The Latest Developments and Future Perspectives of Artificial Intelligence Systems for In-Vehicle Communication Intrusion Detection

Gabriel Marvin
dSPACE Engineering d.o.o., Zagreb, Croatia
GMarvin@dspace.hr

***Abstract* - CAN (Controller Area Network) is a message-based protocol that achieves communication by the exchange of packets of data between devices on the network. The protocol is widely used for in-vehicle communication (IVC) in the automotive industry as it is designed to be robust, able to handle a high rate of data transfer and tolerant of the electrical noise. However, the original CAN implementation lacks built in security mechanisms which makes it vulnerable to intrusion attacks that can be detrimental to the driver or the system itself. With the very rapid evolution of artificial intelligence (AI) various intrusion detection systems (IDS) have been developed to tackle the problem of detecting these attacks. This article aims to get a better insight of the current trend of development by surveying the latest approaches in the field of AI based IDSs. A comparison of various known attacks, detection techniques on available benchmark datasets, and a few advanced improvements of current security implementations and limitations are emphasized.**

Keywords - Intrusion Detection Systems, In-Vehicle Communication, Controller Area Network, Artificial Intelligence

I. Introduction

In-vehicle communication (IVC) refers to the interconnected communication between various electronic control systems within a vehicle also known as electronic control units (ECUs). With the advances in automotive technology and market demand, the modern vehicle now contains over 70 ECUs that control various functions within the vehicle [1]. The communication between various ECUs is facilitated by various standard in-vehicle communication protocols, such as CAN, FlexRay, Local Interconnect Network (LIN), Media Oriented System Transport (MOST), Ethernet, etc. In the automotive industry the CAN communication protocol is standardized and widely used because of its robustness, fast data transmission and reliability [2]. Various experimental attacks were performed to showcase and exploit the protocol's shortcomings. Hoppe et al. [3] conducted frame sniffing and replay attacks in a simulated environment to gain control over systems such as window lift, warning lights, and airbags. Similarly, Koscher et al [4] conducted various attacks on a real vehicle and successfully gained control over various modules such as the body control module, radio and engine. To counteract potential cyber threats significant efforts have been made to secure vehicles from security vulnerabilities. As a result, the research is focused on developing intrusion detection systems (IDS)s for in-vehicle networks as a reactive security measure. IDSs can be classified into two categories: signature-based detection and anomaly-based detection [5]. Signature-based IDSs report an intrusion when a match between the known attack and observed events is found. The anomaly-based approach on the other hand only knows what normal behavior looks like and considers deviations from the normal behavior as intrusions. Anomaly-based detection has received more attention due to its ability to detect novel attacks, whereas signature-based detection has limitations, such as the need for frequent database update in form of novel attacks [5]. This work focuses on the application of artificial intelligence (AI) to IVC IDSs and surveys several papers published from December 2022 to January 2023, examining attack types, detection methods, evaluation of available benchmark datasets and evaluation of performance. The paper is organized as follows: In section 2 existing surveys on the subject are discussed. Section 3 serves as a general introduction to the CAN protocol and common attacks on IVNs. Section 4 introduces the novel AI-based IDS methodologies for IVC, the used datasets as well as the training features. Section 5 discusses the limitations and future research directions. Section 6 concludes the paper.

II. Related work

This paper covers exclusively the state of the art (SoA) papers regarding IDS in CAN communication. Hafeez A. [2] reviewed five different fingerprint-based IDS methods for CAN communication. In the context of this work the term fingerprint-based is used to describe a signature-based method that does not necessarily include the use of machine learning (ML) or AI. This study provides a comprehensive introduction to various IDS techniques. The methods are presented in detail as well as their accuracy in detecting spoofing and impersonating attacks on CAN. However, it lacks a review on the used datasets on which these methods are tested. In the work by Karopoulos G. [1] a unified taxonomy for IVC IDSs is provided. The paper does not provide summaries on individual papers. However, a comprehensive description of the publicly available datasets is presented. The survey also discussed the available open-source simulation tools for communication data farming. In [5] the authors studied 44 articles presenting a division of IDSs by categories. They also addressed research challenges and gaps in IVC IDSs. While authors in [6] compare current methods based on criteria such as real-time constraints, hardware types, changes in CAN bus behavior, attack mitigation types, and the software/hardware used to validate these approaches. They conclude with a discussion of the limitations of attack strategies and research challenges for the future. Loukas G. [7] reviewed 13 ML based IDSs for CAN, among other techniques that are not based only on the automotive sector. In [8] the authors introduce a detailed and systematic view of SoA AI-based IDSs for IVC. Focusing on the used methods to detect attacks, evaluation of used benchmark datasets, reviews on possible attacks and evaluation of performance. The AI-based IDSs in the papers are categorized by the features they are developed on. The methods within each category are presented, with emphasis on whether the learning conducted was supervised or unsupervised.

