Received 24 November 2023, accepted 14 December 2023, date of publication 25 December 2023, date of current version 30 January 2024.

Digital Object Identifier 10.1109/ACCESS.2023.3346943

RESEARCH ARTICLE

CF-AIDS: Comprehensive Frequency-Agnostic Intrusion Detection System on In-Vehicle Network

MD. REZANUR ISLAM[1], MAHDI SAHLABADI[2], (Senior Member, IEEE), KEUNKYOUNG KIM[1], YOONJI KIM[3], AND KANGBIN YIM[2]

[1]Department of Software Convergence, Soonchunhyang University, Asan 31538, South Korea
[2]Department of Information Security Engineering, Soonchunhyang University, Asan 31538, South Korea
[3]Department of Mobility Convergence Security, Soonchunhyang University, Asan 31538, South Korea

Corresponding author: Kangbin Yim (yim@sch.ac.kr)

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.

ABSTRACT Many studies have focused on obtaining high accuracy in the design of Intrusion Detection Systems (IDS) for in-vehicle networks, neglecting the significance of different intensive packet injection techniques. Because of their reliance on scenario-specific training datasets, these IDSs are vulnerable to failing to detect real-world attacks. This study implemented deep learning (DL)–based classification for intrusion detection using a Gated Recurrent Unit (GRU) while considering various intrusion frequencies. Different intrusion frequencies are comprehensively addressed with frequency-agnostic intrusion and resolved by generalizing features for DL input through time series segmentation and frequency domain conversion using Gabor filtering. For training purposes, five types of vehicle data are used, encompassing DoS, fuzzing, and replay attack scenarios. The accuracy range for mechanical version vehicles is typically between 95% and 100%. For electronic vehicles, it is around 90%. Considering the nature of this IDS system, it has been named a Comprehensive Frequency-Agnostic Intrusion Detection System (CF-AIDS). Although this IDS can perform better in all aspects, achieving more efficient results requires a larger amount of situational data.

INDEX TERMS In-vehicle network, CAN, IDS, Gabor transform, frequency-agnostic.

I. INTRODUCTION

In-vehicle networks miss the implementation of encryption and authentication mechanisms and often transmit data to all Electronic Control Units (ECUs) [1]. By utilizing these characteristics, intruders can gain unauthorized access to in-vehicle networks, potentially compromising the security of vehicle operations [2]. Moreover, by incorporating connected vehicle concepts such as Vehicle-to-Everything (V2X) [3], vehicles can engage in continuous data sharing with other vehicles and various infrastructures through Roadside Units (RSUs) and On-Board Units (OBUs), compounding challenges associated with ensuring security and integrity in modern automotive systems [4]. This extended connectivity highlights the importance of Intrusion Detection Systems (IDSs).

IDSs are not always successful, as attackers continually employ various techniques to deceive and evade them. A vulnerability in the security mechanism that can be exploited arises from the attacker's ability to manipulate the injection frequency and employ various data injection patterns [5]. The key aspect of concern here is that this data injection capability is frequency-agnostic, meaning that it can vary with different frequencies as it is not tied to a specific frequency [6]. This characteristic makes the in-vehicle network more susceptible

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Quan.

to intrusion and compromise. In simpler terms, attackers can easily bypass security measures by adjusting how often they inject malicious data and by using different patterns of data injection. This poses a significant risk to the security of the system with complexity, especially when an IDS is developed without considering all of these challenges. To address this challenge effectively, the implementation of a generalized IDS within in-vehicle CAN networks might play a pivotal role. IDS functions are paramount in the detection and mitigation of unauthorized access, abnormal activities, and potential cybersecurity risks [5]. Consequently, they serve as a protective shield, upholding vehicle safety and maintaining data integrity within the continually evolving and interconnected automotive ecosystem.

In-vehicle networks can transmit and receive data through the Controller Area Network (CAN), a specification described previously [7]. Some surveys [8] have prioritized IDS as a means to enhance security within automotive networks. Based on data features used for IDS, IDSs employed in the transportation sector can be categorized into three main types: Flow IDS, Payload IDS, and Hybrid IDS. Flow-based IDS monitors a vehicle's internal network, like the CAN bus, to detect intrusions and unusual activities by analyzing message features such as CAN ID frequency and intervals without inspecting message content. This type of IDS is lightweight with reasonable accuracy. However, it heavily relies on patterns. In contrast, Payload-based IDS examines message content to identify intrusions within the vehicle network. Although it offers superior weight and accuracy in countering DoS and fuzz attacks, its performance tends to decrease when dealing with replay-based attacks. Hybrid IDS combines elements of both flow-based and payload-based techniques, enhancing intrusion detection with high performance. However, these IDS types are heavier. They also consume more computational power.

According to this categorization, this research was focused on flow-based IDS. However, from another perspective, recent observations highlight a distinction in IDS techniques, categorizing them into two groups: rule-based and anomaly-based detection [9]. Rule-based IDSs rely on predefined rules for detecting known attacks with high accuracy but lack adaptability to emerging threats and evolving techniques, potentially leaving vulnerabilities to novel or zero-day attacks not covered by established rules [10], [11]. Under anomaly-based detection, in recent studies, IDS has been further categorized into sub-types including those based on fingerprints, parameter monitoring, information theory, and Artificial Intelligence (AI) [12]. Machine Learning (ML) or Deep learning (DL)-based IDSs are also capable of detecting unknown attacks on in-vehicle networks [13], [14], [15]. The effectiveness of AI-based IDS significantly relies on feature extraction and data preprocessing [16]. However, challenges persist in feature extraction and data input for deep learning models. Most studies directly feed raw data into these models [17], [18], potentially limiting their scopes. This approach, where data are sequentially inputted one by one, can overwhelm deep-learning IDSs in complex scenarios, especially given the extensive data generated in in-vehicle networks. Additionally, data can vary based on driving situations [19], [20], posing a significant challenge for practical IDS effectiveness. To address this complexity, data generalization is the best solution for ML and DL models

IDSs using ML and DL offer several benefits. They excel in recognizing complex and evolving threats, reducing the number of false alarms, and providing adaptability to changing attack tactics [21]. These models can also automate threat detection, scale up to analyze large network traffic volumes, and offer real-time protection. However, they have drawbacks. For example, they demand a substantial amount of high-quality labeled data for effective training [22], which may not always be available. Additionally, building and maintaining ML/DL models can be complex. There is a risk of overfitting, where models work well on training data but struggle [23]. They can be resource-intensive and less interpretable. Sometimes they generate false alarms if not properly tuned. Balancing their advantages and challenges is key to their effective use in network security.

The recognition that attackers in real-world scenarios often employ inventive strategies when injecting packets into the in-vehicle network inspired the present experiment. To enhance security in in-vehicle networks, an advanced IDS system was developed in this study. It combines high-resolution feature extraction and time-series input to create a deep-learning model. Its focus is on detailed feature extraction, utilizing Gabor filters to capture key data patterns. The main goal is to improve IDS effectiveness by reducing complexity and making it more effective, including its ability to detect Frequency-Agnostic types of attacks. This approach aids in detecting evolving attack patterns by analyzing how network traffic changes over time, providing a better view of network behavior crucial for in-vehicle networks. A lightweight Recurrent Neural Network (RNN) Gated Recurrent Unit (GRU) was employed with two features [24]. When incorporating a GRU into the model, the concern regarding computational power consumption becomes negligible [25], particularly given the utilization of only two features as input. Experiments with different attack data confirmed that the approach was robust and versatile.

In the following sections of the paper, a structured overview of the study is provided. Section II reviews prior research on in-vehicle networks, highlighting the limitations of existing IDS approaches. Section III describes data collection methods and scenarios investigated by conducting three types of attacks (Denial-of-Service, Fuzzing, and Replay attacks) on CAN data. Two distinct sets of laboratory data were used and attack frequencies were varied. Section VI describes the practical application of the Gabor transform for feature extraction, offering a comprehensive explanation of the algorithm, feature extraction process, and data preprocessing techniques. Section V presents the deep learning model's results, including hyperparameters and the architecture employed. The model's performance was evaluated under different scenarios, such as high data injection, low data injection, low data injection with synthetic data, and a model trained with high injection data and tested on low injection data. Section VI discusses the advantages and limitations of the approach, providing a comprehensive understanding of its contributions to in-vehicle network security and analysis.

II. RELATED WORK

In this paragraph, the recurring issue in prior research is investigated, which often involves overlooking critical factors. This issue was introduced in the earlier section concerning recent IDSs. Additionally, the discussion covers how the frequency domain, particularly the Gabor transform, has effectively enhanced performance in various fields and its fit within a deep learning model.

A. RELATED WORKS IN IN-VEHICLE NETWORK INTRUSION DETECTION

In this section, according to the categorization, factors will be delved into individually, starting with a hybrid analysis, followed by a payload analysis, and finally, a flow-based analysis.

