2024 IEEE/CIC International Conference on Communications in China (ICCC) | 979-8-3503-7841-2/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICCC62479.2024.10681772

A&D Graph-Based Graph Neural Network Intrusion Detection for In-Vehicle Controller Area Network

Yaru He$^{(1)}$, Jiaqi Gao$^{(1)}$, Mingrui Fan$^{(2)}$, Daoqi Han$^{(2)}$, Yueming Lu$^{(2)}$, Yaojun Qiao$^{(1,*)}$
$^{(1)}$*State Key Laboratory of Information Photonics and Optical Communications*
Beijing University of Posts and Telecommunications
$^{(2)}$*Key Laboratory of Trustworthy Distributed Computing and Service, Ministry of Education*
Beijing University of Posts and Telecommunications
Beijing, China
qiao@bupt.edu.cn

Abstract—**The rapid advancement of the Internet of Vehicles (IoV) has significantly enhanced the diversity and intelligence of Electronic Control Units (ECUs) within the Controller Area Network (CAN) of vehicles. Implementing an effective Intrusion Detection System (IDS) is paramount for ensuring the security of the in-vehicle CAN. Traditional approaches in intrusion detection often rely on single-sample analysis, demanding extensive labeled data. To circumvent this limitation, a graph-based IDS that eliminates the necessity for single-sample labeling becomes imperative. Nonetheless, existing graph-based IDS models encounter the challenge of achieving high accuracy, especially for impersonation attacks. In this paper, we propose Arbitration&Data graph-based Graph Neural Networks (A&D-GNN) IDS to improve detection accuracy for in-vehicle CAN effectively. The proposed A&D-GNN IDS can significantly improve detection accuracy for impersonation attacks, which includes the Arbitration&Data (A&D) graph construction algorithm, representation learning, and intrusion detection. Based on the CAN message characteristics, the A&D directed attribute graph can extract comprehensive information, including information about both the arbitration field and the data field in the CAN message frame, notably, the data field is associated with the arbitration field. Therefore, the following Graph Neural Networks (GNN) with powerful representation capabilities can learn more precise graph-level representations. Lastly, a multi-classification layer is applied to perform intrusion detection. Experimental results on the public benchmark OTIDS dataset show that our proposed model is superior to other models with higher accuracy and an impressive accuracy of 99.92% for impersonation attacks.**

Index Terms—**A&D Graph, Graph Neural Network, Intrusion Detection System, Controller Area Network**

I. Introduction

Communication and information security are essential for protecting sensitive data, ensuring communication privacy, and safeguarding against unauthorized access or malicious attacks. The development of the Internet of Vehicles (IoV) is changing the transportation field, but it also brings security challenges. Smart connected vehicles involve a variety of communication scenarios and sensitive data and have become an important target for hacker attacks. In 2021, the upstream security research team published a global automotive cybersecurity report, analyzing 633 publicly disclosed incidents over the past decade [1]. The report highlights a significant increase in cyberattacks targeting smart connected vehicles. Therefore, ensuring information and communication security has become an important task in the development of the IoV. For a smart connected vehicle, the potential attack surfaces include Controller Area Network (CAN), Vehicle-to-Everything (V2X) communication, Bluetooth connections, and the On-Board Diagnostics (OBD) port. Among all potential attack surfaces, the in-vehicle CAN is particularly susceptible to attacks [2]. The CAN protocol is a widely used In-Vehicle Network (IVN) communication standard, prevalent in both academic literature and practical applications. The microprocessor-based Electronic Control Units (ECUs) communicate through the CAN, which acts as a broadcast medium. CAN utilizes a lossless bit-wise arbitration method to resolve contention during data transmission among various ECUs in vehicles.

However, the CAN protocol has several vulnerabilities, including the absence of authentication, broadcast transmission, lack of encryption, ID-based priority scheme, and open interfaces. Attackers can easily enter the bus system and manipulate data, seriously threatening CAN security and human lives. Consequently, an effective Intrusion Detection System (IDS) to mitigate these vulnerabilities and counter potential cyber threats for in-vehicle CAN is essential. Some works treat the CAN message as a single-sample [3], [4], which require a large amount of labeled data, and labels are difficult to obtain in the real world. Single-sample methods ignore connections between adjacent CAN messages, while graph-based methods provide a new approach to circumvent this issue [5], eliminating the need for single-sample labeling. Islam and colleagues [6] utilized graph theory along with real CAN message data to build a directed graph illustrating the message sequence. They applied the chi-squared test to detect abnormal CAN data. Refat et al. [7] constructed a graph, extracted diverse graph statistical properties, and then inputted the statistical features into Support Vector Machines (SVM) and K-Nearest Neighbors (KNN) for classification. However, constructing a simple graph and extracting statistical features may hinder the ability to capture effective features from the raw CAN message, leading to reduced IDS accuracy, especially for impersonation attacks.

