INTRUSION DETECTION SYSTEM FOR REAL-TIME THREAT IDENTIFICATION IN SELF-DRIVING CARS

PROJECT REPORT

Submitted in the partial fulfilment of the requirements for award of the

Six Months Online Certificate Course

in

Cyber Security

Course Duration: [22-01-2024 to 21-07-2024]

By

Gumma V L Prasad
(Ht. No. 2406CYS107)

Under the Esteemed Guidance

Prof. Valli Kumari Vatsvayi

DIRECTORATE OF INNOVATIVE LEARNING & TEACHING

(DILT)

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
(Formerly SCDE_SCHOOL OF CONTINUING AND DISTANCE EDUCATION)
Kukatpally, Hyderabad, Telangana State, INDIA – 500 085
JULY 2024

ABSTRACT

Modern vehicles, particularly connected and autonomous vehicles, use a large number of electronic control units connected via intra-vehicle networks to implement numerous functionalities and conduct actions. Modern vehicles are also connected to external networks via vehicle-to-everything technologies, which allow them to communicate with other vehicles, infrastructures, and smart gadgets. However, the increasing capability and connection of modern automobiles makes them more vulnerable to cyber-attacks targeting both intra-vehicle and external networks due to their vast attack surfaces. To safeguard vehicular networks, many researchers have concentrated on building intrusion detection systems (IDSs) that employ machine learning to detect malicious cyber-attacks. In this project the vulnerabilities of intra-vehicle and external networks, are discussed and proposes an novel Intrusion Detection System (IDS) that combines a signature-based IDS with an anomaly-based IDS to detect both known and unknown attacks on vehicular networks. The experimental results show that the proposed system can detect all types of known attacks with 99.99% accuracy on the CAN-intrusion dataset representing intra-vehicle network data. and 99.88% accuracy on the CICIDS2017 dataset representing external vehicular network data. On the two datasets listed above, the suggested approach gets high F1-scores of 0.963 and 0.800 for zero-day attack detection. The average processing time of each data packet is less than 0.6 ms, demonstrating the viability of incorporating the proposed system into real-time vehicle systems. This emphasises the effectiveness and efficiency of the planned IDS.

TABLE OF CONTENTS

1. INTRODUCTION

1.0. Overview: The auto industry has undergone an extreme transformation driven by technology, particularly software innovations that elevated safety, sustainability, connectivity, and the overall user experience. Advancements in the field of EVs, autonomous driving, and software updates have revolutionised and enhanced the vehicle's performance, and improved vehicle design, manufacturing, and operational services. The integration of advanced technologies like human-machine Interface has redefined user interaction, all accessible remotely.

Autonomous cars are no longer a futuristic concept but a tangible reality, the future of mobility, equipped with sophisticated sensors, artificial intelligence, and intricate communication systems. However, with these advancements comes the looming threat of cyberattacks, prompting a paradigm shift in how we approach the security of autonomous vehicles solving these cybersecurity issues in autonomous cars has become a priority for manufacturers and users: protecting their systems in a scenario where cyberattacks are on the rise.

1.1. The Rise of Autonomous Vehicles: Autonomous vehicles, or self-driving cars, are rapidly becoming a reality. These vehicles can navigate roads without human intervention, relying on advanced technology to perceive their surroundings, make decisions, and control the vehicle. This emerging technology has the potential to revolutionize transportation.

Self-driving cars promise to enhance safety by eliminating human error, a primary cause of accidents. Additionally, they can contribute to reduced traffic congestion through optimized routing and coordinated movement. Improved efficiency in transportation systems is another potential benefit, as autonomous vehicles can optimize fuel consumption and reduce travel time.

Key technologies powering this revolution include:

- **Sensors:** LiDAR, radar, and cameras provide a comprehensive view of the vehicle’s environment.
- **Artificial Intelligence:** Complex algorithms process sensor data to interpret surroundings and make real-time decisions.
- **High-Performance Computing:** Powerful computers are essential for processing vast amounts of data and executing complex calculations.

  As technology continues to advance, autonomous vehicles are poised to reshape the way we travel and interact with our cities.

1.2. Security Challenges of Autonomous Vehicles: The advent of autonomous vehicles (AVs) has ushered in a new era of transportation, but it has also introduced a complex array of security challenges. These vehicles, heavily reliant on sophisticated software and network connectivity, present a significantly larger attack surface compared to traditional vehicles.

The potential consequences of a successful cyberattack on an AV are far-reaching. Most critically, it can compromise the safety of passengers, pedestrians, and other road users. A compromised AV could be manipulated to behave erratically, leading to accidents. Beyond safety, privacy breaches are a major concern. AVs collect vast amounts of data, including passenger information, driving habits, and location history. A data breach could expose sensitive personal details. Moreover, a large-scale cyberattack on AV infrastructure could disrupt transportation systems, causing economic losses and societal upheaval.

