International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 12 Issue 1 ǁ January 2024 ǁ PP. 140-149

Cyber Attack Detection for Self-Driving Vehicles Using ML Algorithms

Azadeh Namiranian
Department of Tech and Software
University of Europe
Potsdam, Germany
azadeh.namiranian@ue-germany.de

Prof. Dr. Mohammed Nazeh Alimam
Department of Tech and Software
University of Europe
Potsdam, Germany
mohammednazeh.alimam@ue-germany.de

Prof. Dr. Iftikhar Ahmed
Department of Tech and Software
University of Europe
Potsdam, Germany
iftikhar.ahmed@ue-germany.de

Abstract*—The small computers in Connected and Autonomous Vehicles (CAVs) are referred to as Electronic Control Units (ECUs) and are often perceived as being a component of a broader cyber–physical system. The Controller Area Network (CAN) protocol ensures that all these components can effectively communicate with each other. Nevertheless, the integration of smart features has rendered CAVs susceptible to heightened security risks, as hackers can exploit these connections to gain unauthorized access to vehicle systems. The focus of this research is on the use of machine learning algorithms to detect cyber threats. Specifically, the study employs the Random Forest and Support Vector Machine algorithms for intrusion detection on the CAN bus. The research leverages the 'Car Hacking Dataset for Intrusion Detection (HCRL CH),' derived from real vehicle data, to train and evaluate the model. The proposed model proficiently classifies a range of attacks including reconnaissance, Denial of Service (DoS), fuzzing attacks, spoofing gear attacks, and spoofing RPM attacks. Performance evaluation metrics such as accuracy, precision, recall, F-1 score, and AUC-ROC are utilized to gauge the algorithms' efficacy. Furthermore, the research enhances accuracy and computational efficiency through preprocessing steps and feature selection techniques. Notably, the results underscore the superiority of the proposed model, as it exhibits superior accuracy compared to prior investigations. This advancement holds promise for bolstering the security of CAVs against evolving cyber threats.*

***Keywords*—** *Controller Area Network, Cyber Attack, Self-Driving Vehicles, Machine Learning, Connected and Autonomous Vehicles.*

Date of Submission: 05-01-2024 Date of acceptance: 17-01-2024

I. INTRODUCTION

Connected and autonomous vehicles (CAVs) use advanced technologies to enable communication, sensing, and decision-making capabilities. They can navigate and operate independently or with minimal human intervention and improve road safety, reduce congestion, increase efficiency, and enhance mobility [1]. As vehicles evolve into intelligent entities, they become part of larger cyber-physical systems. This opens the door to potential cyberattacks that can cause privacy breaches and safety hazards [2].

The CAN bus protocol is the most recognized and extensively adopted standard in the automotive domain, and it is deeply ingrained within the architecture of contemporary vehicles. Other protocols may offer supplementary benefits, but they are more likely to complement the role of the CAN bus rather than entirely replace it [3] [4] [5] [6].

Numerous in-vehicle networks were initially designed without considering security measures, but today's vehicles boast a range of connectivity features such as cellular service, Wi-Fi, and Bluetooth [7]. When it

comes to protecting CAN, an Intrusion Detection System (IDS) is a pivotal solution. A machine learning-based IDS can dynamically adapt to the intricate and ever-evolving cybersecurity challenges posed by in-vehicle networks [8].

Machine learning-based intrusion detection systems are pivotal components in the defense against an escalating array of cyber threats in modern automobiles. These systems can be classified into two principal groups: unsupervised and supervised models [9]. Unsupervised models learn normal patterns and identify deviations from this norm as potential anomalies, while supervised models learn from known attack instances [10].

The scope of this thesis is to develop and implement a system that monitors CAN bus traffic within CAVs, utilizing state-of-the-art ML algorithms to detect injected attacks accurately and reliably. The focus lies in creating a defense mechanism that ensures the highest level of safety for passengers and road users by mitigating the risks associated with potential cyber threats.

Here is a summary of the important contributions in this article:

- The application of Random Forest and Support Vector Machine (SVM) algorithms has been employed as a robust approach for detecting potential attacks within the CAN bus communication protocol.
- This study leverages real-world vehicle data for modeling, validation, and detection purposes. Various preprocessing steps have been employed to enhance the quality of the data. Moreover, in order to enhance computational efficiency and algorithmic performance, a feature selection process has been implemented. These strategies collectively contribute to refining the accuracy and effectiveness of the applied algorithms in detecting anomalies and security threats within the vehicular context.
- A comprehensive comparative analysis between the proposed methodology and existing techniques underscores its superior accuracy. This quality positions it as a more suitable and effective solution for real-world applications in Connected and Autonomous Vehicles.

Following is an overview of the rest of this study. Section 2 provides a review of the theoretical background of CAN bus concepts, describes attack scenarios and models based on CAN networks, as well as analyzing other literature in this field. Detailed information on the methodology of this study is provided in Section 3, which includes the dataset used, the preprocessing steps, the machine learning algorithms, and the performance metrics used to evaluate results. In section 4, the results are described, figures and tables are included, and the results of this study are compared with those of previous studies. In Section 5, the work of this thesis is summarized, and some future research directions are provided.