III. Background and terminology

A. CAN Communication Protocol

CAN is a communication protocol used for real-time control of message-based systems. It is robust, efficient, and uses a multi-master broadcast system [2]. The physical characteristics include the transmission of data which is done using a differential signal over a twisted pair of wires. The topology of the network can be either linear or starred, with each node connected to a single communication line. This allows for multiple nodes to transmit and receive messages on the same line.

The CAN bus data frame consists of several components. Some of the components are of great importance to the reviewed papers [8].

1. Start of Frame (SOF): Signifies the beginning of a new data frame and is used to synchronize the nodes on the network.
2. Identifier (ID): A 11-bit or 29-bit identifier used to identify the source and priority of the message.
3. Data Field (DATA): The payload of the data frame, containing up to 8 bytes of data.
4. End of Frame (EOF): Signifies the end of the data frame.
5. Intermission: A period of idle time between the end of one data frame and the start of the next. Used to allow the nodes on the network to process the received data and prepare for the next message.

An illustration of a CAN frame and all its components is shown in Figure 1.

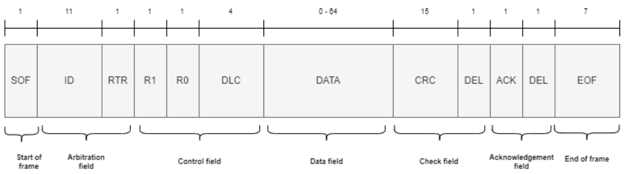

Figure 1: CAN frame

B. Known Attacks

An intruder can gain access to the CAN bus through various means such as wired mediums like the On-Board Diagnostics (OBD) port or USB port, wireless channels such as Global System for Mobile Communication (GSM) or Wi-Fi, and APIs such as SMS, web-interface, and mobile APIs. Once access is gained, the intruder can carry out an attack on a various number of vital processes [8, 9]. Some common attacks are listed below.

1. Denial of Service (DoS): Attacks attempt to disrupt communication services by overwhelming the system with a high volume of frames.
2. Frame Overwrite Attack: The attacker sends frames with a higher priority (lower CAN ID) to overwrite legitimate frames and manipulate the system's behavior.
3. Message Spoofing: Where the attacker sends fake frames that appear to be from a legitimate source to gain unauthorized access or manipulate the system.
4. “Man in the Middle” attack: The attacker intercepts and manipulates communication between nodes, disrupting the flow of data.
5. Replay Attack: where the attacker captures valid frames and retransmits them to the system to gain unauthorized access or manipulate its behavior.
6. Eavesdropping: Where the attacker intercepts and listens to communication between nodes to gain sensitive information.
7. Buffer Overflow Attack: The attacker sends a large number of frames that overflow the system's buffer and causes it to crash.

IV. CAN Bus AI-based IDSs

In this section a review of several papers is conducted. Each reviewed article is devised into five sections: general paper overview, data preprocessing, used method, used dataset, and achieved results.

Zhang H. et al. [10] proposed a novel approach for IDSs, which is based on a graph neural network (GNN) that can detect multiple different attacks: message injection, suspension, and falsification. The IDS is designed to work as a two-stage cascade. In the first stage, a one-class classification layer is used for anomaly detection and the GNN is trained only on normal CAN messages. The second stage determines the specific attack type or labels it as a new attack. The authors provide a detailed analysis of their proposed method by comparing the performance to several other techniques that tackle different attack types. In this way the authors prove the effectiveness of their solution by identifying different attack types. The paper also conducts research to validate the impact of vehicle states on the CAN message contents. The experiment is conducted by comparing two message sequences, with different time periods between messages and then calculating their respective cosine similarities between consecutive messages. With this experiment the authors proved that there is an intrinsic connection between vehicle states and message content variations. A federated approach of training the model is proposed using two different federated learning optimizers. The results indicate that better performance can be achieved using the mentioned optimization techniques. Filtering out malicious participants and preserving privacy and security remains a challenge in federated learning.

