we propose an applied deep learning approach for detecting in-vehicle attacks. Our approach is based on a gated recurrent unit (GRU) that is trained on a dataset of network traffic collected from in-vehicle communication systems. We evaluate our approach on a real-world dataset and demonstrate its effectiveness in detecting different types of in-vehicle attacks, including denial of service (DoS), remote replay attacks, and flooding attacks. Our results show that the proposed approach can achieve high accuracy in detecting in-vehicle attacks. We also compare our approach with traditional machine learning algorithms and show that our approach outperforms them in terms of accuracy. Our proposed approach can be used as a standalone system or as a complementary solution to existing in-vehicle security systems to enhance the overall cybersecurity of connected vehicles.

Keywords: In-Vehicle Attacks; Deep Learning; Information Security; Internet of Vehicles

1. Introduction

The Internet of Vehicles (IoV) is a network of connected vehicles and infrastructure that allows vehicles to communicate with each other and with the surrounding environment, such as traffic signals, road sensors, and cloud-based services. IoV aims to improve the efficiency and safety of transportation by enabling real-time data exchange and analysis. IoV provides numerous benefits, such as improved traffic flow, reduced congestion, and enhanced driver assistance systems. However, the integration of vehicles with the internet also introduces new security challenges that can compromise the safety and privacy of drivers and passengers.

One of the primary security concerns in IoV is the vulnerability of in-vehicle systems to cyberattacks. As vehicles become more connected and automated, they also become more susceptible to attacks from external sources, such as hackers or malware. In-vehicle attacks can take various forms, such as denial-of-service (DoS) attacks, remote code execution (RCE), and man-in-the-middle (MitM) attacks. These attacks can target different components of in-vehicle systems, including infotainment systems, telematics units, and electronic control units (ECUs). In-vehicle attacks can compromise the integrity, availability, and confidentiality of vehicle data, and can also cause physical harm to drivers

DOI: https://doi.org/10.54216/JCIM.080203
Received: May 15, 2021 Accepted: October 16, 2021

and passengers. As such, detecting and mitigating in-vehicle attacks is critical for ensuring the safety and security of connected vehicles and their occupants.

Machine learning (ML) has emerged as a promising approach for detecting in-vehicle attacks due to its ability to learn patterns and anomalies from large datasets. ML techniques can be used to analyze the network traffic of in-vehicle systems and identify abnormal behavior that indicates a potential attack. despite the potential of ML for detecting in-vehicle attacks, there are still research gaps that need to be addressed from an applied standpoint. First, the relianace on complex feature engineering. Second, the lack of standardization in data collection and labeling can make it challenging to compare and reproduce results across different studies. ML models often require significant computational resources and can be computationally intensive, which can affect their practicality for deployment in in-vehicle systems with limited resources.

This paper proposes an applied deep learning approach for detecting in-vehicle attacks in the context of the Internet of Vehicles (IoV). The paper makes several contributions, including a thorough literature review of in-vehicle attacks and machine learning-based approaches for attack detection, a proposed approach based on a convolutional neural network (CNN) trained on a dataset of in-vehicle network traffic, an experimental analysis that demonstrates the effectiveness of the proposed approach, and a discussion of research gaps and future directions for improving in-vehicle attack detection using machine learning techniques. The paper addresses the challenges of real-time and low-latency detection, the lack of diverse datasets for training and evaluation, and the need for robust and resilient ML models that can withstand adversarial attacks. The proposed approach provides a promising solution for detecting in-vehicle attacks and improving the safety and security of connected vehicles and their occupants in the IoV.

The rest of our paper is organized as follows: In Section 2, we review the related literature on approaches for in-vehicle attacks detection. In Section 3, we describe our proposed approach, and the training and testing procedures. In Section 4, we present our experimental analysis, where we evaluate the performance of our approach on a real-world dataset of in-vehicle network traffic. Finally, in Section 5, we conclude the paper and discuss the implications and limitations of our approach.