In the field of hybrid IDS for in-vehicle CAN security, notable innovations have emerged. Zhang et al. [26] have introduced a two-stage hybrid IDS that combines rule-based and Deep Neural Network (DNN)-based components for real-time attack detection. This IDS could swiftly identify disruptions of CAN traffic patterns in its initial rule-based stage. A DNN-based system proficient in capturing attacks was then used. Similarly, Zhang et al. [17] have introduced two DL model-based IDS for CAN, utilizing two representations of CAN data:) raw data, and converted raw data in the form of images. These representations incorporate deep learning techniques, including LSTM and ConvLSTM, along with extensive CAN features. However, this type of IDS has a high computational cost and high response time. One study [27] has introduced a Binary Neural Network (BNN)-based IDS, which achieves three times faster detection speeds than another model, albeit with an accuracy trade-off depending on the attack type. During training, labeled input frames containing ten consecutive CAN messages are used to teach the IDS to recognize attack patterns. Once trained, the BNN model can rapidly analyze real-time CAN traffic and trigger alarms upon detecting malicious activity. In a hybrid IDS, the overall performance is approximately over 90%. The incorporation of various features can increase its computational complexity. If two models collaborate with different feature extraction methods, the system can become even more computationally intensive. While some studies have achieved high accuracy with this approach, it is worth noting that significant accuracy can also be attained using only Payload or CAN ID sequences. Additionally, it is possible to make the system lighter. However, doing so would lead to a trade-off in its performance.

In the area of payload-based IDS for CAN security, Markovitz and Wool [28] have developed a novel system to detect unusual communication patterns between ECUs in vehicles via the CAN bus network. They designed a classifier to categorize messages into different field types (Constant, Multi-value, or Counter/Sensor) without prior knowledge of their format. The system can create models for each ECU based on message characteristics. It uses Ternary Content-Addressable Memory (TCAM) to match incoming messages with expected patterns. Messages not matching these patterns are considered anomalies. This type of IDS highly depends on predefined rules. H-IDFS has been introduced based on the histogram structure for intrusion detection and filtering [29]. In the training phase, CAN data are divided into windows, with each window containing eight consecutive data bytes (Payload) from sequential packets. These windows are processed into histograms for multi-class IDS classification by K-Nearest Neighbors (KNN). Fine-grained features are then extracted for filtering. H-IDFS operates effectively with larger window sizes. A larger window size means a larger response time. A small window can compromise the performance. Hierarchical Temporal Memory (HTM) algorithms, as presented in [30], are used for processing packet-level data in CAN traffic. This approach involves training specialized anomaly detectors for each unique CAN ID's payload, using HTM networks as the foundational model. Afterward, postprocessing steps combine bit-level anomaly scores within defined time windows, which are then compared against predefined thresholds to trigger alerts when anomalies are detected. In a payload-based IDS, a significant challenge arises when dealing with replay attacks. Replay attacks have unique characteristics that can make them difficult to detect effectively. Additionally, the payload typically consists of eight bytes, with each byte frequently changing over time based on the specific situation of the vehicle. To enhance the performance of the IDS, it is essential to incorporate a wide range of vehicle scenarios, including normal driving, transitioning from driving to parking, and from parking to driving, among others.

One study [31] has primarily focused on enhancing in-vehicle network security through a Flow-based IDS. Specifically, it aimed to improve the detection of message injection attacks by adopting a statistical approach. This paper addresses limitations associated with traditional interval-based IDS, particularly the issue of false positives due to message timing variations during different driving modes. To overcome these limitations, the present research introduced a novel frequency-based IDS methodology, incorporating the Fast Fourier Transform (FFT) for frequency domain analysis. The effectiveness of this approach was demonstrated through improved detection capabilities, notably in identifying message injection anomalies. However, it is important to note that this study solely concentrates on spoofing attacks within a simulated attack environment, excluding the assessment of other attack types in real driving scenarios for a more comprehensive performance evaluation.

CANet [32] is an unsupervised LSTM-based anomaly detection method designed for CAN data in the context of flow-based IDS for vehicle communication networks. It employs separate LSTM models for different data sources (IDs) within the vehicle network to capture temporal data dynamics. Outputs of these LSTM models are integrated into a fully connected subnetwork designed like an autoencoder, enabling CANet to consider data interdependencies. During training, CANet learns to reconstruct input data and measures the disparity between real data and its reconstruction. Anomalies are identified based on this disparity exceeding a predefined threshold, prompting the model to flag potential intrusions. The false positive rate is generally higher in unsupervised learning than in supervised learning. A semi-supervised approach implemented in a previous study [33] can enhance vehicle CAN bus security by analyzing CAN ID sequences for anomalies and recognizing disruptions in their patterns indicative of potential attacks. It employs 29-bit CAN ID representations organized into frames for input into the Convolutional Adversarial Autoencoder (CAAE) model. The CAAE operates in a semi-supervised way. It has discriminators to ensure specific distributions. During post-training, only the encoder's weights are used. Although unsupervised IDS systems can achieve an overall performance of approximately over 90%, a major challenge arises from the lack of a well-defined ground truth due to the dynamic and evolving nature of network threats, which hinders objective evaluation of model performance. Additionally, unsupervised approaches encounter difficulties in outlier detection primarily because there is no clear delineation between normal and abnormal network behaviors during training. Few studies have been conducted using a supervised deep-learning approach.

Desta et al. [19] have introduced a method for detecting in-vehicle network attacks. They used convolutional neural networks and generated images using recurrent graphs. Their model assigns binary labels to classify these attacks. When compared to the Inception-ResNet model, their approach demonstrated greater efficiency. For creating images, they used the CAN ID sequence along with timestamp as features. Extracting features from raw data and converting them into images while using long neural networks resulted in high computational costs and response time. GIDCS [34] is a sophisticated system designed for safeguarding CAN traffic. It comprises two main components: a Classifier Configuration Module and a Classification Module. While training, the Configuration Module organizes CAN bus messages into groups based on their CAN IDs and creates graphs. These features set the threshold for the binary classifier. The threshold relies on feature values from normal messages. However, a common issue encountered with most models is their inability to generalize and adjust to diverse situations. In one study [35], researchers utilized Federated Learning (FL) to develop an IDS capable of addressing challenges posed by various automobile manufacturers (Data Diversity). Multiple car models, each with its own dataset of CAN data, were used to find common patterns while maintaining data privacy. The Federated Averaging (FedAvg) algorithm was employed for collaborative model training without sharing data. In the supervised technique, all IDS systems performed well with an accuracy of 95%. For supervised learning, a simple neural network architecture also plays a significant role with CAN ID sequence input. Big models such as Inception and ResNet are known to increase computational costs. While FL models have significance in generalizing IDS, they introduce dependencies on third parties and make the IDS more complex.

B. RELATED WORKS IN FREQUENCY DOMAIN ANALYSIS

Gabor transform or spectrogram is a vital tool in signal analysis [36], [37], [38]. It excels at identifying signal components, making it valuable for sound differentiation, like in Shazam's music classification [39]. In medicine, spectrograms are used in electromyography [40] and image analysis [41]. Additionally, spectrograms are applied in anomaly detection, such as for identifying machine anomalies via vibration spectrograms [42] and for network attack detection [43].

In this study, two primary types of data were examined: time domain and frequency domain data. Time domain analysis involves mathematical functions or signals analysis with respect to time, while frequency domain analysis involves mathematical functions or signals analysis with respect to frequency. Specific time values represent time domain data, while frequency domain data are presented by specific frequency values [44]. The internal data of a car are typically in the form of time series data. In this research, there was a necessity to transform time-domain data into the frequency domain to achieve generalization. This transformation is essential for enabling the IDS to possess frequency-agnostic capabilities both in the context of in-vehicle network data generation, which occurs situationally and from the attacker's perspective, allowing them to inject messages with frequency-agnostic characteristics.

In signal processing, the Fourier transform is widely used for frequency domain analysis. However, it has a trade-off between frequency and time resolution [45]. This trade-off can be limiting for non-stationary signals such as those in CAN data. To address this, the wavelet transform offers efficient solutions, providing high-frequency resolution at low frequencies and high-time resolution at high frequencies [46]. However, challenges arise regarding coefficient length variation based on wavelet labels and processing multi-dimensional data simultaneously, especially in deep learning approaches.

Gabor transform is another transform in the wavelet family. It is also known as a spectrogram, which employs a Gaussian function [47]. The primary difference between the Gabor transform and wavelet transform is that the Gabor transform has fixed bandwidths with fixed-length coefficients, while the wavelet transform has bandwidths that continuously change from arbitrarily small to large [48]. The mathematical definition of the Gabor transform is shown as follows:

$$g(x, y) = e^{-\frac{x'^2}{2\sigma_x^2} - \frac{y'^2}{2\sigma_y^2}} \cos\left(2\pi \frac{x'}{\lambda} + \psi\right) \tag{1}$$

where $x' = x\cos\theta + y\sin\theta$ and $y' = -x\sin\theta + y\cos\theta$.

The equation represents a 2D Gabor function. It combines a Gaussian envelope that controls size and orientation with a cosine modulation introducing oscillations along an orientation defined by the angle θ. Coordinate transformations x' and y' perform a rotation of coordinates x and y by an angle θ, allowing the Gabor function to be oriented in different directions. Adjusting parameters such as σ_x, σ_y, λ, and ψ can customize the function's size, orientation, spatial frequency, and phase.