Data preprocessing in [10] is implemented by using message graphs to describe CAN message streams. To ensure real-time analysis, CAN messages are analyzed in intervals that take a few milliseconds to process. If the interval is too short the message sequence becomes unstable due to the infrequent transmission of messages with high CAN IDs. This instability has been validated in the work through experiments using a dataset from [11]. The message graph comprises of nodes and edges, where the values of the nodes represent the CAN ID of the frame with an edge pointing to another node. This denotes the sequential transmission of CAN IDs. Each edge carries a bias value representing the number of corresponding message pairs appearing in the given message interval. In this way the authors can simulate the behavior of the connected system. The authors in [12] proposed a method for dividing the data in CAN messages to improve the accuracy of intrusion detection. The method called READ, divides the message contents based on the bit-flip rate, which is the rate at which bits change value. If a bit with a high bit-flip rate is followed by one with a low rate, it is likely that the two bits belong to two different signal behaviors or data blocks. To calculate the bit-flip rate, a certain number of CAN messages need to be collected for each CAN ID. Finally, to prepare the data for use in a GNN design, the authors need to describe all the CAN message contents using a node matrix. After applying the READ method, the message contents with different CAN IDs will be separated into different data blocks, each of which is then converted to a decimal number.

The IDS method uses graph learning as it increased in attention in recent years. The proposed CAN bus IDS is based on graph level algorithms. All three levels of models in graph learning start with graph convolution layers, and graph level schemes are used for graph classification tasks through the addition of pooling and readout layers. The proposed CAN bus IDS is based on the GNN model in [13]. Multiple convolution layers are stacked to capture graph substructure features at different scales. Pooling and readout layers are introduced for graph classification tasks and a sorting operation to sort nodes according to their structural roles is introduced. This helps solve node indexing issues caused by variations in CAN message graphs due to different driving regimes. The readout layers consist of 1-D convolution layers and dense layers. Due to the difficulty of acquiring intrusions to CAN buses in real vehicles, the first-stage classifier is designed as an anomaly detection IDS with a one-class classification layer or Support Vector Data Descriptor (SVDD) and only normal CAN bus data will be used for training. The whole architecture of the GNN, except the last one-class classification layer will be considered and the training process will be conducted using mini-batch stochastic gradient descent (SGD). After the anomalies have been filtered by the first-stage classifier, the second-stage classifier takes over the specific attack classification. To address new unknown anomalies the second-stage classifier includes a layer based on meta-recognition algorithms [14]. The paper also describes a novel federated learning strategy as a type of distributed ML where a cloud server works with multiple local users to train a model. During this process each local device trains a model using its own data and only sends the model parameters to the cloud server for optimization. Two federated learning schemes are evaluated [15, 16] in the proposed model. This allows vehicles in varying conditions to train their local model based on the optimized parameters on the cloud.

Two evaluation datasets are used to evaluate the performance of the proposed model with different attack types. The first is collected on a Ford Transit 500 and separated into three sets. The first set is composed of normal CAN messages while the remaining two sets include message injection attacks. In the second and third sets, the CAN IDs related to vehicle speed and revolutions per minute (rpm) are targeted and compromised CAN messages are randomly injected into these two datasets after specified time intervals. The second evaluation dataset is the CAN Signal Extraction and Translation Dataset provided by the Hacking and Countermeasure Research Lab (HCRL) and includes anomalies with five attack types: DoS, fuzzy, suspension, replay, and spoofing. The first dataset in the first baseline is used as the training set. Three baselines [16, 17, 18] are selected to test the GNN. The comparison between the proposed IDS and the first baseline is performed to demonstrate the former's effectiveness in detecting CAN message injection attacks. The second and third baselines are used to test the effectiveness of the GNN to identify other types of attacks with the metrics accuracy, precision, recall, and F1-score. The three intrusion detection strategies in the first baseline are thresholds for Cosine Similarity (CS), thresholds for Pearson Correlation (PC) and statistical CAN message sequence reconstruction using Long-Short Term Memory (LSTM). In the second and third baseline the detection strategies that are compared against the authors models are also LSTM and a CNN-LSTM model named CLAM.