II. THEORICAL BACKGROUND AND LITERATURE REVIEW

A. Theorical Background

The Controller Area Network (CAN) bus is a pivotal component in the realm of modern automotive and industrial control systems, providing a standardized and efficient communication protocol that facilitates seamless data exchange between diverse electronic control units (ECUs) [1] [3]. It was developed by Robert Bosch GmbH in the 1980s [11]. One of its most remarkable features is its capacity to operate without the need for a central computer. This decentralized architecture, where multiple ECUs can communicate directly with each other, is particularly advantageous in scenarios where rapid and reliable information exchange is essential [12]. The CAN bus employs a meticulously structured frame format, with each component playing a specific role. These components include: Start of Frame (SOF), Arbitration Field (Identifier Field, RTR Bit), Control Field (DLC, Reserved Bits), Data Field, CRC Field, ACK Field (ACK Slot, ACK Delimiter), End of Frame (EOF), and Interframe Space (IFS) [3] [7] [8] [9]. The CAN bus, while revolutionary in vehicle and industrial communication, has vulnerabilities necessitating thorough understanding for robust security measures. Key concerns include lack of authentication and encryption, physical access risks, broadcast nature facilitating interception, limited segmentation complicating containment, firmware/software vulnerabilities, potential for cyber-physical attacks, and the absence of intrusion detection mechanisms [8] [13] [14].

The literature review identifies various types of attacks on the CAN bus, such as DoS, Fuzzy, Insertion, Spoofing, and Hybrid attacks, emphasizing the need for understanding and countering these threats in vehicle communication systems [15]. These attacks disrupt communication and can lead to malfunctions. Intrusion Detection Systems (IDS) are employed to enhance detection precision and collect routing information for identifying attack categories swiftly.

Research efforts are actively improving the security of autonomous vehicles, with a focus on artificial intelligence (AI) as a vital component for addressing emerging threats, especially in smart city contexts [16]. Machine learning-based Intrusion Detection Systems (IDS) are pioneering advancements, leveraging AI and data analysis to detect anomalies in CAN bus traffic. These IDS systems adapt to evolving threats, categorizing into unsupervised (detecting deviations from normal patterns) and supervised (trained on labelled data for precise classification) models [9] [13]. These systems play a critical role in safeguarding Connected and Autonomous

Vehicles (CAVs), ensuring their safety, privacy, and integrity in an increasingly technology-driven automotive industry [17].

B. Literature Review

In these research studies, various innovative approaches to intrusion detection in vehicle networks are explored. Article [18] distinguishes between flow-based and payload-based approaches for IDSs in intra-vehicle networks and introduces CANova, a hybrid IDS that combines both approaches to achieve high detection rates and reduced computation demands, demonstrating exceptional accuracy of 0.9997. Article [19] explores the application of transfer learning in designing an in-vehicle IDS, introducing CANPerFL, a federated learning-based system that encourages cross-manufacturer collaboration while respecting data privacy, and demonstrates the system's ability to enhance local models' F1 scores. Article [20] presents CANet, a neural network architecture that operates within the signal space of CAN data and excels in unsupervised detection of unknown attack types with an accuracy over 0.99. In paper [21], H-IDFS is proposed as a Histogram-based Intrusion Detection and Filtering framework that achieves 100% accuracy in window classification and accurately filters out normal packets from malicious windows. Article [22] introduces a method using CNNs trained on recurrence images generated from encoded arbitration ID labels to capture temporal dependencies in CAN bus data, achieving an accuracy of 0.999 in identifying various attacks. Finally, article [23] utilizes generative pretrained transformer (GPT) models to detect pattern changes in CAN ID sequences, offering potential for enhanced detection of abnormal message patterns in the presence of minimal attack IDs. These articles collectively contribute innovative approaches to improve the accuracy and efficiency of intrusion detection in vehicle networks, addressing various challenges and introducing novel techniques.

In article [14], a hybrid intrusion detection system (IDS) is introduced, combining rule-based and machine learning-based approaches in two stages for enhanced efficiency and the detection of a wide range of attack types, demonstrating accuracy between 99.76% and 99.9% using CAN traces from various vehicle models. Article [24] proposes an IDS using Binarized Neural Networks (BNNs) to improve intrusion detection speed and reduce memory and energy consumption, achieving faster detection on CPUs and substantial latency reduction (128 times faster) on FPGAs. Article [25] introduces the CNN-LSTM with Attention model (CLAM) for CAN attack detection, achieving an average F1-score of 0.951. Article [13] presents an IDS for CAN networks using Recurrence Plot (RP) concepts and neural networks, achieving high detection accuracy (95.10476%) and other key performance indicators. Article [26] proposes a dual decision-tree framework for intrusion detection in in-vehicle CAN networks, showing high accuracy in identifying various attack patterns. Article [27] develops an IDS for CAN networks, optimizing threshold values to detect fuzzy, merge, and DoS attacks with low false-positive rates. Article [28] introduces a transfer learning-based self-learning IDS (TLSIDS) for CANs, proficient in detecting both known and unknown attacks. Article [6] addresses message flooding attacks in in-vehicle CANs with a novel mitigator that preserves communication integrity. Article [29] presents a lightweight neural network framework for quicker intrusion detection, achieving significant improvements in detection time and accuracy. Article [30] outlines an IDS for in-car CAN bus traffic, capable of identifying field boundaries and types, with low false-positive rates. Finally, in [11], a transformer-based attention network (TAN) is introduced for multi-class intrusion detection in in-vehicle CAN networks, offering superior accuracy without explicit sequence labeling. In [4], an enhanced voltage-based intrusion detection system (VIDS) is proposed to detect overlapped voltage attacks, achieving a 99.4% accuracy rate and reducing attack success rates significantly compared to traditional VIDS solutions.