In recent times, several IDS have been proposed. However, frequency-agnostic ability, a crucial aspect, has often been overlooked by researchers. This ability is about making the IDS less dependent on a specific data injection frequency, which means that it can function effectively regardless of how often an attacker tries to manipulate their data injection pattern. Comprehensive Frequency-Agnostic Intrusion Detection System (CF-AIDS) is a concept in technology and systems design that essentially means being versatile and flexible across different frequencies or rates of occurrence. In an in-vehicle network security system, CF-AIDS can effectively detect and respond to various events ranging from routine data transmissions during regular driving to rare and potentially malicious activities that could signal a cyberattack. This system does not specialize in just one type of event. Instead, it is capable of handling a wide range of scenarios without being biased toward any particular frequency. This frequency-agnostic capability is vital for IDS performance because it ensures that security measures can remain robust and effective even when attackers attempt to change their tactics. By being able to detect intrusions without relying on a fixed frequency, IDS becomes more resilient with better protection against evolving attack strategies. This flexibility is crucial for maintaining the security of systems in dynamic and unpredictable environments.

Most studies have endeavored to address challenges such as a high false positive rate, extended response time, which demands substantial computational resources, and a limitation known as the 'rule coverage gap.' Remarkably, one vital aspect that has been consistently neglected in previous investigations is the Frequency-Agnostic ability. Thus, the present study aimed to address both conventional challenges and this noteworthy, yet often neglected, problem.

III. UNVEILING ATTACK SCENARIOS: ANALYZING DATA FOR INSIGHTS

In this study, two methods were applied to analyze attacks targeting embedded car systems. The first method uses a focused attack on specific functions, which requires detailed knowledge about the car manufacturer's secure network protocols from CAN (Data Base Container) DBC [13]. This method is challenging due to its need for specialized knowledge. The second method involves random and extensive injection of data, which can easily disrupt car operations without specific knowledge.

In the initial part of the discussion, the definition of attacks is presented. This study introduced three attack methods: DoS, Fuzzing, and Replay attacks. DoS attacks, which stand for "Denial of Service" attacks, have the goal of disrupting normal operations of the CAN by inundating it with an excessive number of messages or incorrect parameters, often by high-priority ID messages. These attacks can lead to failures in the vehicle's systems, necessitating the use of protective tools to identify and counteract them [49]. Fuzzing attacks aim to uncover system vulnerabilities by sending varied and incorrect data, including both high-priority and low-priority ID messages, to the controller network [50]. Replay attacks involve capturing and re-sending legitimate messages within controller networks [51]. Systems may mistakenly view these repeated messages as authentic, leading to unintended parameter changes or actions.

In the context of these methods, data are introduced into the car's network using a frequency-agnostic data injection technique. However, it is important to note that this external device places restrictions on how long data can be injected. For instance, when using the PEAK-CAN system, there is a specific time limit of 3 to 5 seconds for injecting data. In this study, three distinct categories of attack patterns have been incorporated, all of which employ the frequency-agnostic data injection technique. To carry out this study, an IDS was implemented using the Hacking and Countermeasure Research Lab (HCRL) dataset [52]. A proprietary data generation technique has also been developed.

According to HCRL, data were introduced into the network at a controlled pace, with short pauses of 0.0003 to 0.0005 seconds between each injection. This approach allowed for extended attacks involving DoS, fuzzing, and replay techniques using data from Kia Soul and Hyundai Sonata vehicles. The benefit of this method is that it closely mimics the regular data transmission rhythm, potentially bypassing default restrictions set by devices. However, it is important to note that without access to a specific CAN DBC file, these injected packets might not significantly impact the vehicle's normal operations all the time. Therefore, experimental results generally showed a minimal response from the vehicle to these intrusions. In a DoS scenario, a high-priority CAN ID labeled '0 × 00' was used, while fuzzing involves IDs ranging from 0 × 000 to 0 × 7FF.

According to the data generation technique, data were collected from an internal gateway where a central gateway handled all the traffic, as shown in [35]. Introducing data could rapidly disrupt the behavior of the target vehicle. Specifically, the DoS attack utilizes specific ID priorities by injecting a substantial number of '0 × 00' values, causing other IDs to temporarily halt. This primarily impacts functions associated with the top-priority ID, including malfunction warnings. The Fuzzing attack introduces random IDs and data values across the vehicle's priority range, potentially activating preset functions within ECUs. However, this influx of data also leads to processing delays as ECUs manage a high volume of incoming IDs. Additionally, the Replay attack injects normal driving data during vehicle operation to collect attack data. This attack lasted approximately 7 minutes. It was applied multiple times. The DoS method involved three iterations with injections of 5,000 and 10,000 values, each lasting 3 seconds. Fuzzing was conducted 100 and 500 times, while the Replay attack reintroduced 7 minutes of past normal driving data and replayed multiple times in 3-second intervals. It is crucial to note that prolonged data injection can result in timing discrepancies within ECUs, potentially leading to data errors in real-time vehicle feedback.

In this study, the evaluation of IDS responses in critical scenarios, such as various attack frequencies, relied on synthetic data generated through an in-depth analysis of internal vehicle system data. For instance, in Kia vehicles, it was discovered that the most minimal CAN ID that was assigned the highest priority was "0 × 18." Subsequently, a DoS attack was conducted, targeting not only the "0 × 00" CAN ID but also a range of CAN IDs from "0 × 00" to "0 × 17". This attack adhered to the HCRL standard injection pattern, with data inserted at precise time intervals of 0.0003 to 0.0005 seconds. In the fuzzing attack, a CAN ID spectrum ranging from '0 × 00' to '0 × 1F4' encompassing both the highest and lowest priority IDs was selected. The timing structure of the replay attack followed a similar pattern to other attacks, allowing for a comprehensive assessment of IDS performance. Moreover, injecting attack data while the vehicle is in motion poses a significant risk of malfunctions and accidents. Therefore, multiple injections of attack data were performed, taking into consideration critical factors of safety and stability.

IV. OPTIMIZING DEEP LEARNING: FEATURE EXTRACTION AND DATA PREPROCESSING TECHNIQUES

A. HIGH-RESOLUTION FEATURE EXTRACTION IN DEPTH

In the context of in-vehicle IDS from CAN data, the initial step involves feature selection based on CAN ID and a time gap with a sequence length of 100. These selected features are then fed into the Gabor filter for high-resolution feature extraction, a crucial step that can significantly enhance the ability to detect and mitigate potential security threats within the in-vehicle network. After applying FFT, the combination of a Gabor filter offers several signal processing benefits. It helps identify dominant frequencies across different time intervals, thus reducing the dimensionality of complex data for a more concise representation. Additionally, it enhances pattern recognition in applications such as image processing and feature extraction

$$F(u,v)=\sum_{x=0}^{N-1}\sum_{y=0}^{M-1} f(x,y)e^{-j2\pi(\frac{ux}{N}+\frac{vy}{M})} \tag{2}$$

In the equation, $F(u, v)$ is the 2D Discrete Fourier Transform (DFT) of the input matrix $f(x, y)$ with dimensions N and M, and variables u and v are frequencies ranging from 0 to $N-1$ and from 0 to$M-1$, respectively. The double summation accounts for all possible combinations of x and y. The complex exponential function, $exp(-j2(ux/N+vy/M))$, encodes frequency and phase information, allowing us to shift frequency components to the spectrum center. This simplifies visualization and analysis of the spectrum.

In **Algorithm 1**, `convolve2d` is a function used for performing a two-dimensional convolution operation. Convolution is a mathematical operation that combines two functions to produce a third function. In the spectrogram frequency domain, convolution is commonly used for various tasks, such as edge detection and filtering [53]. The `convolve2d` function takes three arguments: the input data, the Gabor filter `gb`, and the `mode` parameter. The input data are the data on which the convolution operation will be applied. The Gabor filter is a kernel or filter used for the convolution operation. The `mode` parameter determines how the boundaries of input data are handled during convolution. The `fftpack.fft2` stands for FFT operation.

Algorithm 1 Extract Feature by FFT From Gabor

```
1. Gabor Transform Function:
data, $\theta = 0$, $\sigma = 1$, Frequency = 1
2. Construct the Gabor filter
$gb \leftarrow$ Gabor($\sigma$, $\theta$, $\frac{1}{\text{Frequency}}$, 0, 1)
3. Apply the filter to the data
$filtered \leftarrow$ convolve2d(data, $gb$, mode = 'same')
4. Compute the Fourier transform of the filtered data
$fft \leftarrow$ fftpack.fft2($filtered$)
5. Initialize parameters
data $\leftarrow$ load_data()
$\theta \leftarrow$ set theta
$\sigma \leftarrow$ set sigma  frequency $\leftarrow$ set frequency
6. Apply Gabor filter to the data
$result \leftarrow$ (data, $\theta$, $\sigma$, frequency)
```

B. DATA PREPOSSESSING

The deep learning GRU model processes input data in a time series format. Initially, 100 data sequences containing CAN ID and time gap were selected. BMW, Kia, and Tesla Lab. of Information System Security Assurance (LISA) generated around 870, 2090, and 3030 data sequences, respectively, representing one-second intervals for each vehicle. A label encoder converted CAN ID categories into decimal numbers. Both CAN ID and time gap data underwent min-max scaling. Finally, data were filtered through a Gabor filter in the frequency domain. This preprocessing ensured standardized input for the GRU model, enabling accurate analysis and prediction. To comprehend the graph, this paragraph provides an explanation. In the analysis, evaluation involved examining various input features such as CAN ID, time gap, and two specific injection patterns. Two different data collection methods were employed. To aid in distinguishing between scenarios with no attacks and potential attack situations, graphs were generated. These graphs offer a visual representation for differentiation between the attack-free scenario and instances where attacks are present. The x-axis represents the sample index and the y-axis represents the amplitude. Blue and green lines correspond to attack-free scenarios while red and yellow lines represent scenarios with attacks. These lines pertain to the CAN ID sequence and time gap.