The results are presented taking into consideration various perspectives of the model to correctly estimate its place with the mentioned baseline models. The GNN outperforms all first baseline models in all accuracy metrics. However, the model is not so successful at predicting replay attacks as the CLAM model. A scalability evaluation is also performed where the model displayed negligible difference in accuracy in respect to the message interval length. In terms of the federated training approach the results show that using the scheme from [16] greatly improves accuracy in this scenario.

Zhao Y. et al. [19] introduces the Same Origin Method Execution (SOME) attack, an advanced variation of a masquerade attack. It can imitate the frequency of messages without changing the ID sequence on the CAN bus while sending attack information. At the same time a GAN-based Vehicle IDS (GVIDS) is proposed to counter the SOME attack. Tests on real vehicles show that GVIDS trained only on SOME can detect various attacks, including spoofing [25], bus-off [26], masquerade [27] and SOME with an average accuracy of 96.64% and a detection time of 0.18 ms. However, the novel method is only tested in controlled environments, but it's planned to evaluate its robustness in more complex environments.

Data preprocessing for GVIDS utilizes one-hot encoding to transform the data into CAN images, reducing the time cost for training and detection. It converts the data of 16 consecutive frames of the CAN bus into a single CAN image. To standardize the data, GVIDS supplements data segments of varying lengths to 8 bytes before encoding. The 16 CAN data frames are transformed into a 64 × 64 CAN image through one-hot encoding.

The IDS method used in this paper is GAN. A ML model composed of a generator (G) and a discriminator (D) that work together to generate data with the characteristics of the training set. G learns the characteristics of the training data to generate new data to further train D, while D distinguishes real data from false data generated by G. The GAN model adopts the GANomaly [20] network training model. The model consists of a G, D, and a reconstruction network (E). G is further composed of an encoder and decoder while E and D have similar structures to the encoder. During training, the input image is compressed into a vector, which is then regenerated into an output image. D discriminates between the output image and the generated image, based on a threshold value to determine an anomaly or normal data.

The model's training dataset is collected from two different vehicles (Luxgen U5 and Buick Regal). For each vehicle 1 million of normal CAN message images are collected. Several different evaluations are conducted to represent the results. The quality of the model was evaluated by a receiver operating characteristic (ROC) curve to plot the false positive rate (FPR) against the true positive rate (TPR) of the model. The best performance of the ROC curve is reached when the FPR is less than 0.1 and the TPR is greater than 0.9. The performance of the model is further evaluated using area under curve (AUC) metric. A higher AUC value, closer to 1, indicates a better performance of the model. In Luxgen, the AUC values for four different attacks are 0.9941 (spoofing), 0.9787 (bus-off), 0.9768 (masquerade), and 0.976 (SOME) respectively. Similarly, the AUC values for the same four attacks in Buick are 0.9982, 0.9778, 0.9665, and 0.9662 respectively. The intrusion detection accuracy for both individual vehicles was over 0.9600 for Luxgen and over 0.9312 for Buick. The real-time performance of GVIDS was analyzed by measuring the running time of intrusion detection in Luxgen and Buick. The average running time for both vehicles was 0.18 ms and it was enough to meet the requirements for the transmission of data frames in CAN bus networks.

The results show that the intrusion detection running time of GVIDS is minimal and can meet the demand for real-time detection.

Al-Jarrah O. Y. et al. [21] proposed a ML based IDS that creates high-level representations of CAN messages transmitted on the bus using the temporo-contextual dependencies between messages in a time frame and individual message data. These two representations are processed by two neural networks designed to detect novel intrusions by combining the views. The performance of the proposed IDS was evaluated and compared to SoA detection methods like Decision Trees (DT), Random Forests (RF) [22] and a deep learning-based IDS from [23]. The results show that the proposed IDS outperforms these methods in various evaluation metrics.

The data preprocessing was done by selecting a timespan that would result in the capture of 10 messages at a time. This enables the authors to construct recurrence plots (RP) that consist of nine CAN messages. The authors use this approach to capture the contextual information which resulted in the sending of the last message. The RP is the first input to the model while the second input is the payload of the last message in the set. Considering that not every CAN message contain exactly 8 bytes of data, the authors resort to padding the payload with values of -1 to create a uniform dataset.