Article [3] introduces a novel intrusion detection method called AMAEID, which combines a threshold-based IDS with a machine learning-based attack type classifier. This comprehensive approach significantly enhances the security of the controller area network (CAN) protocol by reducing the required number of CAN messages for detection and improving combined attack detection accuracy. Study [31] focuses on achieving real-time intrusion detection within vehicles through a low-complexity feature extraction algorithm and a lightweight neural network. Article [32] presents a multi-stage intrusion detection framework for intelligent transportation systems, including autonomous vehicles, with minimal false alarm rates. It uses bidirectional Long Short-Term Memory (LSTM) architecture and demonstrates superior performance in real-time identification of intrusions. Article [33] conducts a comparative investigation of intrusion detection systems utilizing distinct machine learning models, highlighting the effectiveness of Random Forest (RF) in enhancing security. Study [34] transforms CAN messages into temporal graphs and employs machine learning algorithms for intrusion detection, achieving high accuracies. Article [10] introduces a semi-supervised convolutional adversarial autoencoder (CAAE) model for intrusion detection in in-vehicle networks, excelling in detecting unknown attacks and offering real-time capabilities.

In study [35], an AI-based system is introduced to enhance the security of vehicle networks, particularly in the context of connected autonomous vehicles (CAVs). This system utilizes deep learning techniques for real-time detection and classification of cyber threats within vehicle networks. It preprocesses a real-world automatic

vehicle network dataset, converting categorical data into numerical format, and employs convolutional neural network (CNN) and hybrid CNN-long short-term memory (CNN-LSTM) models to identify attack messages. By incorporating LSTM techniques, the study addresses challenges in recurrent neural network (RNN) learning and achieves an accuracy rate of 97.30%. This system's success has broad implications for securing autonomous vehicle networks and can be extended to other complex infrastructure security designs, ensuring secure data processing.

Article [36] introduces the CAN-GAT model, a graph neural network framework for anomaly detection in in-vehicle networks, achieving improved accuracy and efficiency. Article [37] presents ImageFed, a privacy-preserving IDS using federated Convolutional Neural Networks, showcasing high detection accuracy and low latency. Research [38] combines classical CNN and quantum RBM for CAN intrusion detection, outperforming purely classical methods. Article [39] introduces DACNN, an adversarial neural network for security intrusions in CAN buses, achieving low error rates. Study [5] proposes a real-time ECU-based intrusion detection method using a message and time transfer matrix. Article [15] utilizes VGG16 and XBoost classifiers for IVN threat detection, achieving high accuracy. Article [17] presents CAN-CID, an IDS for CAN bus cybersecurity with over 99% F1-Score in most attacks. Investigation [40] develops a hybrid quantum-classical NN for cyberattack detection with 94% accuracy. Article [41] introduces an intrusion detection framework involving feature selection and classifier utilization, improving performance. Article [42] introduces an advanced GAN model for detecting data tampering threats in CAN communication. Article [16] presents SIDuDTW, a methodology using DTW distance to identify malicious messages in vehicle networks, surpassing existing approaches in countering attacks. Finally, Article [43] presents a machine learning-based IDS using SVM, DT, and KNN algorithms, achieving high accuracy with real-world vehicle datasets and efficient feature extraction.

III. METHODOLOGY

The study focuses on leveraging the power of AI and ML algorithms for detecting and preventing injected attacks within the CAN bus, which serves as the in-vehicle network's communication backbone. By effectively distinguishing between normal network traffic and anomalies or outliers, the proposed approach aims to discard or block malicious data sources, ensuring the integrity and safety of CAVs. The goal is to create a robust defence mechanism that can identify injected attacks without triggering any false detections, as the consequences of even a single false negative in this domain are of paramount concern.

Classification algorithms are designed precisely for this task, making them the most suitable choice for this area. Classification algorithms are vital for in-vehicle network security due to their ability to detect anomalies, make real-time decisions, adapt to evolving attack patterns, recognize subtle deviations, minimize false positives, offer predictive analysis, and handle large data volumes efficiently, ensuring the robust protection of connected vehicle networks.

A. Dataset

For the purpose of applying the desired algorithms to detect the attack, standard datasets were used in this study [44]. The quality and accuracy of the data set allows accurate and reliable results to be obtained for the investigated subjects. Furthermore, the data sets were regularly and comprehensively evaluated and analysed in order to investigate the effects of each algorithm and their relationships clearly. This Study utilizes the 'Car hacking dataset for intrusion detection (HCRL CH)' as a dataset. This dataset holds a prominent status in the academic domain due to its extensive utilization within literature [3] [13]. It has been curated and made publicly accessible by the Hacking and Countermeasure Research Lab (HCRL) with the intent of facilitating academic research [44].

The dataset used for the experiments, [44], was constructed using a real vehicle. Two custom Raspberry Pi devices were utilized for data collection: one was responsible for logging the network traffic, and the other was employed to inject fabricated messages as the attack network via the OBD-II port located below the car's steering wheel. Through the OBD-II port, the custom nodes were able to send and receive messages from real ECU nodes on the CAN bus.

The dataset encompasses four distinct attack categories on the CAN bus: flooding attacks, spoofing gear, spoofing RPM, and fuzzy attacks. Flooding attacks overload the CAN network with a high volume of messages, disrupting communication. Spoofing gear and RPM attacks manipulate gear and RPM gauge data to mislead ECUs and potentially compromise safety. Fuzzy attacks exploit software vulnerabilities through careful monitoring and random data input, posing significant threats to automotive network security [44].

Table 1 provides a breakdown of the ratios between injected messages and the total number of messages for each dataset used in the experiments.

Dataset Name	**Number of**		
	Total Messages	***Normal Messages***	***Injected Messages***
DoS Attack	3,665,771	3,078,250	587,521
Fuzzy Attack	3,838,860	3,347,013	491,847
Spoofing the drive gear	4,443,142	3,845,890	597,252
Spoofing the RPM gauze	4,621,702	3,966,805	654,897
Attack-free (normal)	988,987	988,872	-
Merged	17,558,462	15,226,830	2,331,517

Table 1: *Databases' Description*

Each message included the following attributes: Timestamp (recording time), CAN ID (unique message identifier), DLC (payload size), DATA [1~8] (individual data bytes), and Flag ('T' for injected, 'R' for normal messages). Timestamp aided in event sequencing, CAN ID tracked message types, DLC indicated payload size, DATA [1~8] revealed message content, and Flag distinguished between injected and normal messages.