Fig. 1 shows high-frequency data injection. In Fig. 1 (a), the DoS attack showed a clear pattern with recurring red and yellow data frame injections at regular intervals. However, during non-attack periods, the network experienced irregularities in both CAN ID sequences and time intervals between data frame transmissions. Understanding and monitoring these patterns is crucial for effective attack detection and mitigation. In Fig. 1 (b), the Fuzzing attack exhibited noticeable peaks in both features, with higher peaks in the CAN ID sequence during attacks. In Fig. 1 (c), the Replay attack showed lower amplitude peaks than the attack-free scenario. In each case, distinct features served as clear indicators.

Fig. 2 depicts lower-rate injection data for HCRL. In Fig. 2 (a), the CAN ID sequence showed lower amplitude than that in non-attack scenarios, although there were non-periodic amplitude peaks in the time gap. For fuzzing and replay attacks (Fig. 2 b, c), higher amplitude characteristics were observed, although the density was lower than that in DoS attacks. Notably, the CAN ID sequence exhibited higher peaks than in attack-free scenarios. These patterns provided valuable insights for effective attack identification.

In Fig. 3, a synthetic attack scenario is simulated, showing similar characteristics for all attack types. Distinguishing between these attacks was challenging. However, slight differences were noticeable in the CAN ID sequence, while the time gap displayed more pronounced distinctions with lower frequency amplitudes compared to the attack-free scenario.

In summary, Gabor features are valuable for classifying attack-free scenarios and attacks in deep learning. Challenges emerged when classifying attack types with lower-rate injection. The results section will offer a brief overview of deep learning performance using Gabor features.

V. MASTERING DEEP LEARNING ARCHITECTURES: STRATEGIES FOR EFFECTIVE RESULT EVALUATION

A. DEEP LEARNING ARCHITECTURE AND HYPERPARAMETER CONFIGURATION

GRU is a type of RNN architecture that handles sequential data by retaining and selectively updating information over time. It addresses the problem of vanishing gradients in traditional RNNs by incorporating gating mechanisms. GRU uses two gates, an update gate, and a reset gate, to control the flow of information. The update gate determines how much past information should be retained, while the reset gate decides how much of the new input should be considered [54]. This allows GRU to capture long-term dependencies and effectively process sequential data. Fig. 4 presents an overview of the layout for the intrusion detection system. Preprocessed features were inputted into the Gabor filter, which produced high-resolution features. The FFT filter was then applied to extract the main features from the Gabor filter, facilitating the classification of attacks using a deep-learning GRU model. Table 1 explains hyperparameter specification. The GRU model operates on a sequence time series input with a length of 100 and generates the classification result. This approach enhances the effectiveness of attack detection and classification within the intrusion detection system.

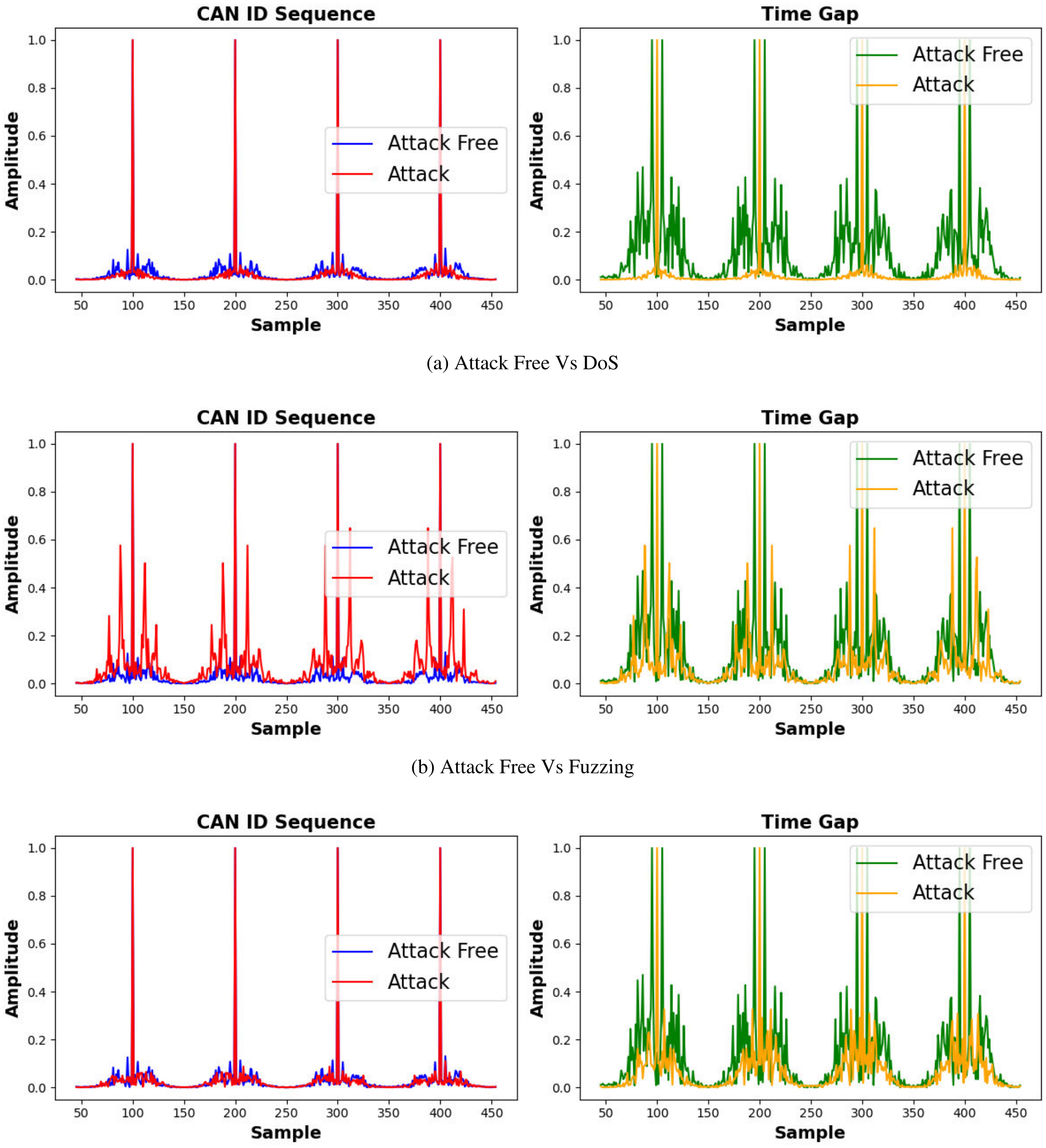
TABLE 1. Deep learning hyperparameters.

Hyperparameter	Value
Model Type	GRU
Input Size	2
Sequence Length	100
Number of GRU Layers	5
Hidden Size (GRU)	128
Fully Connected Layers	1
Output Layer	Linear
Loss Function	Cross-Entropy
Optimizer	Adam
Number of Classes	4 & 2
Number of Epochs	100
Batch Size	64
Learning Rate	0.001

B. RESULT EVALUATION: HIGH-FREQUENCY PACKET INJECTION

In this section, a confusion matrix is provided to illustrate research results. Numbers within the matrix represent quantities of sequences in that category, and percentages indicate the proportion of sequences within each category.

In the case of high-frequency data injection, vehicles exhibit immediate responses, which can introduce a significant risk for safe driving. However, the accuracy matrix of the IDS demonstrated the model's effectiveness for both mechanical and electronic vehicles. The attack detection performance for each vehicle exceeded 100%, with BMW