The IDS method requires two views of the received CAN data, the first view from the data of one CAN message and the second from its temporal context represented in RP format. A LSTM neural network is trained using a stream of individual messages while a convolutional LSTM is trained using the generated RPs. The two LSTMs results are combined to form the input feature vector for a dense neural network that classifies each message as normal or intrusion. The performance of the model was evaluated using the "CAN-intrusion-dataset" [24]. The dataset contains 4 types of attacks, including DoS, rpm and gear spoofing attacks and fuzzy attacks. The DoS, rpm and gear spoofing attacks were used as the training dataset, while the fuzzy attack was used as the testing dataset to measure the performance of the different intrusion detection models. The proposed model was compared to other ML algorithms in literature, including DT and RF, as well as a deep learning approach [23].

The results showed that the proposed model using both inputs achieved the highest accuracy, with a marginal drop in precision, while keeping a low FPR in comparison with the DT, RF [22] and the model used in [23]. The results also showed that using a combination of both views gives the best results in comparison with using one or the other. Table 1 aims to provide a concise and comprehensive summary of the key aspects of each reviewed paper.

TABLE I. COMPARISSON OF THE REVIEW ARTICLES

Reference	[10]	[19]	[21]
Algorithm	GNN	GAN	LSTM
Dataset	[11], [10]	N/A	[24]
Attacks	DoS, fuzzy, suspension, replay, spoofing	SOME [19], spoofing, bus-off, masquerade	DoS, fuzzy, spoofing
Advantages	Brings to attention that different vehicle states caused by variations in message graphs. Detailed analysis on run-time performance and comparison with relevant models.	Dataset collected from multiple vehicles, real time performance analysis, training model on advanced SOME attack shows generalization on other types of attacks.	Individual CAN frames are evaluated as well as their temporo-contextual dependencies.
Limitations	The evaluation of the federated learning approach was conducted on one dataset.	Lacks detailed comparison with more recent deep learning implementations. The driving conditions, number of ECUs and their functions are not mentioned.	Lacks detailed comparison with more recent deep learning implementations. Labeling each individual message may affect the run time performance of the model.

V. Discussion

This paper focused on reviewing the most recent papers in AI-based IDS for IVC. The survey is conducted by summarizing the reviewed papers in several main sections that represent common aspects in all the articles. In this section a discussion is conducted based on the findings, limitations, and future improvements of the reviewed methodologies.

A. Findings

By analyzing the reviewed papers several findings have been made. All the papers display similar trends of research such as the concern for development of models that can detect unknown cyber-attacks, the common use of unsupervised detection techniques primarily based on benign data, feature set selection and used datasets. The biggest concern is to adapt the models to detect attacks based only on benign data. To tackle this requirement researchers in the reviewed papers have turned mostly to unsupervised learning algorithms, which result in better results in detecting previously unknown attacks in comparison with supervised learning methods. Used detection models are GAN, GNN and LSTM which all display great adaptability to variations in the environment and ability to distinguish anomalies from one class data. In the case of GAN and GNN with federated learning a great degree of accuracy is achieved in novel attack detection. This further solidifies the findings in [8]. The use of unsupervised learning models greatly eases the data collection process as it requires only benign data for training. Datasets containing malicious messages and attack tactics at this point are only required to test the models. The selection of the dataset feature sets have also a great impact on the generalization capabilities of the model as on the learning process. The vast amount of different vehicle models and car manufacturers lead to a great amount of diversity in message streams. This has led researchers to search for alternative ways to create feature sets that will lead to training of more generalized models. All the reviewed papers propose methods to extract features from the datasets by either new representations of the dataset like in the works [10, 19] or creating new features as in [21].

VI. Limitations and future improvements

The learning capabilities of AI methods are primarily impacted by the quality of the learning datasets. Due to the low quality of the publicly available datasets, it is often required to create new datasets which can lead to poor translation to real world environments. This process can be resource consuming as unsupervised learning algorithms required large amount of data to generalize properly. This issue is further amplified with the need for datasets that describe daily routines of individual vehicles. The paper [10] takes note of this drawback and proposes by considering the different variations of message streams due to driving conditions, which is also a viable point in the argument of poor datasets. The federated learning approach could be promising in the future coupled with a great amount of data gathered by individual vehicles in different driving conditions. Highly specialized software for ECU communication simulation could be used to farm a great amount of data under different driving conditions.