In this paper, we propose Arbitration&Data graph-based Graph Neural Networks (A&D-GNN) IDS to improve detection accuracy for in-vehicle CAN effectively. The proposed

979-8-3503-7841-2/24/$31.00 ©2024 IEEE

A&D-GNN IDS includes the Arbitration&Data (A&D) graph construction algorithm, graph-level representation learning, and intrusion detection. Initially, based on the CAN message characteristics, we construct the A&D directed attribute graph to represent the CAN messages frame within a window. Notably, the A&D graph utilizes both the arbitration and data fields, and the data field is associated with the arbitration field. Subsequently, graph-level representations of the A&D graph are extracted by employing the Graph Neural Networks (GNN) model with powerful representation capabilities. The introduction of the A&D directed attribute graph with comprehensive information aims to enhance the pattern recognition capabilities of the GNN. Lastly, a multi-classification layer is applied to perform intrusion detection. In summary, by constructing the A&D directed attribute graph and utilizing GNN model, the proposed A&D-GNN IDS can address the problem of low accuracy. Experimental results on the public benchmark OTIDS dataset showcase the superior effectiveness of our proposed model in comparison to several state-of-the-art models. Our contributions are summarized as follows:

- We propose A&D-GNN IDS to address the issue of low accuracy. The GNN is employed to extract graph-level representations from the A&D graphs, facilitating subsequent intrusion detection.
- We design an efficient algorithm for constructing the A&D directed attribute graph that fully utilizes the original information. Specifically, we model the in-vehicle CAN using both the arbitration and data fields in the original CAN message frame within a window.
- Our A&D-GNN IDS is evaluated using a benchmark dataset, demonstrating its superiority over various state-of-the-art methods, and achieving an impressive accuracy of 99.92% for impersonation attacks.

The subsequent sections of the paper begin with related work in Section II, followed by an exploration of the preliminaries in Section III. Section IV offers a detailed exposition of the constructed graph and the proposed model, while Section V presents experimental comparisons between the proposed model and alternative approaches, along with result analysis. Finally, Section VI provides concluding remarks for the paper.

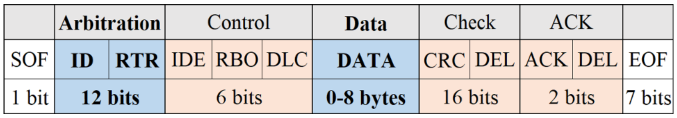
II. Related Work

In this section, we provide an overview of the relevant literature [8] concerning the construction of graphs using CAN messages and representation learning based on graphs.

Building Graphs with CAN Messages. The concept of structuring CAN messages as graphs has gained significant attention since Riadul Islam et al. [6] introduced a graph-based defense system for the CAN. The unique characteristics of CAN messages have made this topic increasingly popular in research. In their work [6], the nodes of the graph represent the arbitration IDs of the CAN, with edges between nodes indicating sequential CAN messages. The direction of the edge signifies the order of message sequences. Subsequent studies [7], [9] adopted a similar graph architecture. More recent works have incorporated additional information from CAN messages to construct directed attribute graphs. For instance, in work [10], the time sequence information for each edge in the generated graph is preserved, leading to a notable improvement in detection efficiency. Additionally, Zhang et al. [1] emphasized the potential use of data content within each CAN message to identify message falsification attacks. Differing from the aforementioned methods, another study [11] introduced a novel graph architecture wherein the nodes represent individual CAN messages. Each node is explicitly linked to its five preceding and succeeding adjacent nodes. In cases where fewer than five adjacent nodes exist, connections are established only with the existing neighboring nodes.