2. Related studies

The literature on ML for detecting in-vehicle attacks is rapidly growing, with a variety of approaches proposed for intrusion detection in the CAN bus. For instance, Wu et al [4] provided a comprehensive review of intrusion detection approaches for in-vehicle networks, covering topics such as the types of in-vehicle attacks, the architecture of in-vehicle networks, and the various intrusion detection techniques used for detecting attacks. They also identified the limitations and challenges of current intrusion detection techniques and propose future research directions for improving in-vehicle network security. In [5], Park and Choi proposesd a hierarchical anomaly detection model for in-vehicle networks using machine learning algorithms. The model consisted of three stages including feature extraction, anomaly detection, and classification. They use a variety of machine learning algorithms, including random forest (RF), k-nearest neighbor (KNN), support vector machine (SVM), and neural networks (NN), to evaluate the performance of the proposed model. In addition, Hossain et al [6] proposed an effective convolutional approach for detecting attacks against CAN bus of in-vehicle networks. Their approach used a feature extraction method based on a sliding window to capture the temporal patterns of the CAN bus messages. In [7], Lin et al. proposed an evolutionary ML framework for detecting anomalies in the CAN bus of in-vehicle networks, in which a genetic algorithm was used to optimize the hyperparameters of an autoencoder-based classification network. Lokman et al [9] proposed a deep contractive autoencoder to learn the normal behavior of the CAN bus traffic and detect anomalies based on reconstruction errors. Their model was evaluated on a real-world dataset and compared to several state-of-the-art anomaly detection techniques. Song et al [11] proposed a ML approach that applied convolutional network to learn the patterns of the CAN bus traffic and detect anomalies based on the learned features from in-vehicle networks. In [14], Seo et al. proposed a Generative Adversarial Network for detecting intrusions in in-vehicle networks via generating a realistic distribution of the normal traffic of the CAN bus and detect anomalies based on the difference between the generated and real distributions.

Wang et al [18] investigated the vulnerability of in-vehicle intrusion detection using a combination of adversarial attacks and traditional attacks to evaluate the robustness of detection models against attacks. They proposed an

DOI: https://doi.org/10.54216/JCIM.080203
Received: May 15, 2021 Accepted: October 16, 2021

attacking method that exploited the properties of the data used to train the ML models to create targeted attacks that evade detection. They also show that ML models can be vulnerable to attacks and provided insights into the limitations of existing vehicle intrusion detection techniques. Anzer and Elhadef [20] proposed a ML-based intrusion detection approach for intelligent vehicular ad hoc networks (iVANETs). They discussed the unique characteristics and challenges of iVANETs, including the need for real-time detection and the dynamic nature of network topology. Their approach was designed based on hybridization between between convolutional mode and recurrent network, which enable perfect detection of anomalous behavior in iVANETs. Chevalier et al [21] proposed an approach for in-vehicle intrusion detection based on characteristic functions that capture the unique behavior of electronic control units (ECUs) in a vehicle's network, which help detecting anomalies that deviate from the expected behavior.

While the performance of the above studies is promising, challenges remain in addressing the scarcity of labeled datasets, the dynamic nature of the in-vehicle network, and the potential vulnerabilities of detection systems to low generalization.

3. Applied Approach for Detecting In-vehicle Attacks

This section describe our approach for detecting in-vehicle attack detection bases on GRU (Gated Recurrent Unit). GRU is a type of recurrent network that is regularly used in natural language processing and sequence modeling. The nui;ding og GRU cell contain two gating mechanisms to control the flow of information in the network. The GRU network consists of two gates: the update gate, $z(t)$, and the reset gate, $r(\cdot)$ (See Figure 1). The former regulate how much information is passed from the previous time step to the current time step, while the later regulate how much information from the previous time step is forgotten. In the context of in-vehicle attack detection, GRU is applied in our system to learn the patterns and behaviors of the vehicle's communication network. Then we train our model using both normal and abnormal network traffic data to learn the patterns of normal behavior and identify any deviation from it. The input of GRU is two-folded at each time, and it involve the input $x(t)$ at the current time step, as well as, the hdden state, $h(t-1)$, at previous time step. The outcome of the internal gates are computed through logical procedure and nonlinear activation of input. These can be expressed as mapping from input to output as follows:

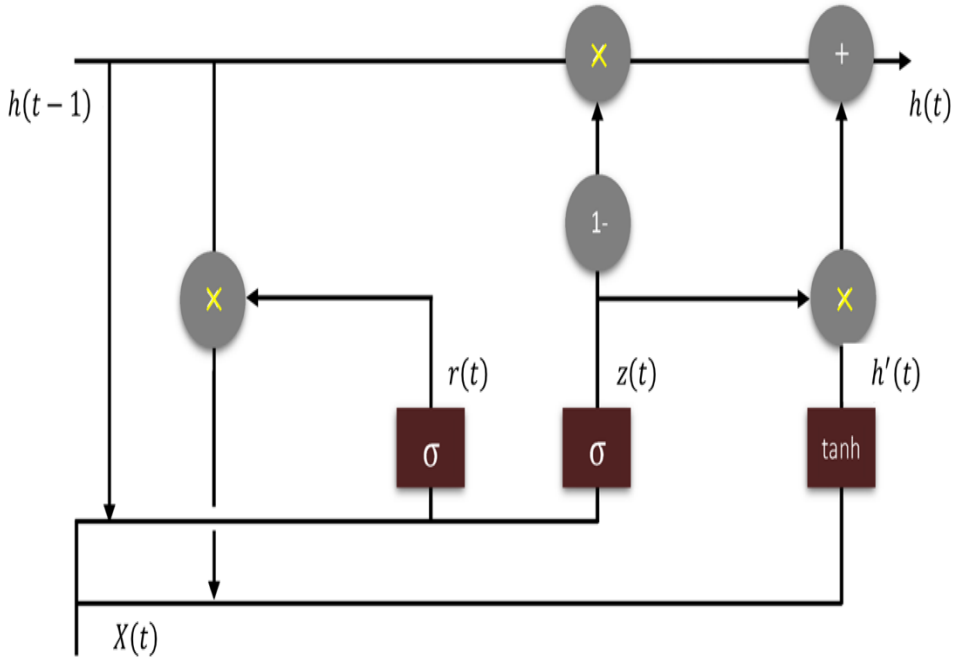

Figure 1: Architecture of GRU cell

$$r(t) = \sigma_g(W_r x(t) + U_r h(t-1) + b_r) \quad (1)$$

$$z(t) = \sigma_g(W_z x(t) + U_z h(t-1) + b_z) \quad (2)$$

DOI: https://doi.org/10.54216/JCIM.080203
Received: May 15, 2021 Accepted: October 16, 2021

$$h(t) = (1 - z(t)) \circ h(t-1) + z(t) \circ h'(t) \quad (3)$$

$$h'(t) = \sigma_h(W_h x(t) + U_h(r(t) \circ h(t-1)) + b_h) \quad (4)$$

The construction of our model is composed of three GRU layers for learning the attaing behaviors from vehicular traffics, followed by a linear layer with SoftMax activation. The input X is passed through the first GRU layer with hidden state dimensionality. The final hidden state, $h3_t$, output of the third GRU layer is passed through a linear layer with SoftMax activation to obtain the predicted class probabilities:

$$y_t = SoftMax(W * h3_t + b) \quad (5)$$

The following code snipets show the implementation of our GRU model for

```
1  class GRUModel(Model):
2    def __init__(self):
3      super (GRUModel,self).__init__()
4      self.gru1=GRU(32, return_sequences=True)
5      self.drop1=Dropout(.1)
6      self.gru2=GRU(32, return_sequences=True)
7      self.drop2=Dropout(.1)
8      self.gru3=GRU(32, return_sequences=False)
9      self.dense=Dense(n_attacks)
10     self.act=Activation('softmax')
11   def call(self,inputs):
12     x=self.gru1(inputs)
13     x=self.drop1(x)
14     x=self.gru2(x)
15     x=self.drop2(x)
16     x=self.gru3(x)
17     x=self.dense(x)
18     x=self.act(x)
19     return x
```