VII. Conclusion

This paper provides a comparative review of three of the most recent AI-based IDSs for the CAN protocol (December 2022 to January 2023). The reviewed papers are categorized based on the training and testing datasets used, the preprocessing methodology and the AI algorithms used. The reviewed papers are significant as they all highlight the importance of creating a system that is aware of the context from which the CAN frame is coming from, to be able to predict the anomalies in the bus. It is important to mention that the impact on the field of research may not be clear as the papers are published in a short time range of only three months, but they suggest that the trend of research they represent is a current and active area. The findings of the paper also highlight the crucial role that high quality datasets play in the development of effective AI-based IDSs and propose several key improvements that can be made to existing systems.

References

[1] G. Karopoulos, G. Kambourakis, E. Chatzoglou, JL. Hernández-Ramos, V. Kouliaridis, "Demystifying In-Vehicle Intrusion Detection Systems: A Survey of Surveys and a Meta-Taxonomy". Electronics. 2022; 11(7):1072. https://doi.org/10.3390/electronics11071072

[2] A. Hafeez, K. Rehman and H. Malik, "State of the Art Survey on Comparison of Physical Fingerprinting-Based Intrusion Detection Techniques for In-Vehicle Security," SAE Technical Paper 2020-01-0721, 2020, doi:10.4271/2020-01-0721.

[3] T. Hoppe, S. Kiltz, and J. Dittmann. "Security threats to automotive CAN networks practical examples and selected short-term countermeasures". In International Conference on Computer Safety, Reliability, and Security., Springer, 235-248., 2008.

[4] K. Koscher et al., "Experimental Security Analysis of a Modern Automobile," 2010 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2010, pp. 447-462, doi: 10.1109/SP.2010.34.

[5] O. Y Al-Jarrah, C. Maple, M. Dianati, D. Oxtoby, and A. Mouzakitis. "Intrusion detection systems for intra-vehicle networks: A review". IEEE Access 7 (2019), 21266-21289.

[6] E. Aliwa, O. Rana, C. Perera, and P. Burnap. 2021. "Cyberattacks and Countermeasures for In-Vehicle Networks". ACM Comput. Surv. 54, 1, Article 21 (January 2022), 37 pages. https://doi.org/10.1145/3431233

[7] G. Loukas, E. Karapistoli, E. Panaousis, P. Sarigiannidis, A. Bezemskij, and T. Vuong. 2019. "A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles". Ad Hoc Networks 84 (2019), 124-147.

[8] S. Rajapaksha, H. Kalutarage, M. O. Al-Kadri, A. Petrovski, G. Madzudzo, and M. Cheah. "AI-based Intrusion Detection Systems for In-Vehicle Networks: A Survey". 2022. ACM Comput. Surv. https://doi.org/10.1145/3570954

[9] S. V. Kumar, G. A. A. Mary, P. Suresh and R. Uthirasamy, "Investigation On Cyber-Attacks Against In-Vehicle Network," 2021 7th International Conference on Electrical Energy Systems (ICEES), Chennai, India, 2021, pp. 305-311, doi: 10.1109/ICEES51510.2021.9383720.

[10] H. Zhang, K. Zeng and S. Lin, "Federated Graph Neural Network for Fast Anomaly Detection in Controller Area Networks," in IEEE Transactions on Information Forensics and Security, doi: 10.1109/TIFS.2023.3240291.

[11] L. b. Othmane, L. Dhulipala, M. Abdelkhalek, N. Multari and M. Govindarasu, "On the Performance of Detecting Injection of Fabricated Messages into the CAN Bus," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 468-481, 1 Jan.-Feb. 2022, doi: 10.1109/TDSC.2020.2990192.

[12] M. Marchetti and D. Stabili, "READ: Reverse Engineering of Automotive Data Frames," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 4, pp. 1083-1097, April 2019, doi: 10.1109/TIFS.2018.2870826.