(a) Attack Free Vs DoS

(b) Attack Free Vs Fuzzing

(c) Attack Free Vs Replay

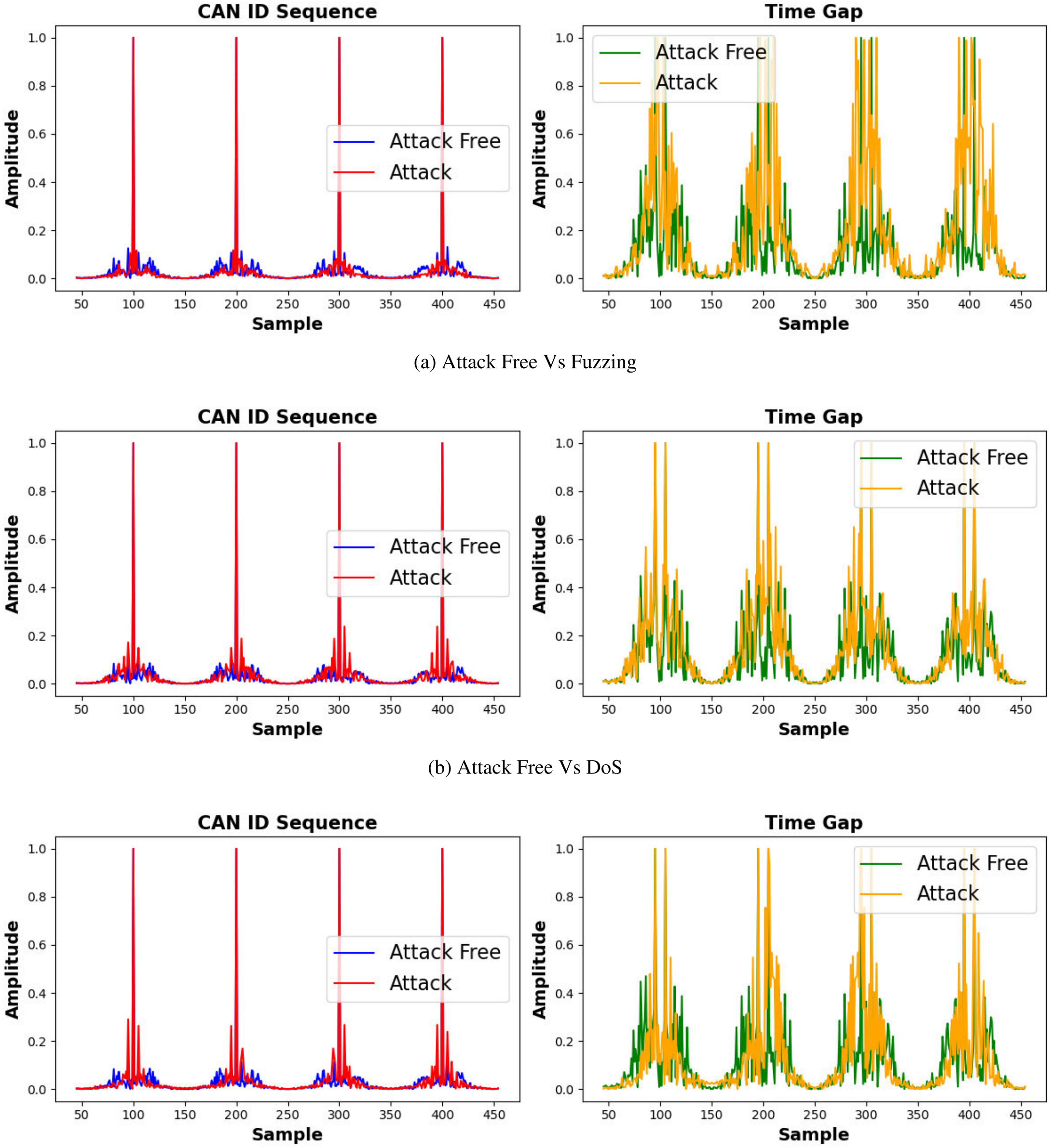
FIGURE 1. Gabor coefficient amplitude distribution in high volume data injection.

and Kia achieving impressive detection rates of over 99% and Tesla reaching 99%. In Fig. 5 and Table 2, a detailed classification report is provided for BMW, Kia, and Tesla where false positive and false negative less than 1% approximately. This report revealed that the error rate was less than 1% for each of these vehicles. This outcome served as compelling evidence of the exceptional effectiveness of Gabor's high-resolution feature extraction when dealing with high packet injection into in-vehicle networks.

In this context, results are initially presented using a multi-class classification approach. However, a subsequent switch to binary-class classification was made. This adjustment aligned with the primary objective, which was to detect attacks within multi-dimensional data injection frequencies, a scenario referred to as 'frequency-agnostic injection.' The focus was on detecting attacks rather than categorizing them into specific attack types.

C. RESULT EVALUATION: LOW-FREQUENCY PACKET INJECTION (HCRL)

In the context of low-frequency data injection, the accuracy of the IDS was notably affected, especially in the context of multi-class classification. Nevertheless, the system's response to low-frequency injection data was not as pronounced. To assess the system's performance, we conducted experiments using data from the HCRL, specifically



(a) Attack Free Vs Fuzzing

(b) Attack Free Vs DoS

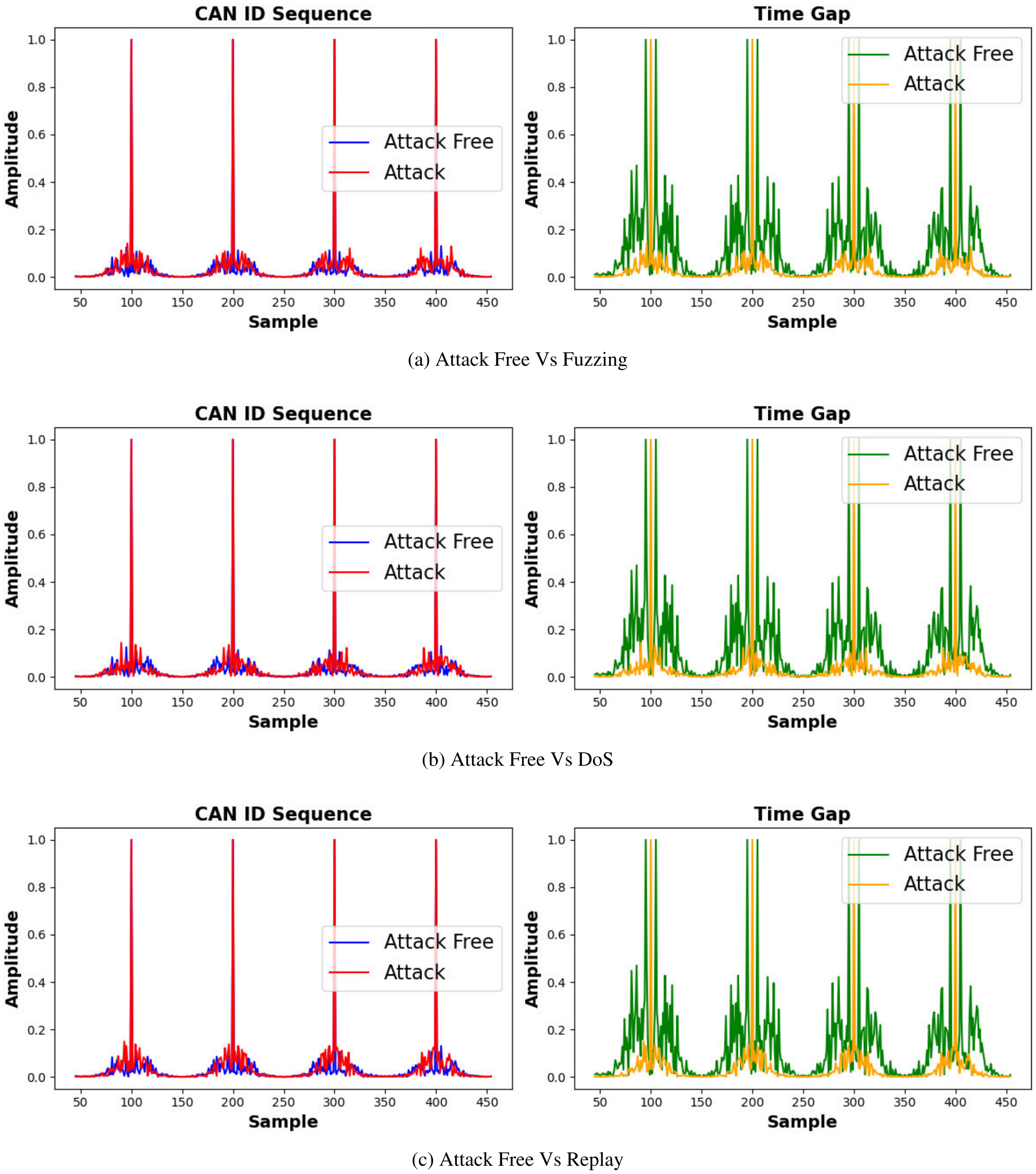
(c) Attack Free Vs Replay

FIGURE 2. Gabor coefficient amplitude distribution in low volume data injection.

TABLE 2. Performance metrics for Kia and Tesla for multi-class classification.

Index	BMW			Kia			Tesla		
	Precision	Recall	F1-score	Precision	Recall	F1-score	Precision	Recall	F1-score
Normal	1.00	1.00	1.00	0.99	0.99	0.99	0.99	1.00	1.00
Fuzzing	0.99	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
DoS	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Replay	1.00	1.00	1.00	0.99	0.99	0.99	1.00	0.99	0.99
Overall Accuracy Metrics									
Accuracy	1.0			0.99			0.99		
Error Rate	0.0015			0.0079			0.0028		
ROC AUC score	0.9989			0.9946			0.9974		

employing data from mechanical vehicles Kia Soul and Hyundai Sonata for both classifications. However, a notable observation from this matrix was that while it struggled to classify the specific types of attacks, it effectively



(a) Attack Free Vs Fuzzing

(b) Attack Free Vs DoS

(c) Attack Free Vs Replay

FIGURE 3. **Gabor coefficient amplitude distribution in low volume data injection.**