Graph-based Representation Learning. Islam et al. [6] transformed the attributes of a graph into distribution features and subsequently applied the chi-square independence test to identify different forms of cyber attacks. In work [8], graph properties were further extracted, and two machine learning algorithms, SVM and KNN, were employed. Reference [10] utilized the variational autoencoder (VAE) to train classifiers without the need for negative samples. Additionally, Islam et al. [12] introduced a novel intrusion detection algorithm, named Graph-based Gaussian Naive Bayes (GGNB), which utilizes graph properties and PageRank-related features for improved performance. Devnath et al. [9] highlighted that their work is the first to apply Graph Convolutional Networks (GCNs) to CAN data for intrusion detection, but the recall value for impersonation attack was only 0.88. Furthermore, work [11] introduced the attention mechanism for graph-based anomaly detection in in-vehicle networks, but only the relationship between adjacent CAN bus messages is considered in each graph.

III. Preliminaries



	Arbitration		Control			**Data**	Check		ACK		
SOF	**ID**	**RTR**	IDE	RBO	DLC	**DATA**	CRC	DEL	ACK	DEL	EOF
1 bit	**12 bits**		6 bits			**0-8 bytes**	16 bits		2 bits		7 bits

Fig. 1. The CAN data frame format, which consists of five fields.

The format of the CAN data frame is visually depicted in Figure 1. The Arbitration Field (CAN ID) is utilized to prioritize messages in situations where multiple ECUs are concurrently transmitting messages. For instance, when two ECUs try to send messages with CAN IDs ‘0x000’ and ‘0xABC’ simultaneously, the message assigned with CAN ID ‘0x000’ gains bus access for frame transmission due to its lower value. The Control Field, which is user-defined, contains message control information. Similarly, the Data Field holds the necessary information for transmission within the CAN, serving as the payload of the CAN data frame with a capacity ranging from 0 to 8 bytes. Additionally, the Check Field is responsible for error detection within the message. Lastly, the acknowledgment (ACK) Field indicates whether the message was received successfully or not. The attack types considered in this paper, as summarized from [13], are as follows:

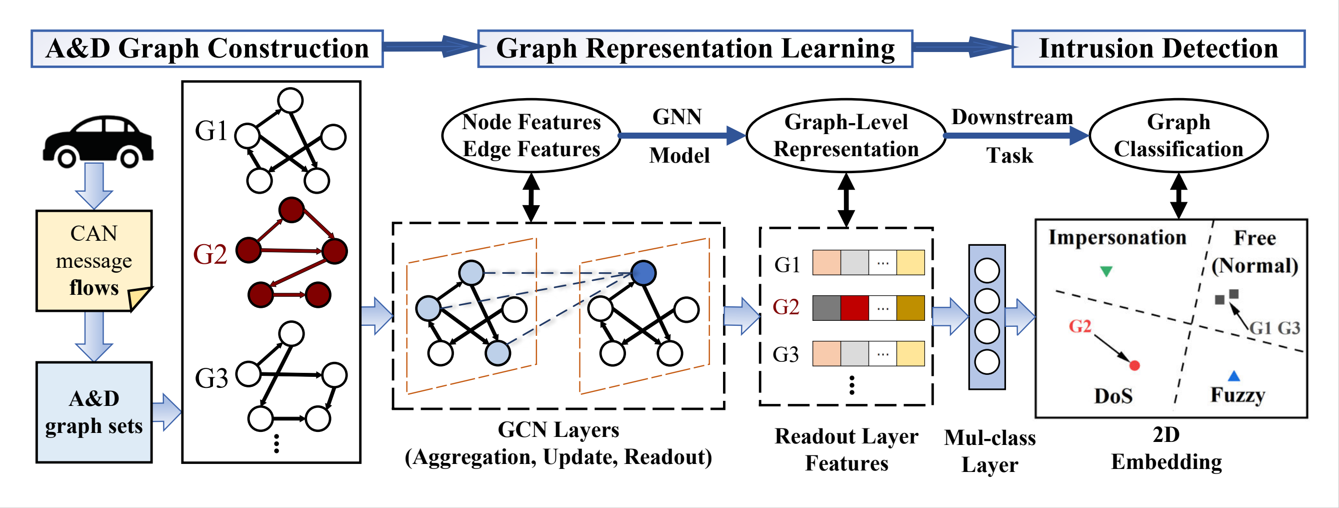


Fig. 2. Workflow of the A&D-GNN IDS, including A&D graph construction, graph representation learning and intrusion detection.