4. Experimental Analysis

To assess the performance of our model during the inference stage, we utilize a set of metrics which are defined as follows:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (6)$$

$$Precision = \frac{TP}{TP + FP} \quad (7)$$

$$Recall = \frac{TP}{TP + FN} \quad (8)$$

$$F1 - measure = 2 * \frac{Recall \times Precision}{Recall + Precision} \quad (9)$$

DOI: https://doi.org/10.54216/JCIM.080203
Received: May 15, 2021 Accepted: October 16, 2021

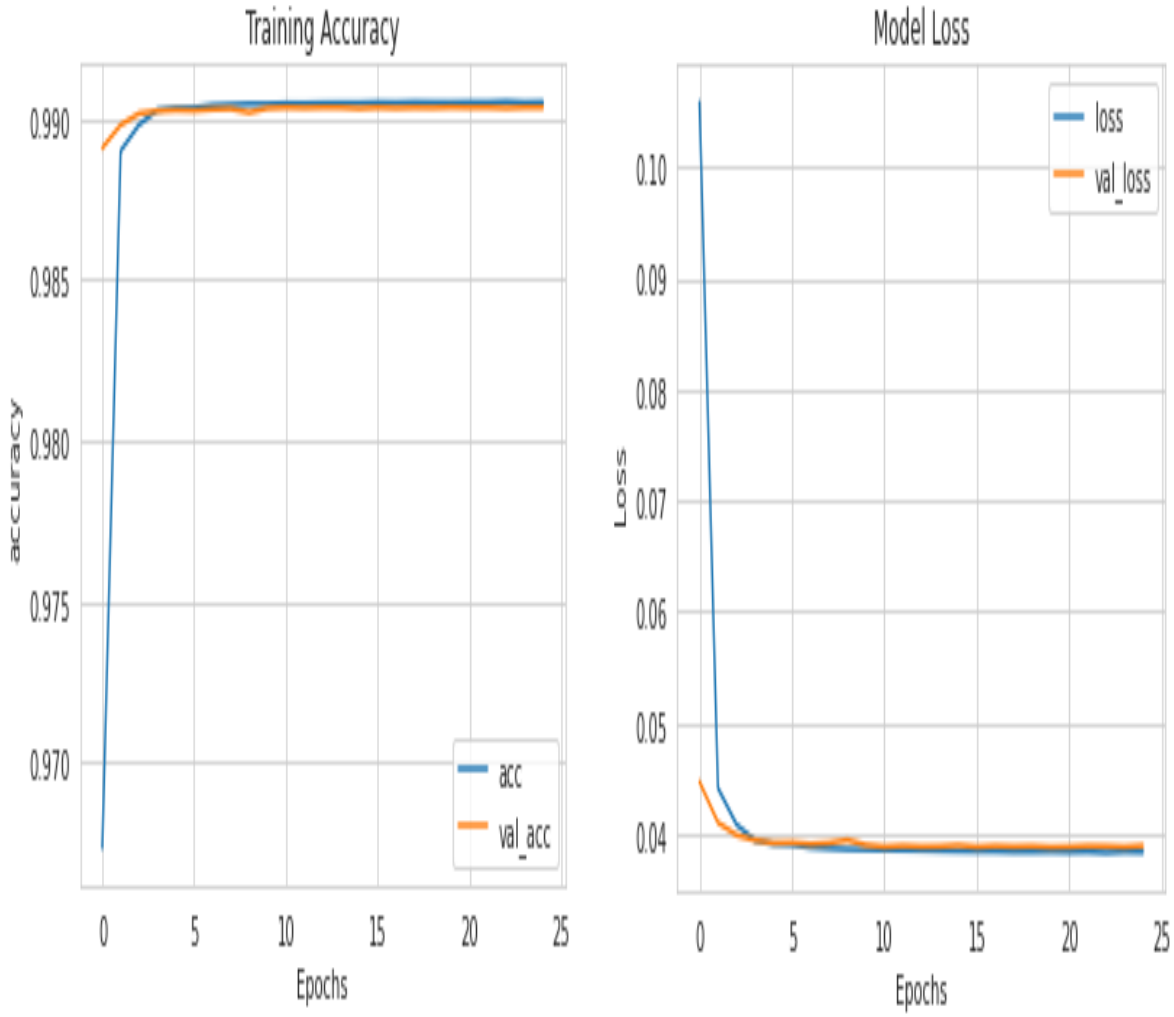

Figure 2: The learning curves of the our system

The Car-Hacking Dataset [14] is used in pur experiment as a publicly available dataset containing a set of experiments on a real vehicle that was conducted to identify possible in-vehicle cyber-attacks. The dataset was collected in a controlled environment, and it consists of a total of 3,225,928 CAN bus messages collected over a period of two months. The dataset includes various types of attacks, such as the injection of unauthorized messages, replay attacks, and denial of service attacks, along