[13] M. Zhang, Z. Cui, M. Neumann, and Y. Chen. 2018. "An end-to-end deep learning architecture for graph classification". In Proceedings of the Thirty-Second AAAI Conference on Artificial Intelligence and Thirtieth Innovative Applications of Artificial Intelligence Conference and Eighth AAAI Symposium on Educational Advances in Artificial Intelligence (AAAI'18/IAAI'18/EAAI'18). AAAI Press, Article 544, 4438–4445.

[14] P. Zhang, J. Wang, A. Farhadi, M. Hebert and D. Parikh, "Predicting Failures of Vision Systems," 2014 IEEE Conference on Computer Vision and Pattern Recognition, Columbus, OH, USA, 2014, pp. 3566-3573, doi: 10.1109/CVPR.2014.456.

[15] T. Li et al., "Federated optimization in heterogeneous networks," arXiv:1812.06127., 2018.

[16] M. Jedh, L. Ben Othmane, N. Ahmed and B. Bhargava, "Detection of Message Injection Attacks Onto the CAN Bus Using Similarities of Successive Messages-Sequence Graphs," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4133-4146, 2021, doi: 10.1109/TIFS.2021.3098162.

[17] A. Taylor, S. Leblanc and N. Japkowicz, "Anomaly Detection in Automobile Control Network Data with Long Short-Term Memory Networks," 2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA), Montreal, QC, Canada, 2016, pp. 130-139, doi: 10.1109/DSAA.2016.20

[18] H. Sun, M. Chen, J. Weng, Z. Liu and G. Geng, "Anomaly Detection for In-Vehicle Network Using CNN-LSTM With Attention Mechanism," in IEEE Transactions on Vehicular Technology, vol. 70, no. 10, pp. 10880-10893, Oct. 2021, doi: 10.1109/TVT.2021.3106940.

[19] Y. Zhao, Y. Xun, J. Liu and S. Ma, "GVIDS: A Reliable Vehicle Intrusion Detection System Based on Generative Adversarial Network," GLOBECOM 2022 - 2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 2022, pp. 4310-4315, doi: 10.1109/GLOBECOM48099.2022.10001410

[20] S. Akcay, A. Atapour-Abarghouei, T.P. Breckon (2019). "GANomaly: Semi-supervised Anomaly Detection via Adversarial Training," In: Jawahar, C., Li, H., Mori, G., Schindler, K. (eds) Computer Vision – ACCV 2018. ACCV 2018. Lecture Notes in Computer Science(), vol 11363. Springer, Cham. https://doi.org/10.1007/978-3-030-20893-6_39

[21] O. Y. Al-Jarrah, K. E. Haloui, M. Dianati and C. Maple, "A Novel Intrusion Detection Method for Intra-Vehicle Networks Using Recurrence Plots and Neural Networks," in IEEE Open Journal of Vehicular Technology, doi: 10.1109/OJVT.2023.3237802.

[22] T. P. Vuong, G. Loukas, D. Gan and A. Bezemskij, "Decision tree-based detection of denial of service and command injection attacks on robotic vehicles," 2015 IEEE International Workshop on Information Forensics and Security (WIFS), Rome, Italy, 2015, pp. 1-6, doi: 10.1109/WIFS.2015.7368559.

[23] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon and D. Gan, "Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning," in IEEE Access, vol. 6, pp. 3491-3508, 2018, doi: 10.1109/ACCESS.2017.2782159.

[24] E. Seo, H. M. Song and H. K. Kim, "GIDS: GAN based Intrusion Detection System for In-Vehicle Network," 2018 16th Annual Conference on Privacy, Security and Trust (PST), Belfast, Ireland, 2018, pp. 1-6, doi: 10.1109/PST.2018.8514157.

[25] E. Seo, H. M. Song and H. K. Kim, "IDS: GAN based Intrusion Detection System for In-Vehicle Network," 2018 16th Annual Conference on Privacy, Security and Trust (PST), Belfast, Ireland, 2018, pp. 1-6, doi: 10.1109/PST.2018.8514157.

[26] K. Cho and K. G. Shin,. "Error Handling of In-vehicle Networks Makes Them Vulnerable." In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). Association for Computing Machinery, New York, NY, USA, 1044–1055. https://doi.org/10.1145/2976749.2978302

[27] K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in 25th USENIX Security Symposium (USENIX Security 16), 2016, pp. 911–927.