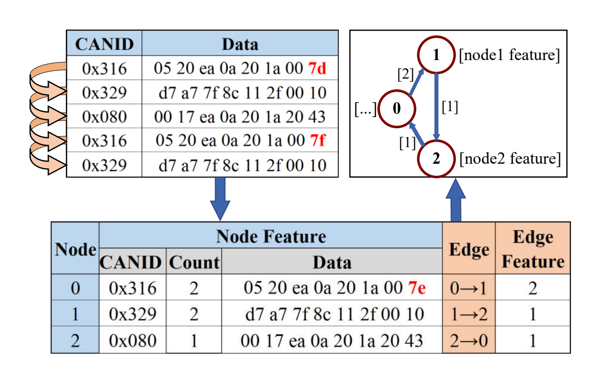
- **Denial-of-Service (DoS) Attack.** An attacker injects high-priority messages into the CAN bus within a short cycle. DoS attack messages are crafted to occupy the CAN bus by continuously injecting legitimate CAN messages with a theoretically highest priority identifier, such as CAN ID ‘0x000’.
- **Fuzzy Attack.** This attack involves the injection of messages with randomly spoofed identifiers and arbitrary data. Unlike the DoS attack, the fuzzy attack aims to paralyze vehicle functions rather than simply delaying normal messages by occupying the CAN bus.
- **Impersonation Attack.** An attacker pretends to be another user or device. In contrast to DoS and fuzzy attacks, the CAN messages of an impersonation attack appear identical to normal CAN messages, both in terms of identifier and data content. This similarity poses significant challenges to intrusion detection systems.

IV. Methodology

The workflow of A&D-GNN IDS encompasses three main stages: graph construction, representation learning, and intrusion detection, as illustrated in Figure 2. Initially, an A&D directed attribute graph is constructed from CAN message flows within a specific time window, effectively modeling network status by utilizing arbitration and data fields. Subsequently, a GNN model is employed to extract graph-level representations through aggregation, update, and readout operations. Finally, the graph-level representations are utilized to train the classifier for intrusion detection.

A. A&D Directed Attribute Graph Construction

To improve the accuracy of future graph-level representations for CAN messages, we exploit the unique properties of CAN messages by effectively constructing A&D directed attribute graphs using arbitration and data fields. CAN messages exhibit distinctive properties: **1) Absence of Source or Destination:** CAN messages do not contain information about their source ECU and destination ECU. **2) Fixed Frequency:** ECUs within the same CAN network typically transmit messages at a relatively fixed frequency, resulting in a stable statistical pattern in the sequences of CAN messages. **3) Cooperative Pairs:** ECUs collaborate, such that when an ECU sends a CAN message with CAN ID ‘A’, the related ECU immediately sends a CAN message with CAN ID ‘B’. **4) Data Consistency:** Over time, the data field in the CAN message with the same CAN ID remains relatively consistent. Therefore, CAN messages within a window reflect the current automobile status, enabling intrusion detection by identifying graph anomalies.



CANID	Data
0x316	05 20 ea 0a 20 1a 00 7d
0x329	d7 a7 7f 8c 11 2f 00 10
0x080	00 17 ea 0a 20 1a 20 43
0x316	05 20 ea 0a 20 1a 00 7f
0x329	d7 a7 7f 8c 11 2f 00 10

Node	Node Feature			Edge	Edge Feature
	CANID	Count	Data		
0	0x316	2	05 20 ea 0a 20 1a 00 7e	0→1	2
1	0x329	2	d7 a7 7f 8c 11 2f 00 10	1→2	1
2	0x080	1	00 17 ea 0a 20 1a 20 43	2→0	1

Fig. 3. Raw CAN messages are converted to A&D directed attribute graph.

Figure 3 depicts the transition from a limited set of five CAN messages to an A&D directed attribute graph. In this graphical representation, CAN IDs are considered as nodes, while consecutive messages are depicted as edges connecting these nodes. The direction of the edges indicates the sequence of messages. In contrast to the CAN message graph described in earlier literature, the A&D graph not only enriches nodes with attributes but also extends attributes to edges. This graphical representation, tailored to the distinctive features of CAN messages, effectively captures the multi-dimensional aspects of the CAN message flow. The node attributes in the A&D diagram include CAN ID, the frequency of CAN ID occurrences, and the average data field value, while the edge attribute signifies the number of connections between two CAN IDs. Figure 4 illustrates an A&D graph constructed from 100 consecutive CAN messages that remained unattacked, labeled "Attack free". The "Parameter Settings" section details the rationale for choosing the window length of 100.