with normal driving scenarios. The attack category includes four subcategories, each containing a different type of attack. The normal driving category includes five different subcategories representing various driving situations, such as accelerating, braking, and cruising.

DOI: https://doi.org/10.54216/JCIM.080203
Received: May 15, 2021 Accepted: October 16, 2021

Figure 2 display the learning curve to shows the performance of the GRU model on the training and validation sets over different epochs during the training phase. As shown, the model achieves high accuracy on both the training and validation sets, indicating that it is not overfitting. The validation accuracy reaches a plateau after about 20 epochs, suggesting that additional training does not improve the model's performance significantly. Generally, the learning curve demonstr

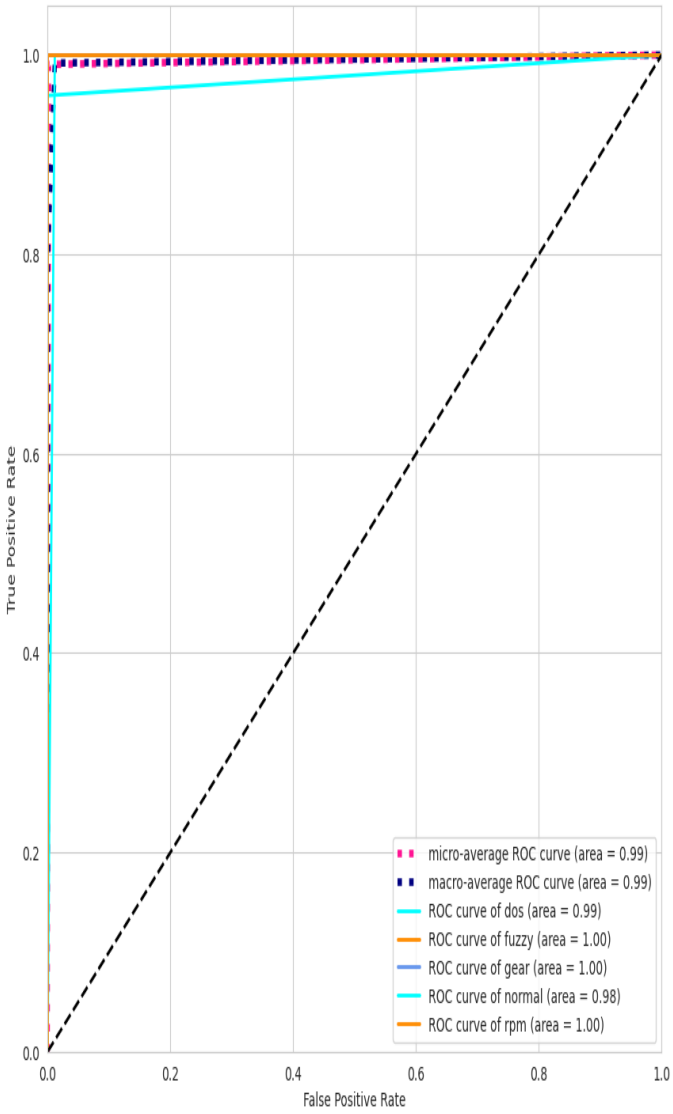

Figure 2: RoC curves for proposed GRU-based in-vehicle attack detection

tes that the GRU model is effective in detecting in-vehicle attacks on the CAN bus network.