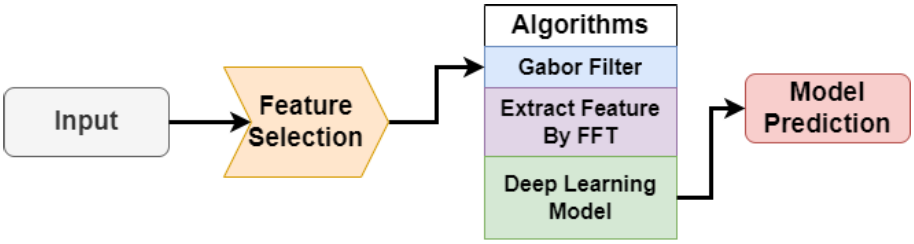
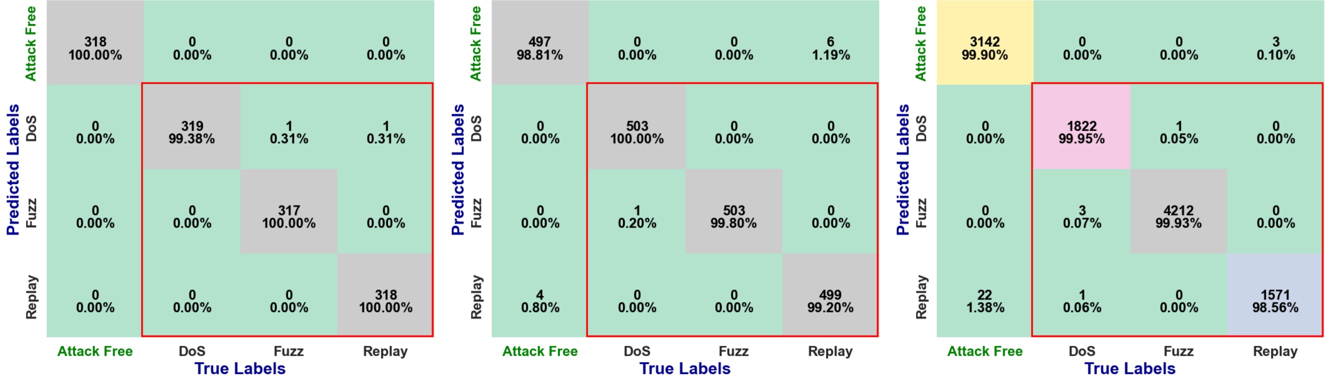


FIGURE 4. **Attack detection model layout.**

distinguished between attack-free scenarios and attacks. To address this, binary class classification was applied, resulting in success rates of approximately 97% and 92% and false positive and false negative rates of approximately 6% and 10%, respectively, for the two vehicles. It was worth noting that there was a decline in detection accuracy, ranging from 3% to 8% when compared to results from high-frequency injection data. The decrease in accuracy



(a) BMW (b) Kia (c) Tesla

FIGURE 5. Confusion matrix on high-frequency anomaly detection.

was expected primarily due to the lower rate of packet injection, which occurred periodically. The system behaved as if this were a normal situation. The relatively lower volume of available training data further contributed to the reduction in accuracy. This information is presented in Table 3 and Fig 6. The incorporation of the Gabor transform for high-resolution feature extraction in the IDS demonstrated promising outcomes. Despite a marginal influence on accuracy when dealing with low-frequency data injections, the system effectively responded to these instances

D. RESULT EVALUATION: LOW-FREQUENCY PACKET INJECTION (LISA)

In the realm of attack classification, we conducted experiments using synthetic data. The rationale behind this choice was the versatility and scalability of simulation, enabling a wide range of experiments, particularly concerning packet injection. Simulation proved valuable in validating the model's performance in scenarios involving extraordinary packet injection patterns and data injection patterns, as mentioned earlier. While time intervals for packet injection were similar to those in the HCRL data, the manner of packet injection exhibited more variation. Results shown in Fig. 7 and Table 4 indicated that the overall accuracy was nearly 100% with false positive and false negative rates of under 1% for Kia (Mechanical) and Tesla (Electronic) in the context of binary-class classification. This demonstrated that the volume of collected data was sufficient for training the model effectively. In this case, Gabor's high-resolution feature extraction performed well for binary-class classification.

E. RESULT EVALUATION: TRAINING THE MODEL WITH HIGH-FREQUENCY DATA INJECTION AND TESTING THE MODEL WITH UNKNOWN LOW-FREQUENCY DATA INJECTION

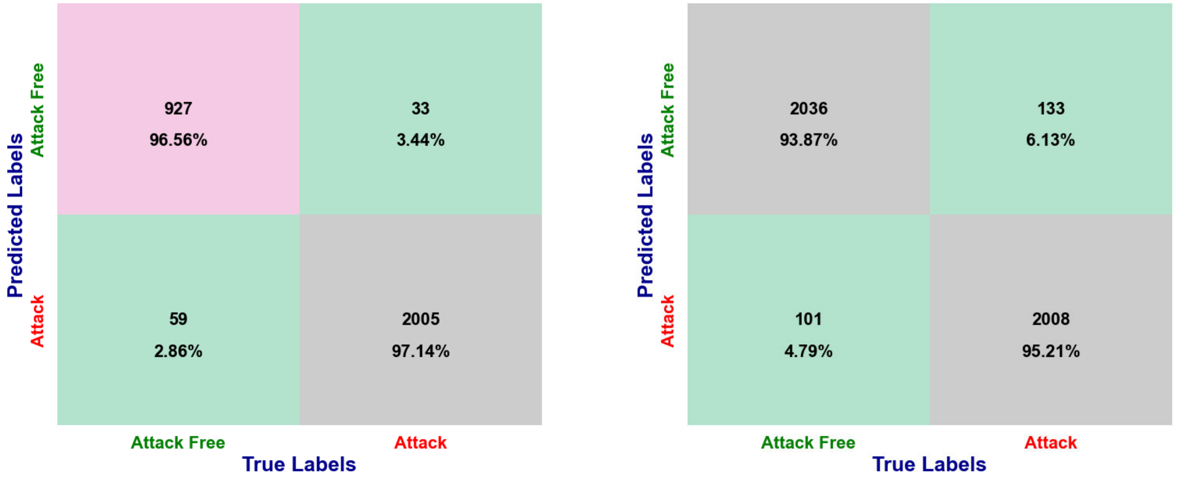
In this experiment, a novel approach was applied by training the model with higher-rate packet injection and subsequently evaluating the model using low-rate packet injection data. The motivation behind this experiment was rooted in the recognition that real-world attackers often employed inventive strategies when injecting packets into the in-vehicle network. They might improvise IDs for various types of attacks using a comprehensive, frequency-agnostic approach. Furthermore, the generation of packets within the network can vary depending on the specific situation. The aim was to assess how the model responded to completely unknown scenarios, a capability not achievable with rule-based IDS systems. We previously explored unsupervised learning for detecting unknown attacks. Here, we applied a supervised learning approach.

Results are illustrated in Fig. 8 and summarized in Table 5, highlighting the effective performance of the Gabor filter. However, in some cases, attack-free data were incorrectly classified as replay attacks. In contrast, in binary-class classification, the model achieved a remarkable overall accuracy of 100% for Kia (Mechanical) and 88% for Tesla (Electronic) and false positive rates under 1% for Kia and 24% for Tesla, but false negative is 0%. This outcome significantly enhanced in-vehicle network security and reinforced the robustness of this IDS.

VI. DISCUSSION

In the field of in-vehicle network security, this research provides valuable insights by utilizing Gabor high-resolution feature extraction and GRU-based classification for intrusion detection. The study covers a wide range of scenarios, including both high and low-frequency data injection, and encompasses real-world and synthetic environments. This approach aims to develop an IDS capable of effectively detecting intrusions generated by attackers in the in-vehicle network, while considering data variations and frequency-agnostic capabilities, across various driving scenarios.

The research underscores the IDS's ability to handle high-frequency data injection, achieving detection rates exceeding 99% for BMW, Kia, and Tesla. Particularly noteworthy is the exceptional performance of the Gabor



(a) Kia

(b) Sonata

FIGURE 6. Confusion matrix on binary class classification low-frequency anomaly detection (HCRL).

TABLE 3. Performance metrics for Kia and Tesla for binary-class classification with low injection rate.

Index	HCRL					
	Kia			Sonata		
	Precision	Recall	F1-Score	Precision	Recall	F1-Score
Attack Free	0.97	0.94	0.95	0.94	0.95	0.95
Attack	0.97	0.98	0.98	0.95	0.94	0.94
Overall Accuracy Matrix						
Accuracy	0.97			0.95		
Error Rate	0.03042			0.0472		
AUC Score	0.97			0.95		

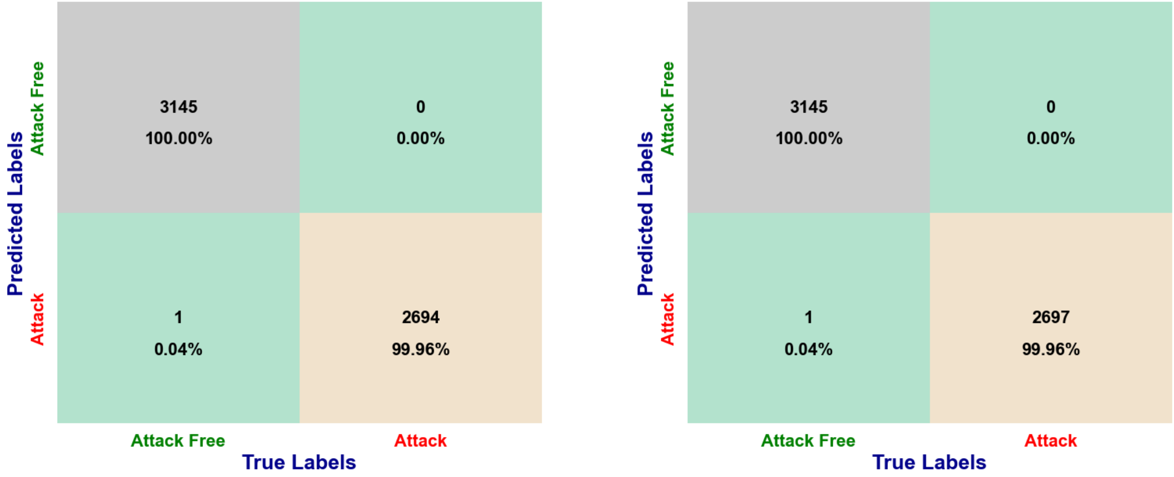
TABLE 4. Performance metrics for Kia and Tesla for binary-class classification with low injection rate.