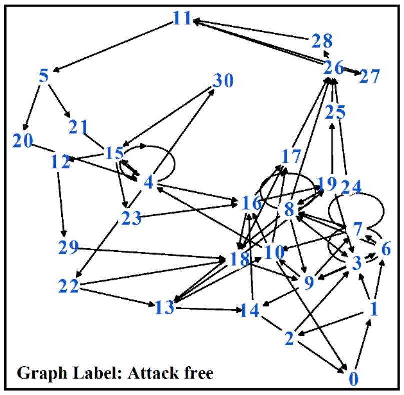


Fig. 4. Labeled "Attack free" A&D graph with a window length of 100.

B. GNN Model for Representation

Upon converting CAN messages into A&D CAN message graphs, we employ two Graph Convolutional Network (GCN) layers and a readout layer to extract graph-level features. Subsequently, the multi-classification layer is utilized to execute downstream graph classification tasks.

GCN Layer. The A&D-GNN IDS utilizes a two-layer GCN to extract representations for each node. The formulation for the feature vectors of the nodes is as follows:

$$H^{k+1} = \sigma\ (\tilde{D}^{-1/2}\tilde{A}\tilde{D}^{-1/2}H^kW^k) \tag{1}$$

where $\tilde{A} = A + I$ denotes the self-connected adjacency matrix of a given undirected graph. $I \in \mathbb{R}^{N\times N}$ denotes the identity matrix. $\tilde{D}$ is a diagonal matrix, Among $\tilde{D}$, each $\tilde{D}_{ii} = \sum_j \tilde{A}_{ij}$. $\sigma(\cdot)$ is the ReLU activation function, specifically defined as $ReLU(x) = max(0, x)$. $W^k \in \mathbb{R}^{F\times F'}$ represents a hierarchical linear transformation matrix that will be optimized during training, F and F' are the dimensions of node representation in the k layer and $k+1$ layer respectively. For a node i, the node update formula can be re-expressed as follows:

$$H_i^k = \sigma\left(\sum_{j\in\{N(i)\cup i\}} \frac{\tilde{A_{ij}}}{\sqrt{\tilde{D}_{ii}\tilde{D}_{jj}}} H_j^{k-1}W^k\right) \tag{2}$$

TABLE I
Statistics Of The Public Benchmark OTIDS Dataset

Type	Num of Sample	Num of Graph
Dos	656579	6566
Fuzzy	591990	5920
Impersonation	995472	9955
Attack Free	2369868	23699

Equation (2) comprises two components: the aggregate function for $N(i)$ and the combine function for all nodes, which are defined as the weighted average of neighbor node representations and the sum of aggregate messages along with node representations themselves. In addition, layer-level neural aggregation functions are GNN modules designed to aggregate contextual information from different hops, which can be expressed as follows:

$$I_v^{(i)(k)} = AGG_{layer}(I_v^{(i)(k-1)}, h_v^{(i)(k)}) \tag{3}$$

where $h_v^{(i)(k)}$ denotes the feature vector of node v at the k-th layer, $I_v^{(i)(k)}$ denotes the aggregate representation of node v in the $(k-1)$ hop domain of the k-th layer.

Readout Layer. After obtaining the updated feature vector for each node, the A&D-GNN IDS needs to merge these vectors into a graph-level representation that encapsulates the entire CAN message graph. While some researchers have proposed more intricate aggregation layers beyond mean, attention, and LSTM, we opt for the mean strategy because it offers faster training convergence and detection speed compared to the alternatives. The formula for the feature vectors of the complete CAN message graph is as follows:

$$g = Mean(h_{v_1}^{(final)}, h_{v_2}^{(final)}, \cdots, h_{v_V}^{(final)}) \tag{4}$$

where $h_{v_i}^{(final)}$ is the final node feature of the node $i, i \in (1, V)$. And g is the N-dimensional graph-level feature calculated by executing the readout function. Finally, a multi-classification layer is applied to perform intrusion detection.

V. Experiments

This section presents the experimental dataset, evaluation metrics, parameter settings of the A&D-GNN IDS model, baseline method for comparison, and a comprehensive display of experimental findings, encompassing visualization outcomes.