The ROC (Receiver Operating Characteristic) curve is displayed in Figure 3 to provide a graphical representation of the performance of our system as its discrimination threshold is varied. The ROC curve for our GRU model shows that the model has a high true positive rate and a low false positive rate, indicating that it is effective in identifying in-vehicle attacks while minimizing the number of false alarms. The area under the curve (AUC) for the ROC curve is 0.99, indicating that the model has a high level of accuracy.

DOI: https://doi.org/10.54216/JCIM.080203
Received: May 15, 2021 Accepted: October 16, 2021

In our experimental analysis, the confusion matrix for the GRU model was presented in Figure 4, with the actual class labels as rows and the predicted class labels as columns. The diagonal elements of the matrix represent the number of correctly classified samples, while the off-diagonal elements represent misclassified samples. By analyzing the confusion matrix, we can decide which classes are being misclassified and adjust the model accordingly to improve its performance.

Furthermore, we compared the performance of the proposed system with the state-of-the-art ML studies on the same car-hacking dataset, and the results are given in Table 1. The proposed GRU model outperformed all the previous methods in terms of the accuracy, precision, recall, F1-score, and AUC metrics. Therefore, it can be concluded that the GRU model is a promising approach for in-vehicle attack detection compared to the existing ML methods.

Table 1: comparison of the performance of ML methods for in-vehicle attack detection.

	Accuracy	Precision	recall	F1-score	AUC
RF	**97.981**	95.995	97.930	97.039	98.273
SVM	**97.414**	96.680	98.247	97.598	97.149
KNN	**97.934**	95.933	95.439	95.727	96.853
Ours	**99.050**	99.010	99.180	99.110	99.110

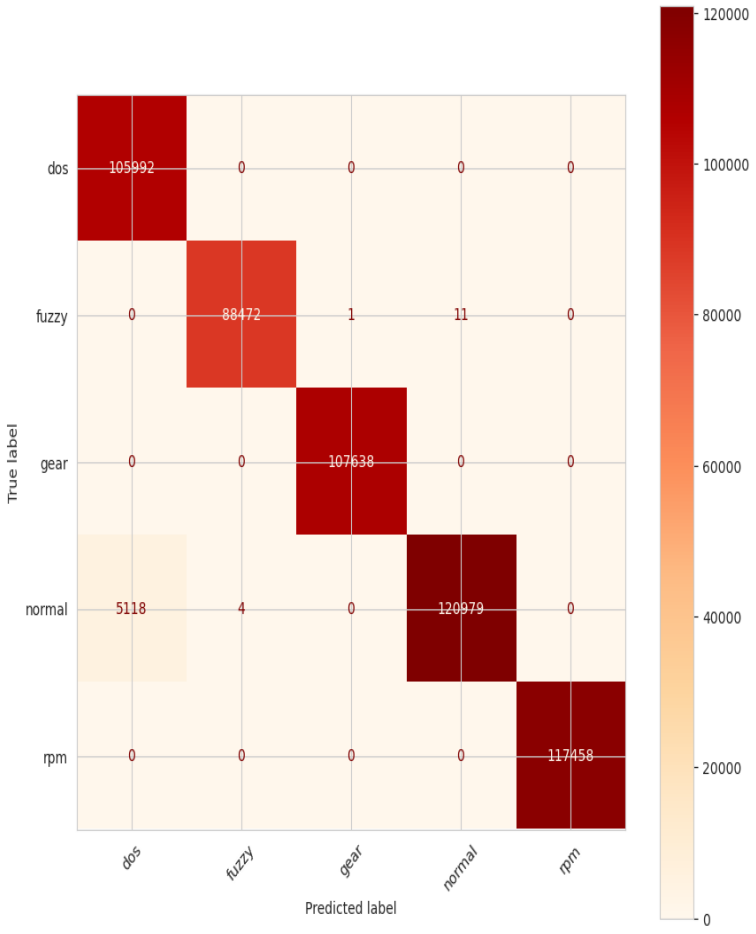

Figure 3: Confusion matrix of the proposed model

DOI: https://doi.org/10.54216/JCIM.080203
Received: May 15, 2021 Accepted: October 16, 2021