B. Preprocessing of Data

Preprocessing is a crucial step in machine learning that involves preparing and cleaning the raw dataset before applying machine learning algorithms [45]. It aims to enhance the quality of data, reduce noise, and ensure that the data is suitable for analysis by algorithms. Following is the several steps involves in preprocessing:

- Handling Missing Data: Data imputation is a common technique used in data preprocessing to handle missing values in a dataset and maintain the integrity of the data for subsequent analysis or modelling. For this purpose, imputing the missing data bytes with the placeholder value '00' for the rows where 'DLC' is equal to 2. This is done to ensure that all rows have a consistent row length of 8, allowing you to retain both message lengths (8 and 2).
- Data Conversion: In the given dataset, we have attributes such as 'CAN_ID', 'DLC', and 'DATA1' to 'DATA8', all of which contain values in hexadecimal format. To perform the conversion, the code utilizes Python's Pandas library, specifically the apply function along with lambda functions. This transformation ensures that the 'CAN_ID', 'DLC', 'DATA1' to 'DATA8' columns are now represented as integers, making them suitable for various data exploration, visualization, and machine learning tasks that require numeric input.
- Normalization and Scaling: Maximum-Minimum normalization, also known as Min-Max scaling has been used in this thesis which is suitable for this dataset [26] [55]. It's important to note that normalization should be applied to each feature independently, so that each feature is scaled based on its own range. Additionally, it's crucial to use the same maximum and minimum values during both training and testing phases to maintain consistency in the scaling. The purpose for using this context is to ensure that all features are on the same scale, preventing features with larger ranges from dominating the training process.
- Encoding Categorical Data: One-hot encoding is one of the most frequently used methods for obtaining numerical values by converting categorical characteristics, like the "Flag" feature in dataset [15]. Each category is represented by a binary column using one-hot encoding. Each column corresponds to a category, and a binary value of 1 or 0 indicates the presence or absence of that category in the original data. This approach avoids implying ordinality and is suitable for non-ordinal categorical data.
- Feature Selection: Feature selection techniques help identify and retain the most relevant features, reducing complexity and improving model performance. The application of Feature Importance Analysis from the Random Forest Classifier serves as a practical preprocessing step, facilitating a more streamlined and efficient utilization of the Random Forrest and SVM algorithm.

C. Random Forest Classifier

The Random Forest algorithm is exceptionally well-suited for classifying CAN bus traffic and detecting potential attacks due to its ensemble approach, which combines multiple decision trees, allowing it to handle high-dimensional datasets, mitigate overfitting, and maintain reliability in the face of data variations. Additionally, its feature importance analysis helps uncover critical attributes contributing to potential attacks, aiding in the enhancement of security measures. Notably, Random Forest's high accuracy is crucial for distinguishing between normal and malicious CAN bus messages, particularly in scenarios with imbalanced datasets, where it excels in providing reliable and robust detection of attack patterns.

D. The Sweet Spot

As mentioned above, there are four attack types, and accordingly four datasets for which the first random forest classifier was applied. This classifier's effectiveness is determined by two primary factors, and by effectiveness we mean that it is more accurate and consumes less computing power.

First, the number of features used to train the classifier makes a difference. As the number of features decreases, the amount of computing required for training the classifier decreases. In order to increase accuracy, feature selection is used, which involves selecting a subset of relevant and informative features from the original set of input features. Choosing a subset of features allows the model to be more efficient, less subject to overfitting, and potentially more generalizable to new data sets. It was for this purpose that the Random Forest algorithm was used to assess the importance of each feature. Based on the results of this analysis, the most influential attributes affecting attack detection were identified.

Second, there is a hyperparameter of the random forest classifier known as 'n-estimator'. The "n_estimators" parameter determines how many decision trees are included in the Random Forest. As a general rule, a model with more estimators is generally more robust and accurate, up to a certain point. However, adding too many trees can result in longer training times and increased memory usage without a notable improvement in performance. The 'n_estimators' parameter must be tuned in order to achieve a balance between model complexity and performance.

A methodical approach was adopted to determine the most appropriate hyperparameter settings and the optimal number of features for each experiment when evaluating the Random Forest algorithm. The value of the hyperparameter "n_estimators" was varied over a range of 5, 10, 50, and 100, allowing evaluation of how different decision tree quantities impacted algorithm performance. Additionally, the analysis was guided by feature selection, including a minimum of four features and up to all 11 features. Our objective was to identify the optimal configuration - the right combination of feature count and number of estimators - that would maximize algorithm accuracy while minimizing computational complexity. This parameter space was systematically explored in order to find the sweet spot setup that achieved an optimal balance between the use of features and the efficiency of computations.

E. Merged Dataset

As a matter of fact, in the real-world scenario, classification of CAN bus traffic according to attack types is not a straightforward task. As opposed to controlled experiments, in which attack types can be isolated for accuracy assessment, real-world scenarios require a more comprehensive approach. It is not a realistic representation of the classification system's performance in a holistic environment if you calculate the accuracy for each attack type dataset independently, and then average them. As a solution to this issue, all five datasets are merged into one comprehensive dataset, encompassing all types of attacks as well as normal messages.

With the creation of this merged dataset, a more comprehensive and representative sample of the complex and dynamic CAN bus traffic can be obtained. By merging these datasets, we have taken into account the complex interactions between different attack types and normal messages that may occur in real-world vehicular networks. In the following steps, a new Random Forest classifier is generated, trained, and applied to this merged dataset. As a result, a more accurate and practical assessment of the classifier's performance is possible under real-world conditions, in which the complexities of mixed traffic can affect the accuracy of the detection algorithm.