A variety of cyberattacks can target AVs. One common threat is sensor spoofing. By manipulating sensor data, attackers can deceive the vehicle into believing it is in a different environment than reality. For instance, a spoofed radar signal might make the vehicle believe there is no obstacle ahead, leading to a collision. Another critical vulnerability lies in the Electronic Control Units (ECUs) that govern various vehicle functions. By compromising these ECUs, attackers could gain control over steering, acceleration, or braking, potentially causing catastrophic consequences.

Denial-of-Service (DoS) attacks aim to overwhelm a system with traffic, rendering it inoperable. In the context of AVs, a DoS attack could disable critical functions like navigation or communication, making the vehicle unsafe. Finally, the increasing reliance on Vehicle-to-Everything (V2X) communication introduces new attack vectors. Malicious actors could intercept or manipulate data exchanged between vehicles, infrastructure, and pedestrians, leading to various security risks, including false information dissemination, unauthorized access, and privacy breaches.

Addressing these security challenges requires a multi-faceted approach involving robust encryption, secure software development practices, continuous monitoring, and incident response plans. As the deployment of AVs increases, so too must the focus on ensuring their cybersecurity.

1.3. Importance of Intrusion Detection Systems (IDS) for AVs: The increasing complexity and connectivity of autonomous vehicles (AVs) have magnified their vulnerability to cyberattacks. To safeguard these vehicles and their occupants, Intrusion Detection Systems (IDS) are indispensable.

An IDS serves as a vigilant guardian, constantly monitoring network traffic and system activity for anomalies indicative of malicious behaviours. By analysing data patterns, an IDS can identify potential threats such as unauthorized access, data breaches, and system tampering. This proactive approach is crucial for detecting and responding to cyberattacks before they can cause significant harm.

Real-time threat identification is paramount for the safety of AVs. Unlike traditional vehicles, AVs rely on a multitude of interconnected systems for operation. A cyberattack compromising these systems could have catastrophic consequences, including loss of control, unintended acceleration, or compromised braking. An IDS that can swiftly detect and alert system administrators to emerging threats is essential to prevent such incidents and protect the lives of passengers and pedestrians.

In essence, an IDS acts as a critical safety net for AVs, providing an early warning system against potential cyberattacks. By detecting threats in real-time, an IDS enables timely countermeasures to be implemented, safeguarding the integrity and reliability of these complex vehicles.

1.4. Existing Intrusion Detection Approaches for AVs : The development of effective intrusion detection systems (IDS) for autonomous vehicles (AVs) is a rapidly evolving field. Various approaches have been explored to address the unique challenges posed by this domain.

Signature-Based IDS

Signature-based IDS is a traditional approach that relies on predefined patterns or signatures of known attacks. This method involves creating a database of attack signatures and comparing incoming network traffic against these patterns. While effective for detecting known threats, it is limited in its ability to identify new or evolving attacks.

Anomaly-Based IDS

Anomaly-based IDS operates on the principle of detecting deviations from normal system behavior. By establishing a baseline of normal traffic patterns, this approach can identify unusual activities that may indicate a potential attack. While effective in detecting unknown threats, anomaly-based IDS can generate a high number of false positives, requiring additional analysis and refinement.

Machine Learning-Based IDS

Leveraging the power of machine learning, these IDS employ algorithms to learn patterns from historical data and identify anomalies or malicious activities. By analyzing vast amounts of data, machine learning models can adapt to evolving threats and improve detection accuracy over time. However, developing robust machine learning models for IDS requires significant computational resources and expertise.

Hybrid IDS

Recognizing the strengths and weaknesses of individual approaches, hybrid IDS combine multiple techniques to enhance detection capabilities. By integrating signature-based, anomaly-based, and machine learning components, hybrid IDS aim to achieve a balance between detection accuracy and false positive rates. This approach offers a more comprehensive and resilient solution for protecting AVs.

While these approaches provide a foundation for IDS development in the AV domain, several challenges remain. The dynamic nature of network traffic, the increasing complexity of AV systems, and the emergence of new attack techniques require continuous refinement and adaptation of IDS solutions. Additionally, ensuring low latency and minimal computational overhead is crucial for real-time threat detection in the fast-paced environment of autonomous driving.

Future research efforts should focus on developing intelligent IDS capable of handling large volumes of data, adapting to changing threat landscapes, and providing actionable insights to security personnel.