5. Conclusion

This study proposed a GRU-based model for in-vehicle attack detection using the car-hacking dataset. The model achieved a high accuracy and a low false-positive rate. The performance of the model was evaluated using various metrics such as precision, recall, F1-score, and the ROC curve. The results showed that the model was effective in detecting in-vehicle attacks and outperformed other existing methods. However, the model's vulnerability to adversarial attacks remains a limitation of our work, indicating the need for further research in this area.

References

[1] Zhang, Jiayan, Fei Li, Haoxi Zhang, Ruxiang Li, and Yalin Li. "Intrusion detection system using deep learning for in-vehicle security." *Ad Hoc Networks* 95 (2019): 101974.

[2] Berger, Ivo, Roland Rieke, Maxim Kolomeets, Andrey Chechulin, and Igor Kotenko. "Comparative study of machine learning methods for in-vehicle intrusion detection." In *Computer Security: ESORICS 2018 International Workshops, CyberICPS 2018 and SECPRE 2018, Barcelona, Spain, September 6–7, 2018, Revised Selected Papers 2*, pp. 85-101. Springer International Publishing, 2019.

[3] Gao, Lulu, Fei Li, Xiang Xu, and Yong Liu. "Intrusion detection system using SOEKS and deep learning for in-vehicle security." *Cluster Computing* 22 (2019): 14721-14729.

[4] Wu, Wufei, Renfa Li, Guoqi Xie, Jiyao An, Yang Bai, Jia Zhou, and Keqin Li. "A survey of intrusion detection for in-vehicle networks." *IEEE Transactions on Intelligent Transportation Systems* 21, no. 3 (2019): 919-933.

[5] Park, Seunghyun, and Jin-Young Choi. "Hierarchical anomaly detection model for in-vehicle networks using machine learning algorithms." *Sensors* 20, no. 14 (2020): 3934.

[6] Hossain, Md Delwar, Hiroyuki Inoue, Hideya Ochiai, Doudou Fall, and Youki Kadobayashi. "An effective in-vehicle CAN bus intrusion detection system using CNN deep learning approach." In *GLOBECOM 2020-2020 IEEE Global Communications Conference*, pp. 1-6. IEEE, 2020.

[7] Lin, Yubin, Chengbin Chen, Fen Xiao, Omid Avatefipour, Khalid Alsubhi, and Arda Yunianta. "An evolutionary deep learning anomaly detection framework for in-vehicle networks-CAN bus." *IEEE Transactions on Industry Applications* (2020).

[8] Xiao, Junchao, Hao Wu, and Xiangxue Li. "Internet of things meets vehicles: sheltering in-vehicle network through lightweight machine learning." *Symmetry* 11, no. 11 (2019): 1388.

[9] Lokman, S. F., Othman, A. T., Musa, S., & Abu Bakar, M. H. (2019). Deep contractive autoencoder-based anomaly detection for in-vehicle controller area network (CAN). *Progress in Engineering Technology: Automotive, Energy Generation, Quality Control and Efficiency*, 195-205.

[10] Barletta, Vita Santa, Danilo Caivano, Antonella Nannavecchia, and Michele Scalera. "Intrusion detection for in-vehicle communication networks: An unsupervised Kohonen SOM approach." *Future Internet* 12, no. 7 (2020): 119.

[11] Song, Hyun Min, Jiyoung Woo, and Huy Kang Kim. "In-vehicle network intrusion detection using deep convolutional neural network." *Vehicular Communications* 21 (2020): 100198.

[12] Mongelli, Maurizio, Marco Muselli, and E. Ferrari. "Achieving zero collision probability in vehicle platooning under cyber attacks via machine learning." In *2019 4th international conference on system reliability and safety (ICSRS)*, pp. 41-45. IEEE, 2019.