The same as all four previous datasets, A thorough and meticulous approach has been taken in the preprocessing of the data for this merged dataset , ensuring that all necessary steps are applied consistently. The procedure includes handling missing data through data imputation, converting hexadecimal values into decimal integers, performing Min-Max scaling for normalization, and eliminating certain less important features from the analysis. In addition, the number of features as well as the value of 'n_estimators', a crucial hyperparameter in the Random Forest classifier, have been carefully considered for the merged dataset.

F. Support Vector Machine Classifier

The utilization of the Support Vector Machine (SVM) classifier for detecting attacks within the CAN bus network offers several advantages tailored to the intricacies of CAN bus traffic analysis and attack detection. SVM excels in high-dimensional feature spaces, making it well-suited for the complex nature of CAN bus data. It can handle nonlinear decision boundaries through kernel functions, accommodating the intricate distribution of CAN bus messages. SVM's focus on maximizing the margin between classes enhances generalization and robustness, especially against outliers or noisy data points. The SVM's core principle involves finding the optimal hyperplane that best separates data into distinct classes, with support vectors playing a crucial role. SVM's ability to generalize effectively, even with limited labeled data, is vital for maintaining the integrity of vehicular communication systems and preventing cyber-attacks in the context of CAN bus attack detection, ensuring vehicle safety and security.

G. Performance Measurements

Evaluating a CAN bus security system is crucial to ensure its effectiveness in detecting and preventing attacks on the communication network within modern vehicles. Various metrics are employed to comprehensively assess the system's ability to distinguish normal from malicious traffic.

A key tool in this assessment is the Confusion Matrix, which breaks down predicted and actual classes, enabling analysis of true positives, true negatives, false positives, and false negatives. Components of this matrix include True Positive (TP), correctly identifying attacks; False Positive (FP), wrongly identifying normal messages as attacks; True Negative (TN), correctly identifying normal messages; and False Negative (FN), missing actual attacks. These components form the basis of several performance measurements.

False Negative Rate (FNR) gauges missed detections of real threats, while False Positive Rate (FPR) indicates unnecessary alarms. Accuracy measures overall correctness, while Precision evaluates the accuracy of attack identifications. Recall (or Sensitivity) captures identified attacks out of actual attack messages. The AUC-ROC (Area Under the Receiver Operating Characteristic curve) quantifies the model's performance, particularly in imbalanced datasets. Lastly, the F1 Score balances precision and recall, especially useful when dealing with imbalanced data.

These measurements provide valuable insights into the security system's ability to accurately detect attacks and avoid false alarms. By using these metrics, automakers and cybersecurity experts can identify system weaknesses, optimize performance, and continuously enhance the security of vehicle networks.

IV. RESULTS AND DISCUSSION

Results from the fuzzy attack dataset show that the algorithm consistently achieves the highest levels of accuracy when it employs 10 features for classification and the 'n_estimators' parameter is set to either 10 or 50. A flawless accuracy rate of 100 percent is achieved when both the number of features and the number of estimators is aligned at 10. According to this insight, an optimum point exists within the parameter space that yields optimal results for the Fuzzy attack dataset.

Using the DOS attack dataset, the rigorous experimentation showed that changes in the 'n_estimators' hyperparameter have a negligible impact on accuracy levels. For this dataset, the accuracy trends remain consistent regardless of the value of 'n_estimators', suggesting that this parameter does not significantly affect the algorithm's performance. A notable finding is that when a minimum of 9 features are selected, the algorithm consistently achieves a perfect accuracy rate of 100 percent. The optimal configuration for the DOS attack dataset is revealed by carefully identifying this key threshold of 9 features and pairing it with a value of 'n_estimators' of 5.

A study of the Random Forest classifier on datasets associated with two different attack types, namely Spoofing RPM and gear attacks, reveals remarkable consistency in its performance. In both of these datasets, the classifier achieved an unwavering 100 percent accuracy rate. This striking level of accuracy demonstrates the effectiveness of the chosen machine learning algorithm in detecting and mitigating these types of attacks. It becomes increasingly evident that the Random Forest classifier proves to be particularly adept at handling these scenarios, showcasing its robustness in the realm of in-vehicle network security within the context of connected vehicles.

For both Spoofing RPM and Gear Attack datasets, the "sweet spot" occurs when a minimal set of only four carefully selected features is used, together with a value of 'n_estimators' of 5. This configuration consistently yields the highest accuracy, highlighting the significance of feature selection and emphasizing the importance of this specific number of features and the choice of 'n_estimators' in achieving optimal performance. Not only do these results underscore the effectiveness of the Random Forest classifier, but they also provide valuable insights into fine-tuning the classifier for these specific types of attacks.

A. Merged Dataset Analysis

In accordance with what has been discussed previously, the optimal configuration for the Fuzzy attack dataset involves utilizing 10 features and setting the number of 'n_estimators' to 10. A configuration based on 9 features and a 'n_estimators' value of 5 is optimal for the DOS attack dataset. On the other hand, an optimal setting was determined for the other two datasets at four features and five 'n_estimators' values.

On the basis of these insightful findings, two primary experiments were conducted to evaluate the Random Forest classifier's performance on merged dataset. First, an experiment was conducted using the optimal configuration of 10 features and a value of 'n_estimators' set to 10. In the second experiment, 9 features were employed, ‘n_estimators’ was equal to 50, and the aim was to explore whether a slightly reduced dimensionality of features, along with a larger number of trees, would improve classifier robustness and generalization. The results show that both scenarios are highly effective in detecting attacks, with a detection accuracy of 0.999999 % in both cases.