Index	LISA					
	Kia			Tesla		
	Precision	Recall	F1-Score	Precision	Recall	F1-Score
Attack Free	1	1	1	1	1	1
Attack	1	1	1	1	1	1
Overall Accuracy Matrix						
Accuracy	1			1		
Error Rate	0.00017			0.00017		
AUC Score	1			1		

high-resolution feature extraction method, with error rates of less than 1% for each vehicle. However, in cases of low-frequency data injection, especially within the context of multi-class classification, the intrusion detection system experiences a reduction in accuracy for specific classifications. While it may face challenges in classifying specific attack types, it excels at distinguishing between attack-free scenarios and attacks. Binary-class classification is an effective solution for detecting attacks on vehicles. This method has shown success rates ranging from approximately 100% to 92% for four selected vehicle types. However, the accuracy decreases when there is a higher frequency of data injections, especially for electric vehicles. The study faced a notable limitation due to the availability of diverse vehicle datasets. In the future, incorporating hybrid and electric vehicles will help improve attack detection accuracy

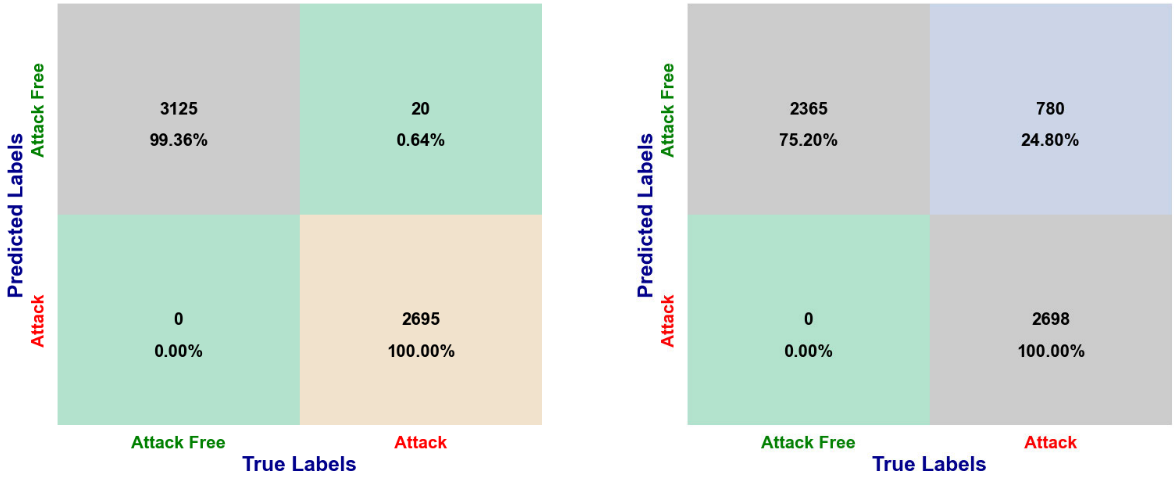
TABLE 5. Performance metrics for Kia and Tesla in the context of binary-class classification with low injection rate, high injection train, and low injection test.

Index	LISA (High Injection Train and Low Injection Test)					
	Kia			Tesla		
	Precision	Recall	F1-Score	Precision	Recall	F1-Score
Attack Free	0.99	1	1	0.75	1	0.86
Attack	1	0.99	1	1	0.78	0.87
Overall Accuracy Matrix						
Accuracy	1			0.87		
Error Rate	0.00342			0.13349		
AUC Score	1			0.88		



(a) Kia (b) Tesla

FIGURE 7. Confusion matrix on binary class classification low-frequency anomaly detection (LISA).



(a) Kia (b) Tesla

FIGURE 8. Confusion matrix on binary class classification low-frequency anomaly detection with low injection rate, low injection train, and high injection test.

and data generalizability. Despite resource constraints, the Gabor filter has been used to generalize data effectively while maintaining acceptable overall accuracy levels. It is worth noting that the biggest challenge in this type of research is the need for a substantial volume of data from various vehicles. The study used the most commonly available publicly accessible datasets. In comparison to other studies, the IDS's performance aligns with established standards. Furthermore, the research explores the model's capabilities through a novel experiment. It involves training the model with high-rate packet injection data and subsequently testing it with low-rate packet injection scenarios. This experimentation is crucial because real-life attackers may inject packets in creative and unpredictable ways, and in-vehicle networks generate data situationally, making it challenging to cover all possible scenarios during training. The results demonstrate that the Gabor filter effectively enhances the model's performance from this perspective. Notably, in binary-class classification, Kia and Tesla achieve remarkable accuracies of 100% and 88%, respectively.

In summary, this research highlights the effectiveness of Gabor high-resolution feature extraction and GRU-based classification models in enhancing in-vehicle network security. The system's capability to accommodate diverse injection patterns and its promising performance in high-frequency data scenarios emphasize its practical significance. These findings have a substantial impact on the advancement of intrusion detection systems for in-vehicle networks, ultimately enhancing their security and robustness.

VII. CONCLUSION

This in-vehicle network security research utilizes Gabor high-resolution feature extraction and GRU-based classification for intrusion detection across high- and low-frequency data injection scenarios in real-world and synthetic environments. The IDS detects high-frequency intrusions effectively, with exceptional performance in Gabor high-resolution feature extraction. However, accuracy improvement is needed for specific low-frequency data injection and multi-class classification scenarios. Binary-class classification mitigates this, yielding success rates ranging from moderate to high. Despite accuracy variations, the IDS's versatility aligns with established standards. The research demonstrates the model's flexibility by training with high-rate packet injection data and testing with low-rate scenarios, highlighting the effectiveness of the Gabor filter. Notably, Kia and Tesla achieve remarkable accuracies in binary-class classification.

REFERENCES

[1] M. Bozdal, M. Samie, and I. Jennions, "A survey on CAN bus protocol: Attacks, challenges, and potential solutions," in *Proc. Int. Conf. Comput., Electron. Commun. Eng. (iCCECE)*, Aug. 2018, pp. 201–205.

[2] S. Nie, L. Liu, and Y. Du, "Free-fall: Hacking Tesla from wireless to can bus," *Briefing, Black Hat USA*, vol. 25, no. 1, p. 16, 2017.

[3] L. Zhao, H. Chai, Y. Han, K. Yu, and S. Mumtaz, "A collaborative V2X data correction method for road safety," *IEEE Trans. Rel.*, vol. 71, no. 2, pp. 951–962, Jun. 2022.

[4] A. Ghosal and M. Conti, "Security issues and challenges in V2X: A survey," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107093.

[5] E. Aliwa, O. Rana, C. Perera, and P. Burnap, "Cyberattacks and countermeasures for in-vehicle networks," *ACM Comput. Surv.*, vol. 54, no. 1, pp. 1–37, Jan. 2022.

[6] Y. Lee, Y.-E. Kim, J.-G. Chung, and S. Woo, "Real time perfect bit modification attack on in-vehicle CAN," *IEEE Trans. Veh. Technol.*, vol. 72, no. 12, pp. 15154–15171, Dec. 2023.

[7] H. M. Song and H. K. Kim, "Discovering CAN specification using on-board diagnostics," *IEEE Des. Test. Comput.*, vol. 38, no. 3, pp. 93–103, Jun. 2021.

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

[9] M. Müter and N. Asaj, "Entropy-based anomaly detection for in-vehicle networks," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2011, pp. 1110–1115. [Online]. Available: https://api.semanticscholar.org/CorpusID:9017380

[10] S. Applebaum, T. Gaber, and A. Ahmed, "Signature-based and machine-learning-based web application firewalls: A short survey," *Proc. Comput. Sci.*, vol. 189, pp. 359–367, Jan. 2021.

[11] M. Müter, A. Groll, and F. C. Freiling, "A structured approach to anomaly detection for in-vehicle networks," in *Proc. 6th Int. Conf. Inf. Assurance Secur.*, Aug. 2010, pp. 92–98.

[12] W. Wu, R. Li, G. Xie, J. An, Y. Bai, J. Zhou, and K. Li, "A survey of intrusion detection for in-vehicle networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 3, pp. 919–933, Mar. 2020.

[13] M. Marchetti and D. Stabili, "Anomaly detection of CAN bus messages through analysis of ID sequences," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2017, pp. 1577–1583, doi: 10.1109/IVS.2017.7995934.

[14] Y. Wang, D. W. Ming Chia, and Y. Ha, "Vulnerability of deep learning model based anomaly detection in vehicle network," in *Proc. IEEE 63rd Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Aug. 2020, pp. 293–296.

[15] H. K. Kalutarage, M. O. Al-Kadri, M. Cheah, and G. Madzudzo, "Context-aware anomaly detector for monitoring cyber attacks on automotive CAN bus," in *Proc. ACM Comput. Sci. Cars Symp.*, Oct. 2019, pp. 1–8.

[16] Y. A. Farrukh, S. Wali, I. Khan, and N. D. Bastian, "SeNet-I: An approach for detecting network intrusions through serialized network traffic images," *Eng. Appl. Artif. Intell.*, vol. 126, Nov. 2023, Art. no. 107169.