2. LITERATURE SURVEY

With the increasing research and rapid development of the Internet of Vehicles (IoV) technology, connected vehicles (CVs) and autonomous vehicles (AVs) are becoming increasingly popular in the modern world [1]. IoV serves as a primary vehicular communication framework that enables reliable communications between vehicles and other IoV entities, such as infrastructures, pedestrians, and smart devices. [1]. IoV consists mainly of intra-vehicle networks (IVNs) and external vehicular networks [1]. IVNs involve an increasing number of electronic control units (ECUs) to adopt various functionalities [2].

All ECUs in a vehicle are connected by a controller area network (CAN) bus to transmit messages and perform actions [3]. On the other hand, external networks connect modern vehicles to the outer environment by vehicle- to-everything (V2X) technologies. V2X technology allows modern vehicles to communicate with other vehicles, roadside infrastructures, and road users [4] [5]. However, with the increasing level of connectivity and complexity of modern vehicles, their security risks have become a significant concern. Cyber threats may decrease the stability and robustness of IoV, as well as cause vehicle unavailability or traffic accidents.

A real-life example can be found in [6]: two attackers compromised and fooled a jeep car into performing dangerous actions, including turning the steering wheel and activating the parking brake at highway speeds, causing severe accidents. In IVNs, CANs are mainly vulnerable to message injection attacks due to their broadcast communication strategy and the lack of authentication [4]. In external networks of IoV, vehicle systems are exposed to various common cyber-attacks, like denial-of-service (DoS), sniffing, and global positioning system (GPS) spoofing attacks [7]. This is because, in large external vehicular networks comprising various types of networks and entities, every node is a potential entry point for cyber-attacks.

Many traditional security mechanisms, like certain authentication and cryptographic techniques, are unsuitable for intra- vehicle networks because they are not supported in CANs or may violate timing constraints of CAN communications [8]. Thus, intrusion detection systems (IDSs) have become an essential component in modern IoV to identify malicious threats on vehicular networks [9]. IDSs are often incorporated into external networks as an essential component of the defense system to identify malicious attacks that can breach firewalls and authentication mechanisms. Although many previous works have made some success developing IDSs, intrusion detection is still a challenging problem due to the high volume of network traffic data, numerous available network features, and various cyber-attack patterns [7]. Machine learning (ML) and data mining algorithms have been recognized as effective models to design IDSs [10].

In this project the proposed novel IDS efficiently identifies known and zero-day cyber-attacks on both intra-vehicle and external networks using multiple ML algorithms. The proposed novel IDS framework consists of two traditional ML stages (data pre- processing and feature engineering). A comprehensive and robust IDS with both known and unknown attack detection functionalities can be obtained after the model learning and optimization procedures. Additionally, the quality of the used datasets can be improved by data pre-processing and feature engineering procedures to achieve more accurate attack detection. The performance of the proposed IDS is evaluated on two public network datasets, the CAN-intrusion-dataset [9] and the CICIDS2017 dataset [11], representing the intra- vehicle and external network traffic data, respectively. The model's feasibility, effectiveness, and efficiency are evaluated using various metrics, including accuracy, detection rates, false alarm rates, F1-scores, and model execution time.

The main contributions of this paper are:

- It proposes a novel IDS that can accurately detect the various surveyed types of cyber- attacks launched on both intra-vehicle and external vehicular networks.
- It proposes a novel feature engineering model based on information gain (IG), fast correlation-based filter (FCBF), and kernel principal component analysis (KPCA) algorithms.
- It proposes a novel anomaly-based IDS to detect zero-day attacks.
- It evaluates the performance and overall efficiency of the proposed model on two state-of-the-art datasets, CAN-intrusion-dataset and CICIDS2017, and discusses its feasibility in real-world IoV devices.

3. PROBLEM STATEMENT

The rapid development and increasing popularity of Internet of Vehicles (IoV) technology, encompassing both connected vehicles (CVs) and autonomous vehicles (AVs), has ushered in an era of enhanced vehicular communication. IoV, as a vehicular communication framework, facilitates reliable interactions between vehicles and other entities such as infrastructure, pedestrians, and smart devices. However, the increased connectivity and complexity of modern vehicles introduce significant security risks, making them susceptible to cyber threats that could compromise their stability, robustness, and safety. Traditional security mechanisms, such as authentication and cryptographic techniques, are often unsuitable for intra-vehicle networks (IVNs) due to the unique constraints and requirements of Controller Area Networks (CANs). Consequently, intrusion detection systems (IDSs) have emerged as crucial components for identifying and mitigating malicious threats within vehicular networks. Despite various advancements in IDS development, challenges remain due to the high volume of network traffic data, the plethora of available network features, and the diverse patterns of cyber-attacks. To address these challenges, the proposed study introduces a novel IDS that leverages multiple machine learning algorithms to detect both known and zero-day cyber-attacks on intra-vehicle and external networks. This innovative approach aims to enhance the accuracy and efficiency of IDSs in detecting sophisticated cyber threats in modern vehicular environments

4. OBJECTIVES

- Develop a novel Intrusion Detection System: Create an IDS framework utilizing multiple machine learning algorithms to identify known and zero-day cyber-attacks on both intra-vehicle and external networks.
- Optimize Learning Models for Enhanced Performance: Implement optimization techniques to improve the accuracy and efficiency of the supervised and unsupervised learning models used in the IDS.
- Evaluate the Proposed IDS on Public Datasets: Test the IDS on the CAN-intrusion-dataset and CICIDS2017 dataset to validate its effectiveness, efficiency, and generalizability in detecting various cyber-attacks on vehicular networks.