[13] Kalkan, Soner Can, and Ozgur Koray Sahingoz. "In-vehicle intrusion detection system on controller area network with machine learning models." In *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1-6. IEEE, 2020.

[14] Seo, Eunbi, Hyun Min Song, and Huy Kang Kim. "GIDS: GAN based intrusion detection system for in-vehicle network." In *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, pp. 1-6. IEEE, 2018.

DOI: https://doi.org/10.54216/JCIM.080203
Received: May 15, 2021 Accepted: October 16, 2021

[15] Barletta, Vita Santa, Danilo Caivano, Antonella Nannavecchia, and Michele Scalera. "A Kohonen SOM architecture for intrusion detection on in-vehicle communication networks." *Applied Sciences* 10, no. 15 (2020): 5062.

[16] Hossain, Md Delwar, Hiroyuki Inoue, Hideya Ochiai, Doudou Fall, and Youki Kadobayashi. "LSTM-based intrusion detection system for in-vehicle can bus communications." *IEEE Access* 8 (2020): 185489-185502.

[17] Minawi, Omar, Jason Whelan, Abdulaziz Almehmadi, and Khalil El-Khatib. "Machine learning-based intrusion detection system for controller area networks." In *Proceedings of the 10th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, pp. 41-47. 2020.

[18] Wang, Yi, Dan Wei Ming Chia, and Yajun Ha. "Vulnerability of deep learning model based anomaly detection in vehicle network." In *2020 IEEE 63rd International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 293-296. IEEE, 2020.

[19] Gherbi, Elies, Blaise Hanczar, Jean-Christophe Janodet, and Witold Klaudel. "Deep Learning for In-Vehicle Intrusion Detection System." In *Neural Information Processing: 27th International Conference, ICONIP 2020, Bangkok, Thailand, November 18–22, 2020, Proceedings, Part IV 27*, pp. 50-58. Springer International Publishing, 2020.

[20] Anzer, Ayesha, and Mourad Elhadef. "Deep learning-based intrusion detection systems for intelligent vehicular ad hoc networks." In *Advanced Multimedia and Ubiquitous Engineering: MUE/FutureTech 2018 12*, pp. 109-116. Springer Singapore, 2019.

[21] Chevalier, Yannick, Roland Rieke, Florian Fenzl, Andrey Chechulin, and Igor Kotenko. "Ecu-secure: Characteristic functions for in-vehicle intrusion detection." In *Intelligent Distributed Computing XIII*, pp. 495-504. Springer International Publishing, 2020.

[22] Loukas, George, Tuan Vuong, Ryan Heartfield, Georgia Sakellari, Yongpil Yoon, and Diane Gan. "Cloud-based cyber-physical intrusion detection for vehicles using deep learning." *Ieee Access* 6 (2017): 3491-3508.

[23] Hossain, Md Delwar, Hiroyuki Inoue, Hideya Ochiai, Doudou Fall, and Youki Kadobayashi. "Long short-term memory-based intrusion detection system for in-vehicle controller area network bus." In *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*, pp. 10-17. IEEE, 2020.

[24] Avatefipour, Omid, Ameena Saad Al-Sumaiti, Ahmed M. El-Sherbeeny, Emad Mahrous Awwad, Mohammed A. Elmeligy, Mohamed A. Mohamed, and Hafiz Malik. "An intelligent secured framework for cyberattack detection in electric vehicles' CAN bus using machine learning." *IEEE Access* 7 (2019): 127580-127592.

[25] Avatefipour, Omid, Ameena Saad Al-Sumaiti, Ahmed M. El-Sherbeeny, Emad Mahrous Awwad, Mohammed A. Elmeligy, Mohamed A. Mohamed, and Hafiz Malik. "An intelligent secured framework for cyberattack detection in electric vehicles' CAN bus using machine learning." *IEEE Access* 7 (2019): 127580-127592.

DOI: https://doi.org/10.54216/JCIM.080203
Received: May 15, 2021 Accepted: October 16, 2021