A. Dataset and Evaluation Indicators

Our experiments are conducted on the public benchmark CAN dataset OTIDS, released by the Hacking and Countermeasures Research Lab (HCRL) as referenced in [13] and the OTIDS dataset is detailed in Table I. Each record includes a timestamp, CAN ID, number of data bytes, and payload data. It is important to note that the "sample" lacks labels, but the "graph" is labeled.

We adopt accuracy, precision, recall, and F1-score to evaluate the proposed model, which are as follows,

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{5}$$

$$Precision = \frac{TP}{TP + FP} \tag{6}$$

$$Recall = \frac{TP}{TP + FN} \tag{7}$$

$$F1 - score = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{8}$$

where TP, TN, FP, and FN represents the numbers of packets belonging to True Positive, True Negative, False Positive, and False Negative, respectively.

B. Parameter Settings

Empirically, we set the learning rate to 0.001 and maintain a consistent batch size of 64 for both training and testing. The hidden layer size is fixed at 64, with 2 GCN layers utilized. Additionally, the training and testing sets are divided in an 80:20 ratio, with training conducted over 60 epochs.

The window length emerges as a crucial parameter in our experiment. When too small, the CAN message sequence may lack stability, leading to insufficient information for determining specific message states within the window. Conversely, an excessively large window length compromises real-time detection capabilities. Our experiments employ a window length of 100. We performed statistical analyses on the number of nodes and edges within various categories of constructed CAN message graphs, each category comprising 1,000 graphs. Figure 5 illustrates the average nodes and edges, revealing significant variances among CAN message graphs in different categories such as “attack-free,” “DoS,” and “fuzzy.” The results underscore the adequacy of a window length of 100 in capturing these distinctions. The variance between “attack-free” and “impersonation” is minor, which highlights the challenge associated with detecting impersonation attacks.

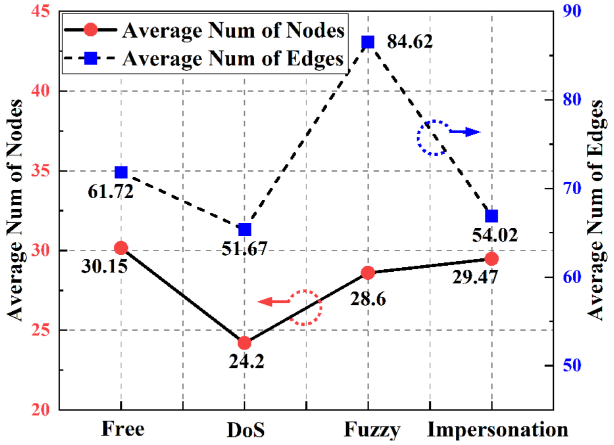


Fig. 5. Average number of nodes (red) and edges (blue) for four different graph categories, which include attack free, DoS attack, fuzzy attack and impersonation attack.

C. Baselines

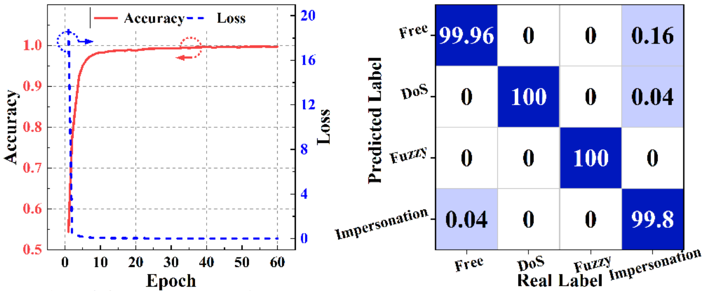
To ensure a fair comparison, our A&D-GNN IDS model is evaluated against several intrusion detection methods based on the OTIDS dataset. These methods include: **1) VGG-16**, which introduced the VGG-16 architecture and trained it to detect various network intrusion patterns for identifying malicious attacks [14]. **2) GB**, which presented a graph-based intrusion detection system comprising four stages and utilizing the chi-squared method [6]. **3) GGNB**, which proposed a novel Gaussian Naive Bayes intrusion detection algorithm based on graphs, incorporating graph properties and PageRank-related features [12].

TABLE II
MULTI-CLASS INTRUSION DETECTION RESULTS OF PROPOSED A&D-GNN IDS.