5. METHODOLOGY

The methodology for developing and evaluating the novel Intrusion Detection System (IDS) encompasses several critical steps to ensure its efficiency and robustness in detecting both known and zero-day cyber-attacks in vehicular networks. The approach integrates data pre-processing, feature engineering, model training, and evaluation using various machine learning algorithms and optimization techniques.

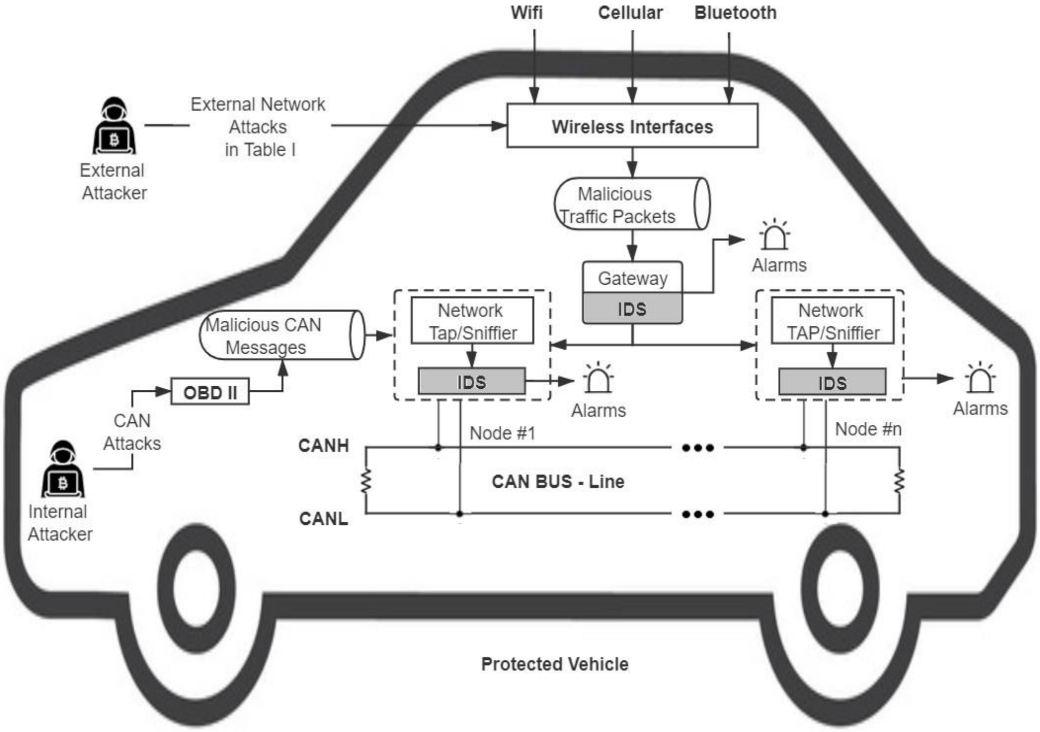


Fig. 5.1. The proposed IDS-protected vehicle architecture.

5.1. Data Pre-processing

1. Data Sampling by K-means Clustering:

To manage the extensive network traffic data typically generated in vehicular environments, a k-means clustering method is employed for data sampling. This method groups the original data into multiple clusters, and a representative subset is then selected from each cluster. This technique reduces training complexity and ensures the sampled data is highly representative of the original dataset. Bayesian Optimization (BO) is used to fine-tune the number of clusters (k) to improve the quality of the data subset.

2. Addressing Class-Imbalance with SMOTE:

Network traffic data often exhibit class imbalance, with normal data samples vastly outnumbering attack samples. The Synthetic Minority Oversampling Technique (SMOTE) is used to generate synthetic instances for the minority classes, balancing the dataset and preventing biased model performance. This technique enhances the detection rate of the IDS by ensuring that minority attack classes are adequately represented during training.

5.2. Feature Engineering

1. Feature Selection and Extraction:

Various techniques are applied to select and extract relevant features from the dataset. Information Gain (IG) and Fast Correlation-Based Filter (FCBF) methods remove irrelevant and redundant features, respectively, thus improving model accuracy and training efficiency. Kernel Principal Component Analysis (KPCA) is then used to further extract the most relevant features, reducing dimensionality and noise in the data.