B. Analysis SVM Classifier

The next contribution in this thesis consists of the use of a SVM classifier to detect attacks on CAN buses. The SVM algorithm is capable of excellent performance in terms of accuracy, precision, recall, and F1-score; however, the time it takes for the algorithm to classify data can be a significant drawback, particularly when dealing with real-time scenarios such as Connected and Autonomous Vehicles (CAVs). Detection speed is critical in CAVs, where decisions must be made in real time to ensure both the safety of the vehicle's occupants and the safety of others on the road. Despite its high-performance metrics, SVM classifiers may not be the best match for CAN bus attack detection in CAVs if they take a long time to detect threats.

C. Comparing Results with Articles

In Table 2, the results of five different articles utilizing different machine learning algorithms were compared, in order to provide a comprehensive understanding of how each approach performs. A weighted average of four datasets' accuracy, which is 100%, is used for this comparison. By comparing the results of these articles, it is evident that this study showcases its remarkable achievement in achieving a higher accuracy than previous benchmarks, thereby significantly enhancing the security protocols for interconnected automobiles.

References	***Algorithms***	***Model (Accuracy %)***	***Number of Attacks***
[8]	CNN-LSTM	97	4 attacks and normal
[46]	LSTM model	80	4 attacks and normal
[36]	ML	90	4 attacks and normal
[37]	Neural network and LSTM	90	3 attacks and normal
[47]	Deep autoencoder	99.98	4 attacks and normal
My System	Random Forest	100	4 attacks and normal

Table 2:Comparison Results of 6 Research

V. CONCLUSION AND FUTURE WORK

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

A. Conclusion

The Controller Area Network (CAN) bus is a crucial component in modern vehicles and industrial control systems, enabling seamless data exchange among electronic control units (ECUs). However, it faces vulnerabilities like the lack of authentication and encryption, physical access risks, and more. To address these issues, comprehensive security measures are necessary, including intrusion detection systems (IDS) to monitor and detect abnormal network behaviour.

To employ the power of machine learning algorithms for detecting attacks, this thesis specifically utilized the random forest and support vector machine (SVM) classifiers. Both Random Forest and SVM share the virtue of being relatively resistant to overfitting when properly tuned, making them suitable for the limited labelled data that might be available for training in the CAN bus domain.

The study relied on the 'Car-Hacking Dataset for Intrusion Detection (HCRL CH),' a dataset compiled from a real vehicle's CAN bus traffic. The dataset was collected using custom Raspberry Pi devices placed in a vehicle. These devices logged network traffic and injected fabricated messages simulating various attack scenarios via the OBD-II port.

The preprocessing in this study includes handling missing data through data imputation, converting hexadecimal data into integers, normalizing numerical data using Min-Max scaling, and encoding categorical variables using one-hot encoding, all of which improve data integrity and enable accurate machine learning models.

In the study, a comprehensive exploration of machine learning techniques for enhancing in-vehicle network security is undertaken. The study highlights two critical factors that significantly influence the performance of Random Forest classifiers in the context of attack detection. Firstly, the number of features used for classifier training plays a pivotal role. Feature selection, which involves choosing a subset of relevant features, is employed to boost accuracy while maintaining efficiency and generalizability. This approach is meticulously assessed, revealing optimal configurations for specific attack datasets. Furthermore, the 'n_estimators'

hyperparameter, which controls the number of decision trees in the Random Forest ensemble, is examined. Striking a balance between model complexity and performance is essential, and systematic experimentation identifies the most effective 'n_estimators' settings for different attack scenarios.

A notable achievement is the determination of optimal configurations for specific attack types, such as fuzzy and Denial of Service (DoS) attacks. For instance, the thesis demonstrates that the Random Forest classifier achieves the highest accuracy when using 10 features and setting 'n_estimators' to either 10 or 50 for fuzzy attack datasets. In contrast, the 'n_estimators' parameter has minimal impact on accuracy in the case of DoS attack datasets, where consistent high accuracy levels are observed regardless of its value. The findings underscore the adaptability and robustness of the Random Forest classifier in handling diverse attack scenarios within in-vehicle network security.

Additionally, the study addresses the real-world complexity of classifying CAN bus traffic by merging various attack datasets into one comprehensive dataset. This approach provides a more accurate representation of dynamic vehicular networks and allows for a practical evaluation of the classifier's performance in complex, mixed-traffic scenarios. Subsequent experiments reveal optimal configurations that maintain exceptional detection accuracy while considering computational efficiency. This research contributes significantly to the advancement of in-vehicle network security, offering insights into the fine-tuning of machine learning algorithms for specific attack scenarios and real-world environments.

B. Future Work

Future research in this field could benefit from addressing five research gaps in this section.

1) There's a scarcity of diverse data for machine learning-based intrusion detection on the CAN bus, necessitating innovative strategies like data augmentation and transfer learning to enhance model performance with limited data.

2) The diversity of data sources across car manufacturers poses a challenge in building universal intrusion detection models, requiring adaptive and transferable models capable of handling varying data distributions.

3) The intersection of data privacy and collaborative learning in intrusion detection calls for secure and privacy-preserving techniques to facilitate knowledge sharing among manufacturers without compromising data confidentiality.

4) Future research should explore more complex and sophisticated attack scenarios to assess the robustness and adaptability of intrusion detection systems, considering multifarious attack patterns.

5) Existing research often overlooks novel cyber-attacks, emphasizing the need for broader approaches that can adapt to and detect emerging threats, enhancing overall intrusion detection system effectiveness.

REFRENCES

[1] Akib Anwar, Anika Anwar, Lama Moukahal, Mohammad Zulkernine, "Security assessment of in-vehicle communication protocols," *Vehicular Communications,* 2023.

[2] SMMT., "Innovation is great: connected and automated vehicles booklet," 2020.