Type	Precision	Recall	F1-score
Attack Free	0.9996	0.9985	0.9990
DoS	1.0000	0.9994	0.9997
Fuzzy	1.0000	1.0000	1.0000
Impersonation	0.9980	0.9996	0.9988

D. Experiment Results

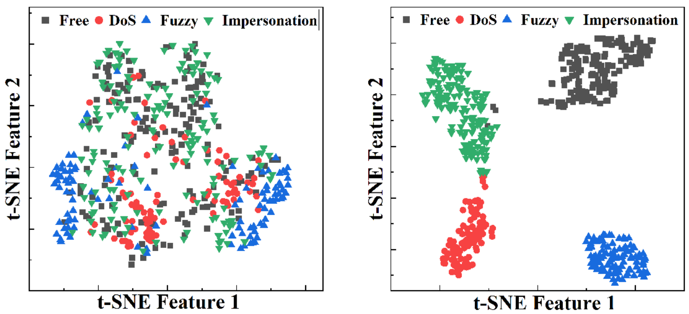
Our A&D-GNN IDS. Employing A&D-GNN IDS, we conducted simultaneous classification of three types of attacks and attack-free instances using the OTIDS dataset. Figure 6 (a) shows the training accuracy and loss variation across epochs, indicating the rapid convergence of the model, thus confirming the effectiveness of the parameter design. Furthermore, Figure 6 (b) presents the multi-class confusion matrix, demonstrating 100% precision for DoS and fuzzy attacks, as well as high precision for attack-free and impersonation attacks at 99.96% and 99.8% respectively. For detailed results, refer to Table II.



(a) Training Accuracy and Loss
(b) Confusion Matrix

Fig. 6. Proposed A&D-GNN IDS experiment results. (a) Training accuracy (red) and loss (blue) curve; (b) Multi-class confusion matrix.

Visualization Results. In order to gain a more intuitive understanding of the impressive performance of the A&D-GNN IDS, we visualized the graph embedding vectors. Initially, we extracted the graph embeddings from both the ‘raw’ data and the data post-classification. Subsequently, we applied the t-Distributed Stochastic Neighbor Embedding (t-SNE) dimensionality reduction algorithm and depicted the visualization outcomes in Figure 7. The comparative results in the visualization highlight the effectiveness of the A&D graph and demonstrate the capability of the graph embedding mechanism in the A&D graph-based GNN IDS to leverage the inherent graph structure present in the CAN message data.



(a) Raw Data

(b) Data After Classification

Fig. 7. Our A&D-GNN IDS visualization results after using t-SNE algorithm. (a) The 'raw' data at epoch 0; (b) The post-classification data at epoch 60.

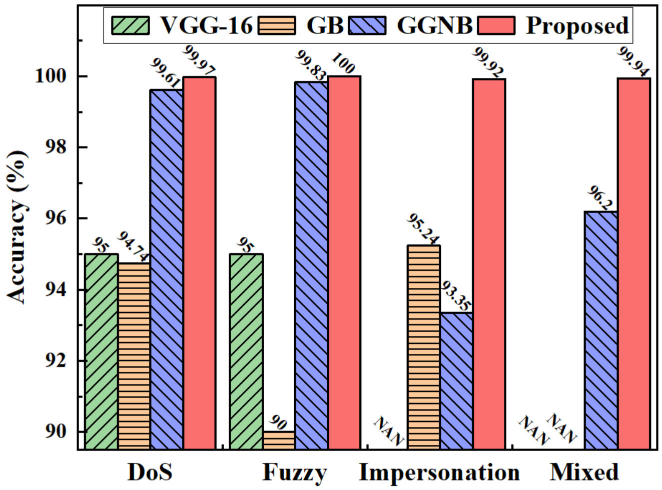


Fig. 8. Incomplete classification accuracy of VGG-16 and GB methods, and complete classification accuracy of GGNB and proposed A&D-GNN methods.