5.3. Model Training and Optimization

1. Training Machine Learning Models:

Multiple tree-based machine learning algorithms are used to train base classifiers for known intrusion detection. These algorithms are selected for their superior performance with complex tabular data typical of vehicular networks.

2. Hyper-Parameter Optimization:

Bayesian Optimization is utilized to fine-tune the hyper-parameters of the machine learning models. This optimization ensures the models achieve the best possible performance by systematically exploring the hyper-parameter space based on prior evaluation results.

5.4. Anomaly-Based Detection:

For unknown attack detection, a clustered k-means (CL-k-means) approach is used. This method identifies clusters of normal and attack data, enabling the detection of zero-day attacks and unknown attack patterns.

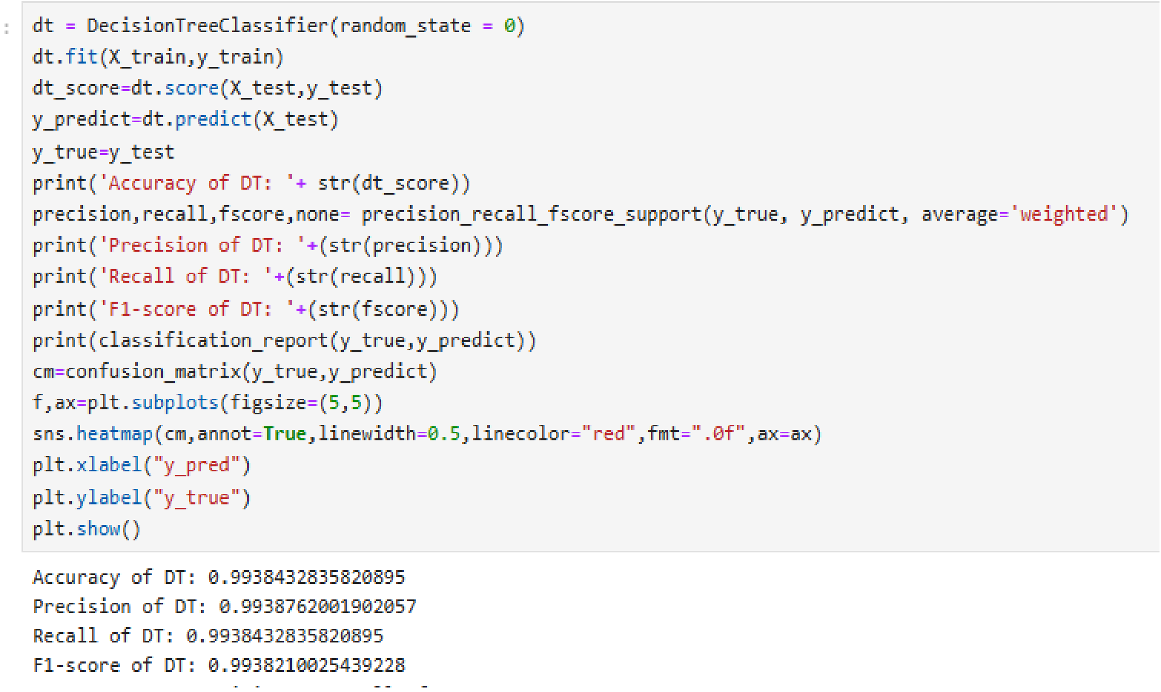
5.5. Runtime Complexity:

To ensure the IDS is suitable for real-time applications in vehicular environments, its runtime complexity is analysed. The testing process, implemented in vehicle systems, is designed to minimize latency and meet real-time requirements. The overall runtime complexity of the proposed IDS is maintained at a low level, ensuring its feasibility for practical deployment.

This comprehensive methodology ensures that the IDS is robust, efficient, and capable of accurately detecting a wide range of cyber-attacks in vehicular networks, addressing both known and emerging threats.