[3] Park, Sung Bum and Jo, Hyo Jin and Lee, Dong Hoon, "G-IDCS: Graph-Based Intrusion Detection and Classification System for CAN Protocol," *IEEE Access,* vol. 11, pp. 39213-39227, 2023.

[4] Long Yin, Jian Xu, Chen Wang, Qiang Wang, Fucai Zhou, "Detecting CAN overlapped voltage attacks with an improved voltage-based in-vehicle intrusion detection system," *Journal of Systems Architecture,* 2023.

[5] Zixiang Bi, Guoai Xu, Guosheng Xu, Miaoqing Tian, Ruobing Jiang, Sutao Zhang, "Intrusion Detection Method for In-Vehicle CAN Bus Based on Message and Time Transfer Matrix," *Security and Communication Networks,* p. 19, 2022.

[6] Sung Bum Park, Hyo Jin Jo, Dong Hoon Lee, "Flooding attack mitigator for in-vehicle CAN using fault confinement in CAN protocol," *Computers & Security,* vol. 126, 2023.

[7] Bozdal, Mehmet, Mohammad Samie, Sohaib Aslam, and Ian Jennions, "Evaluation of CAN Bus Security Challenges," vol. 8, p. 2364, 2020.

[8] Brooke Lampe, Weizhi Meng, "A survey of deep learning-based intrusion detection in automotive applications," *Expert Systems with Applications,* vol. 221, 2023.

[9] Rajapaksha, Sampath and Kalutarage, Harsha and Al-Kadri, M. Omar and Petrovski, Andrei and Madzudzo, Garikayi and Cheah, Madeline, "AI-Based Intrusion Detection Systems for In-Vehicle Networks: A Survey," *Association for Computing Machinery,* vol. 55, 2023.

[10] Thien-Nu Hoang, Daehee Kim, "Detecting in-vehicle intrusion via semi-supervised learning-based convolutional adversarial autoencoders," *Vehicular Communications,* vol. 38, 2022.

[11] R. B. Gmbh, "BOSCH CAN Specification," Gerlingen, Stuttgart, 1991.

[12] Rathore, Rajkumar Singh, Chaminda Hewage, Omprakash Kaiwartya, and Jaime Lloret., "In-Vehicle Communication Cyber Security: Challenges and Solutions," *Sensors,* vol. 17, 2022.

[13] Al-Jarrah, Omar Y. and Haloui, Karim El and Dianati, Mehrdad and Maple, Carsten, "A Novel Detection Approach of Unknown Cyber-Attacks for Intra-Vehicle Networks Using Recurrence Plots and Neural Networks," *IEEE Open Journal of Vehicular Technology,* vol. 4, pp. 271-280, 2023.

[14] Ma, L. Zhang and D., "A Hybrid Approach Toward Efficient and Accurate Intrusion Detection for In-Vehicle Networks," *IEEE Access,* vol. 10, pp. 10852-10866, 2022.

[15] Lin, Hsiao-Chung, Ping Wang, Kuo-Ming Chao, Wen-Hui Lin, and Jia-Hong Chen, "Using Deep Learning Networks to Identify Cyber Attacks on Intrusion Detection for In-Vehicle Networks," *Electronics,* vol. 11, no. 14, 2022.

[16] Kyounggon Kim, Jun Seok Kim, Seonghoon Jeong, Jo-Hee Park, Huy Kang Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," *Computers & Security,* vol. 103, 2021.

[17] Rajapaksha, Sampath and Kalutarage, Harsha and Al-Kadri, M. Omar and Madzudzo, Garikayi and Petrovski, Andrei V., "Keep the Moving Vehicle Secure: Context-Aware Intrusion Detection System for In-Vehicle CAN Bus Security," *2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon),* vol. 700, pp. 309-330, 2022.

[18] Alessandro Nichelini, Carlo Alberto Pozzoli, Stefano Longari, Michele Carminati, Stefano Zanero, "CANova: A hybrid intrusion detection framework based on automatic signal classification for CAN," *Computers & Security,* vol. 128, 2023.

[19] T.-N. M. R. I. K. Y. a. D. K. Hoang, "CANPerFL: Improve In-Vehicle Intrusion Detection Performance by Sharing Knowledge," *Applied Sciences,* vol. 13, no. 11, 2023.

[20] 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.

[21] 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 Transactions on Intelligent Transportation Systems,* vol. 13, no. 3, pp. 2366-2379, 2022.

[22] Araya Kibrom Desta, Shuji Ohira, Ismail Arai, Kazutoshi Fujikawa, "Rec-CNN: In-vehicle networks intrusion detection using convolutional neural networks trained on recurrence plots," *Vehicular Communications,* vol. 35, 2022.

[23] M. Nam, S. Park and D. S. Kim, "Intrusion Detection Method Using Bi-Directional GPT for in-Vehicle Controller Area Networks," *IEEE Access,* vol. 9, pp. 124931-124944, 2021.

[24] 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.

[25] Sun, Heng and Chen, Miaomiao and Weng, Jian and Liu, Zhiquan and Geng, Guanggang, "Anomaly Detection for In-Vehicle Network Using CNN-LSTM With Attention Mechanism," *IEEE Transactions on Vehicular Technology,* vol. 70, pp. 10880-10893, 2021.

[26] Wang, B., Zhang, Y., Zhang, Z., Hu, H. et al., "An Intrusion Detection System Based on the Double-Decision-Tree Method for In-Vehicle Network," *SAE Technical Paper,* p. 7, 2023.

[27] Khan, Junaid, Dae-Woon Lim, and Young-Sik Kim., "Intrusion Detection System CAN-Bus In-Vehicle Networks Based on the Statistical Characteristics of Attacks," *Sensors,* vol. 7, 2023.