[17] O. Y. Al-Jarrah, K. E. Haloui, M. Dianati, and C. Maple, "A novel detection approach of unknown cyber-attacks for intra-vehicle networks using recurrence plots and neural networks," *IEEE Open J. Veh. Technol.*, vol. 4, pp. 271–280, 2023.

[18] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall, and Y. Kadobayashi, "LSTM-based intrusion detection system for in-vehicle can bus communications," *IEEE Access*, vol. 8, pp. 185489–185502, 2020.

[19] A. K. Desta, S. Ohira, I. Arai, and K. Fujikawa, "Rec-CNN: In-vehicle networks intrusion detection using convolutional neural networks trained on recurrence plots," *Veh. Commun.*, vol. 35, Jun. 2022, Art. no. 100470.

[20] A. Gazdag, S. Lestyán, M. Remeli, G. Ács, T. Holczer, and G. Biczók, "Privacy pitfalls of releasing in-vehicle network data," *Veh. Commun.*, vol. 39, Feb. 2023, Art. no. 100565.

[21] G. Kocher and G. Kumar, "Machine learning and deep learning methods for intrusion detection systems: Recent developments and challenges," *Soft Comput.*, vol. 25, no. 15, pp. 9731–9763, Aug. 2021.

[22] M. M. Najafabadi, F. Villanustre, T. M. Khoshgoftaar, N. Seliya, R. Wald, and E. Muharemagic, "Deep learning applications and challenges in big data analytics," *J. Big Data*, vol. 2, no. 1, pp. 1–21, Dec. 2015.

[23] A. R. Munappy, J. Bosch, H. H. Olsson, A. Arpteg, and B. Brinne, "Data management for production quality deep learning models: Challenges and solutions," *J. Syst. Softw.*, vol. 191, Sep. 2022, Art. no. 111359.

[24] H. Shi and D. Zhao, "License plate recognition system based on improved YOLOv5 and GRU," *IEEE Access*, vol. 11, pp. 10429–10439, 2023.

[25] H. M. Lynn, S. B. Pan, and P. Kim, "A deep bidirectional GRU network model for biometric electrocardiogram classification based on recurrent neural networks," *IEEE Access*, vol. 7, pp. 145395–145405, 2019.

[26] L. Zhang, L. Shi, N. Kaja, and D. Ma, "A two-stage deep learning approach for can intrusion detection," in *Proc. Ground Vehicle Syst. Eng. Technol. Symp. (GVSETS)*, Aug. 2018, pp. 1–11.

[27] L. Zhang, X. Yan, and D. Ma, "A binarized neural network approach to accelerate in-vehicle network intrusion detection," *IEEE Access*, vol. 10, pp. 123505–123520, 2022.

[28] M. Markovitz and A. Wool, "Field classification, modeling and anomaly detection in unknown CAN bus networks," *Veh. Commun.*, vol. 9, pp. 43–52, Jul. 2017.

[29] A. Derhab, M. Belaoued, I. Mohiuddin, F. Kurniawan, and M. K. Khan, "Histogram-based intrusion detection and filtering framework for secure and safe in-vehicle networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2366–2379, Mar. 2022.

[30] C. Wang, Z. Zhao, L. Gong, L. Zhu, Z. Liu, and X. Cheng, "A distributed anomaly detection system for in-vehicle network using HTM," *IEEE Access*, vol. 6, pp. 9091–9098, 2018.

[31] C. Young, H. Olufowobi, G. Bloom, and J. Zambreno, "Automotive intrusion detection based on constant CAN message frequencies across vehicle driving modes," in *Proc. ACM Workshop Automot. Cybersecurity*, Mar. 2019, pp. 9–14.

[32] M. Hanselmann, T. Strauss, K. Dormann, and H. Ulmer, "CANet: An unsupervised intrusion detection system for high dimensional CAN bus data," *IEEE Access*, vol. 8, pp. 58194–58205, 2020.

[33] T.-N. Hoang and D. Kim, "Detecting in-vehicle intrusion via semi-supervised learning-based convolutional adversarial autoencoders," *Veh. Commun.*, vol. 38, Dec. 2022, Art. no. 100520.

[34] S. B. Park, H. J. Jo, and D. H. Lee, "G-IDCS: Graph-based intrusion detection and classification system for CAN protocol," *IEEE Access*, vol. 11, pp. 39213–39227, 2023.

[35] T.-N. Hoang, M. R. Islam, K. Yim, and D. Kim, "CANPerFL: Improve in-vehicle intrusion detection performance by sharing knowledge," *Appl. Sci.*, vol. 13, no. 11, p. 6369, May 2023. [Online]. Available: https://www.mdpi.com/2076-3417/13/11/6369

[36] Y. Saishu, A. H. Poorjam, and M. G. Christensen, "A CNN-based approach to identification of degradations in speech signals," *EURASIP J. Audio, Speech, Music Process.*, vol. 2021, no. 1, pp. 1–10, Dec. 2021.

[37] N. Hajarolasvadi and H. Demirel, "3D CNN-based speech emotion recognition using K-means clustering and spectrograms," *Entropy*, vol. 21, no. 5, p. 479, May 2019.

[38] D.-Y. Wu and Y.-H. Yang, "Speech-to-singing conversion based on boundary equilibrium GAN," 2020, *arXiv:2005.13835*.

[39] A. Wang, "An industrial strength audio search algorithm," in *Proc. ISMIR*, Washington, DC, USA, 2003, pp. 7–13.

[40] T. N. S. T. Zawawi, A. R. Abdullah, E. F. Shair, I. Halim, and O. Rawaida, "Electromyography signal analysis using spectrogram," in *Proc. IEEE Student Conf. Res. Developement*, Dec. 2013, pp. 319–324.

[41] O. Christensen, H. Feichtinger, and S. Paukner, "Gabor analysis for imaging," in *Handbook in Imaging*. Cham, Switzerland: Springer, 2010.

[42] H. Kim, "Machine anomaly detection using sound spectrogram images and neural networks," Ph.D. dissertation, School Mech. Eng., Purdue Univ. Graduate School, West Lafayette, Indiana, 2019.

[43] A. S. Khan, Z. Ahmad, J. Abdullah, and F. Ahmad, "A spectrogram image-based network anomaly detection system using deep convolutional neural network," *IEEE Access*, vol. 9, pp. 87079–87093, 2021.

[44] S. L. Brunton and J. N. Kutz, *Data-Driven Science and Engineering: Machine Learning, Dynamical Systems, and Control*. Cambridge, U.K.: Cambridge Univ. Press, 2022.

[45] J. Chou, D. R. Solli, and B. Jalali, "Real-time spectroscopy with subgigahertz resolution using amplified dispersive Fourier transformation," *Appl. Phys. Lett.*, vol. 92, no. 11, Mar. 2008, Art. no. 111102.

[46] S. K. Sinha, P. S. Routh, P. D. Anno, and J. P. Castagna, "Optimum time-frequency resolution of seismic data using continuous wavelet transform," in *Proc. 5th Conf. Expo. Petroleum Geophys.*, Hyderabad, India, 2004, p. 984.

[47] S. Qiu and H. G. Feichtinger, "Discrete Gabor structures and optimal representations," *IEEE Trans. Signal Process.*, vol. 43, no. 10, pp. 2258–2268, 1995.

[48] A. Teolis and A. Teolis, "Continuous wavelet and Gabor transforms," in *Computational Signal Processing with Wavelets*. Cham, Switzerland: Birkhäuser, 1998, pp. 59–88.

[49] F. Fakhfakh, M. Tounsi, and M. Mosbah, "Cybersecurity attacks on CAN bus based vehicles: A review and open challenges," *Library Hi Tech*, vol. 40, no. 5, pp. 1179–1203, Nov. 2022.

[50] Z. Bi, G. Xu, G. Xu, M. Tian, R. Jiang, and S. Zhang, "Intrusion detection method for in-vehicle CAN bus based on message and time transfer matrix," *Secur. Commun. Netw.*, vol. 2022, pp. 1–19, Mar. 2022.

[51] M. R. Ansari, W. T. Miller, C. She, and Q. Yu, "A low-cost masquerade and replay attack detection method for CAN in automobiles," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2017, pp. 1–4.

[52] *OCSLab*. Accessed: Oct. 31, 2023. [Online]. Available: https://ocslab.hksecurity.net/welcome

[53] G. Manhertz and A. Bereczky, "STFT spectrogram based hybrid evaluation method for rotating machine transient vibration analysis," *Mech. Syst. Signal Process.*, vol. 154, Jun. 2021, Art. no. 107583.

[54] R. Dey and F. M. Salem, "Gate-variants of gated recurrent unit (GRU) neural networks," in *Proc. IEEE 60th Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Aug. 2017, pp. 1597–1600.

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.

MAHDI SAHLABADI (Senior Member, IEEE) 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.

KEUNKYOUNG KIM received the B.S. and M.S. degrees from the Department of Electronics Engineering, Ajou University, Suwon, South Korea, in 1999 and 2002, respectively. She is currently pursuing the Ph.D. degree with the Department of Software Convergence Engineering, Soonchunhyang University. Her research interests include big data analysis and deep learning technology for malicious packet filtering and misbehavior detection.

YOONJI KIM received the B.S. degree from the Department of Information Security Engineering, Soonchunhyang University, South Korea, in 2023. She is currently pursuing the master's degree in mobility convergence security with Soonchunhyang University. Her research interests include external sensor vulnerability analysis and automotive security.

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, malware 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*.