6. ALGORITHMS

In the development of the intrusion detection system (IDS) discussed in the article, algorithms were implemented using Python for effectively in handling complex data. The datasets used for training and testing the IDS were the CAN-intrusion-dataset for intra-vehicle network data and the CICIDS2017 dataset for external network data. Python libraries such as pandas for data handling, scikit-learn for implementing the machine learning models. Data preprocessing steps like feature engineering were performed to enhance the quality of the data, involving methods like information gain, fast correlation-based filter, and kernel principal component analysis. Overall, the development process heavily relied on Python for data manipulation, model training, and optimization, leveraging powerful libraries and techniques to create an effective IDS capable of accurately detecting various cyber-attacks on vehicular networks.



```
dt = DecisionTreeClassifier(random_state = 0)
dt.fit(X_train,y_train)
dt_score=dt.score(X_test,y_test)
y_predict=dt.predict(X_test)
y_true=y_test
print('Accuracy of DT: '+ str(dt_score))
precision,recall,fscore,none= precision_recall_fscore_support(y_true, y_predict, average='weighted')
print('Precision of DT: '+(str(precision)))
print('Recall of DT: '+(str(recall)))
print('F1-score of DT: '+(str(fscore)))
print(classification_report(y_true,y_predict))
cm=confusion_matrix(y_true,y_predict)
f,ax=plt.subplots(figsize=(5,5))
sns.heatmap(cm,annot=True,linewidth=0.5,linecolor="red",fmt=".0f",ax=ax)
plt.xlabel("y_pred")
plt.ylabel("y_true")
plt.show()
```

```
Accuracy of DT: 0.9938432835820895
Precision of DT: 0.9938762001902057
Recall of DT: 0.9938432835820895
F1-score of DT: 0.9938210025439228
```

7. IMPLEMENTATION

The implementation of the proposed Multi-Tier Hybrid Intrusion Detection System (MTH-IDS) involves several key steps, which are meticulously designed to ensure high performance and accuracy in detecting both known and zero-day cyber-attacks on intra-vehicle and external vehicular networks.

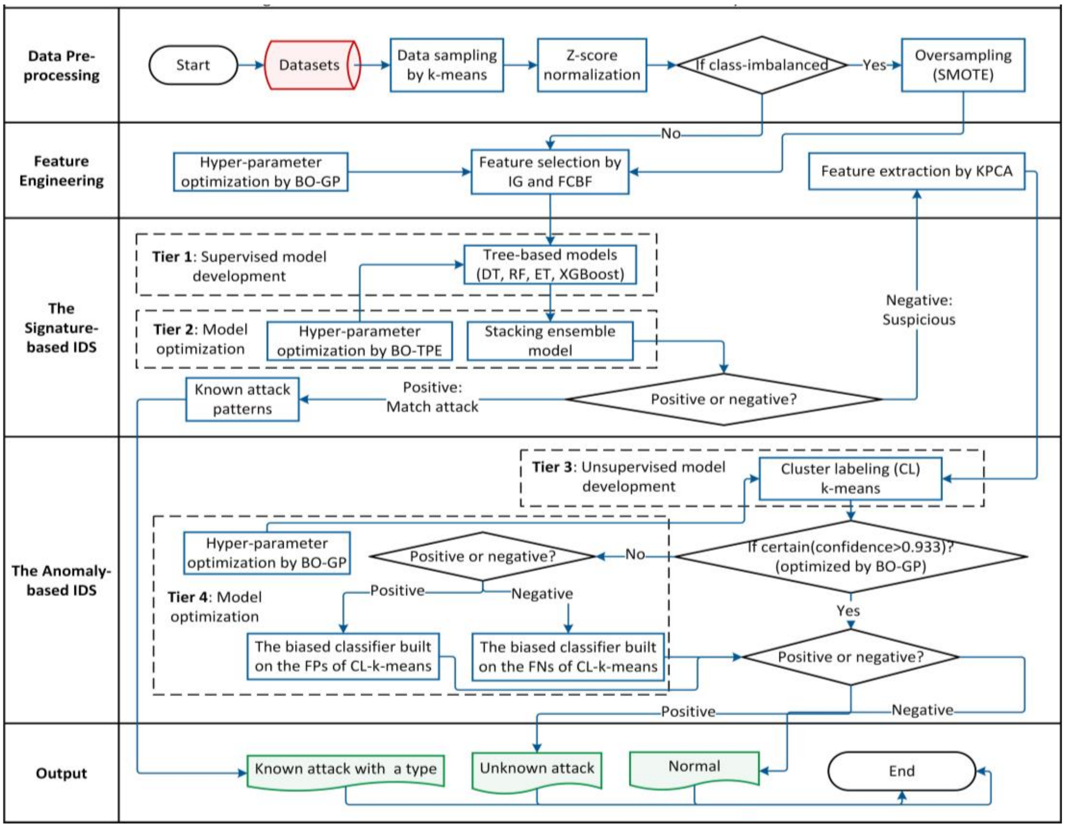

Data Pre-processing
Start
Datasets
Data sampling by k-means
Z-score normalization
If class-imbalanced
Yes
Oversampling (SMOTE)
No
Feature Engineering
Hyper-parameter optimization by BO-GP
Feature selection by IG and FCBF
Feature extraction by KPCA
The Signature-based IDS
Tier 1: Supervised model development
Tree-based models (DT, RF, ET, XGBoost)
Tier 2: Model optimization
Hyper-parameter optimization by BO-TPE
Stacking ensemble model
Negative: Suspicious
Known attack patterns
Positive: Match attack
Positive or negative?
The Anomaly-based IDS
Tier 3: Unsupervised model development
Cluster labeling (CL) k-means
Hyper-parameter optimization by BO-GP
Positive or negative?
No
If certain(confidence>0.933)? (optimized by BO-GP)
Tier 4: Model optimization
Positive
Negative
Yes
The biased classifier built on the FPs of CL-k-means
The biased classifier built on the FNs of CL-k-means
Positive or negative?
Positive
Negative
Output
Known attack with a type
Unknown attack
Normal
End

Fig. 7.1. The framework of the proposed IDS.