Performance Comparisons. Figure 8 illustrates the classification accuracy of the four methods, among them, VGG-16 and GB cannot detect some attack types. **1) VGG-16** only exhibits low accuracy in detecting DoS attacks and fuzzy attacks. **2) GB** can detect impersonation attacks, but with low accuracy; its detection accuracy for fuzzy attacks is only 90%. **3) GGNB** can detect three types of attacks and mixed attacks, but its accuracy against impersonation attacks and mixed attacks remains relatively low at 93.35% and 96.20% respectively. **4) A&D-GNN IDS** achieves high accuracy in detecting all attack types and mixed attacks, with rates of 99.97%, 100%, 99.92%, and 99.94% respectively. This represents a significant improvement in the detection performance of impersonation attacks and mixed attacks.

VI. Conclusion

In this study, we introduce a novel IDS for in-vehicle CAN networks, named the A&D-GNN IDS, aiming to address the issue of low accuracy, particularly in detecting impersonation attacks. We develop an efficient algorithm for constructing an A&D directed attribute graph by leveraging more available information, including both the arbitration and data fields. This approach enhances the data processing and facilitates the subsequent learning process of the GNN with powerful representation capabilities. Our experimental results on the widely used OTIDS dataset demonstrate the effectiveness of the A&D-GNN IDS model. Our model outperforms existing state-of-the-art models by simultaneously detecting all types of attacks and achieving an impressive accuracy rate of 99.92% specifically for impersonation attacks.

Future Work

For the future work, we will focus on including more attack types and exploiting the timestamps of CAN messages.

Acknowledgment

This work is supported by the National Key R&D Program of China (2022YFB3104900).

References

[1] H. Zhang, K. Zeng, and S. Lin, "Federated graph neural network for fast anomaly detection in controller area networks," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 1566–1579, 2023.

[2] 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," *ACM Computing Surveys*, vol. 55, no. 11, pp. 1–40, 2023.

[3] K. Wang, A. Zhang, H. Sun, and B. Wang, "Analysis of recent deep-learning-based intrusion detection methods for in-vehicle network," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 1843–1854, 2022.

[4] L. Yang, A. Moubayed, and A. Shami, "Mth-ids: A multitiered hybrid intrusion detection system for internet of vehicles," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 616–632, 2021.

[5] X. Ma, J. Wu, S. Xue, J. Yang, C. Zhou, Q. Z. Sheng, H. Xiong, and L. Akoglu, "A comprehensive survey on graph anomaly detection with deep learning," *IEEE Transactions on Knowledge and Data Engineering*, 2021.

[6] R. Islam, R. U. D. Refat, S. M. Yerram, and H. Malik, "Graph-based intrusion detection system for controller area networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 3, pp. 1727–1736, 2020.

[7] R. U. D. Refat, A. A. Elkhail, A. Hafeez, and H. Malik, "Detecting can bus intrusion by applying machine learning method to graph based features," in *Intelligent Systems and Applications: Proceedings of the 2021 Intelligent Systems Conference (IntelliSys) Volume 3*, pp. 730–748, Springer, 2022.

[8] C. S. Wickramasinghe, D. L. Marino, H. S. Mavikumbure, V. Cobilean, T. D. Pennington, B. J. Varghese, C. Rieger, and M. Manic, "Rx-ads: Interpretable anomaly detection using adversarial ml for electric vehicle can data," *IEEE Transactions on Intelligent Transportation Systems*, 2023.

[9] M. K. Devnath, "Gcnids: Graph convolutional network-based intrusion detection system for can bus," *UMBC Student Collection*, 2023.

[10] Y. Meng, J. Li, F. Liu, S. Li, H. Hu, and H. Zhu, "Gb-ids: An intrusion detection system for can bus based on graph analysis," in *2023 IEEE/CIC International Conference on Communications in China (ICCC)*, pp. 1–6, IEEE, 2023.

[11] J. Xiao, L. Yang, F. Zhong, H. Chen, and X. Li, "Robust anomaly-based intrusion detection system for in-vehicle network by graph neural network framework," *Applied Intelligence*, vol. 53, no. 3, pp. 3183–3206, 2023.

[12] R. Islam, M. K. Devnath, M. D. Samad, and S. M. J. Al Kadry, "Ggnb: Graph-based gaussian naive bayes intrusion detection system for can bus," *Vehicular Communications*, vol. 33, p. 100442, 2022.

[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)*, pp. 57–5709, IEEE, 2017.

[14] I. Ahmed, G. Jeon, and A. Ahmad, "Deep learning-based intrusion detection system for internet of vehicles," *IEEE Consumer Electronics Magazine*, vol. 12, no. 1, pp. 117–123, 2021.