[28] Wang, Y., Lai, Y., Chen, Y. et al., "Transfer learning-based self-learning intrusion detection system for in-vehicle networks," *Neural Comput & Applic,* vol. 35, p. 10257–10273, 2023.

[29] Ding, Defeng ,Wei, Yehua, Cheng, Can, Long, Jing, "Intrusion Detection for In-Vehicle CAN Bus Based on Lightweight Neural Network," *Journal of Circuits, Systems and Computers,* vol. 32, no. 7, 2023.

[30] Moti Markovitz, Avishai Wool, "Field classification, modeling and anomaly detection in unknown CAN bus networks," *Vehicular Communications,* vol. 9, pp. 43-52, 2017.

[31] Ma, Haoyu and Cao, Jianqiu and Mi, Bo and Huang, Darong and Liu, Yang and Li, Shaoqian and Chen, Chen, A GRU-Based Lightweight System for CAN Intrusion Detection in Real Time, USA: John Wiley & Sons, Inc., 2022.

[32] Khan, Izhar Ahmed and Moustafa, Nour and Pi, Dechang and Haider, Waqas and Li, Bentian and Jolfaei, Alireza, "An Enhanced Multi-Stage Deep Learning Framework for Detecting Malicious Activities From Autonomous Vehicles," *IEEE Transactions on Intelligent Transportation Systems,* vol. 23, no. 12, pp. 25469-25478, 2022.

[33] Moulahi, Tarek and Zidi, Salah and Alabdulatif, Abdulatif and Atiquzzaman, Mohammed, "Comparative Performance Evaluation of Intrusion Detection Based on Machine Learning in In-Vehicle Controller Area Network Bus," *IEEE Access,* vol. 9, pp. 99595-99605, 2021.

[34] Refat, R.U.D., Elkhail, A.A., Hafeez, A., Malik, H., "Detecting CAN Bus Intrusion by Applying Machine Learning Method to Graph Based Features," in *Intelligent Systems and Applications,* 2022.

[35] Aldhyani, Theyazn H. H., and Hasan Alkahtani, "Attacks to Automatous Vehicles: A Deep Learning Algorithm for Cybersecurity," *Sensors,* vol. 1, 2022.

[36] Xiao, J., Yang, L., Zhong, F. et al., "Robust anomaly-based intrusion detection system for in-vehicle network by graph neural network framework," *Appl Intell,* vol. 53, p. 3183–3206, 2023.

[37] Taslimasa, Hamideh and Dadkhah, Sajjad and Carlos Pinto Neto, Euclides and Xiong, Pulei and Iqbal, Shahrear and Ray, Suprio and Ghorbani, Ali A., "ImageFed: Practical Privacy Preserving Intrusion Detection System for In-Vehicle CAN Bus Protocol," *2023 IEEE 9th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS),* pp. 122-129, 2023.

[38] Salek, M Sabbir and Biswas, Pronab and Pollard, Jacquan and Hales, Jordyn and Shen, Zecheng and Dixit, Vivek and Chowdhury, Mashrur and Khan, Sakib and Wang, Yao, "A Novel Hybrid Quantum-Classical Framework for an In-vehicle Controller Area Network Intrusion Detection," *IEEE Access,* vol. 8, 2023.

[39] Fatemeh Asghariyan, Mohsen Raji, "An Intrusion Detection System based on Deep Learning for CAN Bus," *Journal of Information and Communication Technology,* 2023.

[40] Islam, Mhafuzul and Chowdhury, Mashrur and Khan, Zadid and Khan, Sakib Mahmud, "Hybrid Quantum-Classical Neural Network for Cloud-Supported In-Vehicle Cyberattack Detection," *IEEE Sensors Letters,* vol. 6, no. 4, pp. 1-4, 2023.

[41] Dogukan Aksu, Muhammed Ali Aydin, "MGA-IDS: Optimal feature subset selection for anomaly detection framework on in-vehicle networks-CAN bus based on genetic algorithm and intrusion detection approach," *Computers & Security,* vol. 118, 2022.

[42] Guoqi Xie, Yang Laurence , Yuanda Yang, Haibo Luo, Renfa Li, Mamoun Alazab, "Threat Analysis for Automotive CAN Networks: A GAN Model-Based Intrusion Detection Technique," *IEEE Transactions on Intelligent Transportation Systems,* vol. 22, no. 7, pp. 4467-4477, 2021.

[43] Bari, Bifta Sama, Kumar Yelamarthi, and Sheikh Ghafoor., "Intrusion Detection in Vehicle Controller Area Network (CAN) Bus Using Machine Learning: A Comparative Performance Study," *Sensors,* vol. 7, 2023.

[44] Kim, Huy Kang, "CAR-HACKING DATASET," [Online]. Available: https://ocslab.hksecurity.net/Datasets/car-hacking-dataset. [Accessed August 2023].

[45] Nguyen, Trieu Phong and Nam, Heungwoo and Kim, Daehee, "Transformer-Based Attention Network for In-Vehicle Intrusion Detection," *IEEE Access,* vol. 11, pp. 55389-55403, 2023.

[46] Zhu, Konglin and Chen, Zhicheng and Peng, Yuyang and Zhang, Lin, "Mobile Edge Assisted Literal Multi-Dimensional Anomaly Detection of In-Vehicle Network Using LSTM," *IEEE Transactions on Vehicular Technology,* vol. 68, no. 5, pp. 4275-4284, 2019.

[47] Yang, Yun, Zongtao Duan, and Mark Tehranipoor., "Identify a Spoofing Attack on an In-Vehicle CAN Bus Based on the Deep Features of an ECU Fingerprint Signal," *Smart Cities,* vol. 3, no. 1, pp. 17-30, 2022.