7.1. Data Pre-processing

Data Sampling by K-means Clustering:

Due to the massive volume of network traffic data, training machine learning models directly on such large datasets is impractical. To address this, K-means clustering is used for data sampling. This method groups data points into clusters, from which representative samples are drawn, significantly reducing the training complexity while maintaining data representativeness.

Synthetic Minority Over-sampling Technique (SMOTE):

Network traffic data is often imbalanced, with a majority of data points representing normal conditions. SMOTE is applied to create synthetic samples for minority classes, ensuring balanced training data and improving the detection rate of the classifier.

7.2. Feature Engineering

Information Gain (IG):

IG is employed to select the most relevant features by measuring the information each feature contributes to the target variable. Features are ranked based on their IG scores, and those exceeding a set threshold are retained for model training.

Fast Correlation-Based Filter (FCBF):

FCBF is used to remove redundant features by calculating the correlation between features, thereby retaining only those that contribute unique information. This step reduces the risk of overfitting and enhances model performance.

Kernel Principal Component Analysis (KPCA):

KPCA is applied to further reduce the dimensionality of the data by extracting the most relevant features. This step minimizes noise and improves the accuracy of the intrusion detection system.

7. 3. Model Training and Optimization

The IDS uses tree-based algorithms such as Decision Trees (DT), Random Forest (RF) for supervised learning. These algorithms are chosen for their effectiveness in handling complex tabular data, characteristic of vehicular networks.

7.4. Anomaly Detection

Cluster-based Local Outlier Factor (CL-K-means):

For detecting unknown or zero-day attacks, a novel CL-K-means method is implemented. This unsupervised learning technique identifies anomalies by analyzing deviations from normal behavior within clusters.

8. RESULT & ANALYSIS

The proposed Intrusion Detection System (IDS) was evaluated for its effectiveness in detecting both known and unknown cyber-attacks in vehicular networks. The evaluation was conducted using two primary datasets: the CAN-intrusion dataset and the CICIDS2017 dataset. The results of these evaluations are discussed in terms of detection rates (DR), false alarm rates (FAR), F1-scores, and execution times.

8.1. Performance on Known Intrusions

For known intrusions, the IDS was tested on the CAN-intrusion and CICIDS2017 datasets using signature-based machine learning models.

1.CAN-Intrusion Dataset:

The proposed IDS achieved an accuracy of 99.999% an F1-score of 0.99999, demonstrating its high reliability in distinguishing between normal and malicious traffic.

2. CICIDS2017 Dataset:

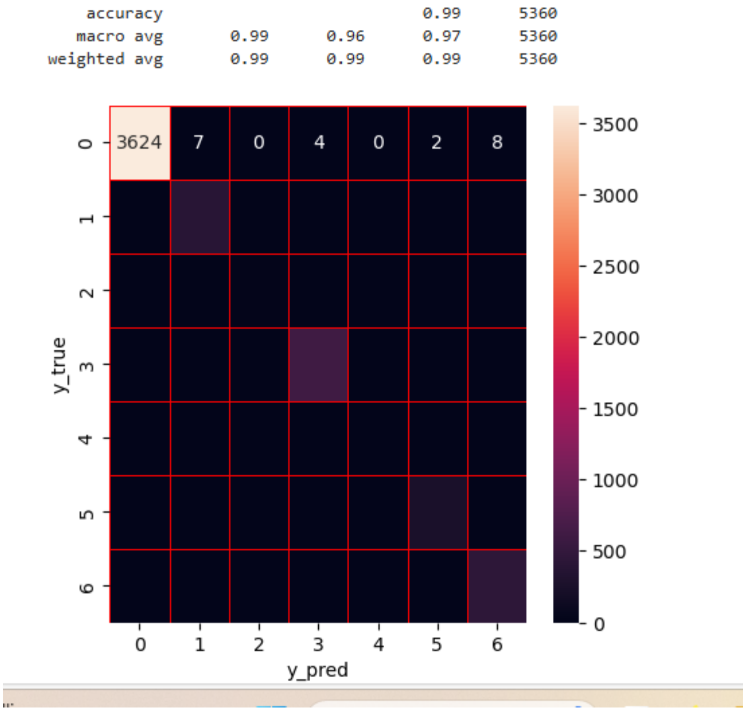
Implementing the proposed IG-FCBF feature selection method and achieved F1-score to 99.879%.

8.2. Performance on Unknown Intrusions

The IDS also evaluated its ability to detect unknown intrusions using anomaly-based detection models. Each type of CAN attack was treated as a new attack type in different experiments.

1. CAN-Intrusion Dataset: The proposed IDS achieved a 100% detection rate for DoS, attacks with high F1-scores close to 1.0.

2. CICIDS2017 Dataset: The IDS demonstrated high detection rates for various attack types, such as "Web Attack – Brute Force" and "Web Attack – Sql Injection," with F1-scores greater than 0.80. The average F1-score for the unknown attacks was 0.80013, indicating a robust detection capability, though improvements are needed for certain attack types.



```
    accuracy                           0.99      5360
   macro avg       0.99      0.96      0.97      5360
weighted avg       0.99      0.99      0.99      5360
```

9. CONCLUSIONS

1. The proposed IDS effectively detects both known and unknown cyber-attacks in vehicular networks.

2. Advanced machine learning techniques and optimization methods ensure high accuracy and low false alarm rates.

3. Evaluations on CAN-intrusion and CICIDS2017 datasets show robust performance across various attack types.

4. The system is a reliable solution for enhancing cybersecurity in modern vehicles.

- Future improvements will focus on better detection of less common attacks and further optimization for real-time deployment.

10. FUTURE SCOPE

The future scope of this research involves enhancing the detection capabilities of the IDS for less common and emerging cyber-attacks by incorporating advanced deep learning techniques and continuously updating the system with new attack signatures. Additionally, optimizing the IDS for deployment in real-time vehicular environments, including integration with onboard vehicle systems and infrastructure, is essential. Further research will also explore the use of distributed and collaborative detection mechanisms to improve the overall security of the Internet of Vehicles (IoV) ecosystem. Expanding the dataset and improving the system's adaptability to different vehicular network configurations will ensure comprehensive and robust protection against evolving cyber threats.

REFERENCES

[1] H. Liang *et al.*, “Network and system level security in connected vehicle applications,” *IEEE/ACM Int. Conf. Comput. Des. Dig. Tech. Pap. ICCAD*, pp. 1–7, 2018.

[2] M. Gmiden, M. H. Gmiden, and H. Trabelsi, “An intrusion detection method for securing in-vehicle CAN bus,” *2016 17th Int. Conf. Sci. Tech. Autom. Control Comput. Eng. STA 2016 - Proc.*, pp. 176–180, 2017.

[3] J. Liu, S. Zhang, W. Sun, and Y. Shi, “In-vehicle network attacks and countermeasures: Challenges and future directions,” *IEEE Netw.*, vol. 31, no. 5, pp. 50–58, 2017.

[4] 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.

[5] L. Yang, ”Comprehensive Visibility Indicator Algorithm for Adaptable Speed Limit Control in Intelligent Transportation Systems”, M.A.Sc. thesis, University of Guelph, 2018.

[6] J. Golson, “Jeep hackers at it again, this time taking control of steering and braking systems,” *The Verge*, Aug. 2016. [Online]. Available: https://www.theverge.com/2016/8/2/12353186/car-hack- jeep-cherokee-vulnerability-miller-valasek. [Accessed: 11-Nov-2020].

[7] L. Yang, A. Moubayed, I. Hamieh, and A. Shami, “Tree-based Intelligent Intrusion Detection System in Internet of Vehicles,” *proc. 2019 IEEE Glob. Commun. Conf.*, pp. 1–6, Hawaii, USA, 2019.

[8] Q. Wang, Y. Qian, Z. Lu, Y. Shoukry, and G. Qu, “A delay based plug-in-monitor for Intrusion Detection in Controller Area Network,” *Proc. 2018 Asian Hardw. Oriented Secur. Trust Symp. AsianHOST 2018*, pp. 86–91, 2019.

[9] E. Seo, H. M. Song, and H. K. Kim, “GIDS: GAN based Intrusion De- tection System for In-Vehicle Network,” *2018 16th Annu. Conf. Privacy, Secur. Trust. PST 2018*, pp. 1–6, 2018.

[10] M. Injadat, A. Moubayed, A. B. Nassif, and A. Shami, “Machine learning towards intelligent systems: applications, challenges, and opportunities,” *Artif. Intell. Rev.*, 2021.

[11] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward generating a new intrusion detection dataset and intrusion traffic characterization,” *in Proc. Int. Conf. Inf. Syst. Secur. Privacy*, 2018, pp. 108–116.