A Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles

Apoorva Mani[1], Aishwarya Virigineni[2], Maturi Tanuj[3], Niranjan D K[4]
Department of Computer Science Engineering
Amrita School of Engineering, Bengaluru
Amrita Vishwa Vidyapeetham, India

[1]bl.en.u4aie19007@bl.students.amrita.edu, [2]bl.en.u4aie19068@bl.students.amrita.edu, [3]bl.en.u4aie19041@bl.students.amrita.edu,
[4]dk_niranjan@blr.amrita.edu

***Abstract*— Modern vehicles, including connected vehicles and autonomous vehicles, nowadays involve many electronic control units connected through intra-vehicle networks to implement various functionalities and perform actions. Modern vehicles are also connected to external networks through vehicle-to-everything technologies, enabling their communications with other vehicles, infrastructures, and smart devices. However, the improving functionality and connectivity of modern vehicles also increase their vulnerabilities to cyber-attacks targeting both intra-vehicle and external networks due to the large attack surfaces. To secure vehicular networks, many researchers have focused on developing intrusion detection systems (IDSs) that capitalize on machine learning methods to detect malicious cyber- attacks. In this paper, the vulnerabilities of intra-vehicle and external networks are discussed, and a multi-tiered hybrid IDS that incorporates a signature-based IDS and an anomaly-based IDS is proposed to detect both known and unknown attacks on external vehicular networks. Experimental results illustrate that the proposed system can detect various types of known attacks with 99.88% accuracy on the CICIDS2017 dataset illustrating the external vehicular network data. For the zero-day attack detection, the proposed system achieves high F1-scores of 0.800. This emphasizes the effectiveness and efficiency of the proposed IDS.**

***Keywords*— Intrusion detection system, Internet of Vehicles, CAN bus, Anomaly detection, Zero-day attacks, Bayesian optimization.**

I. INTRODUCTION

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. 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. IoV consists mainly of intra-vehicle networks (IVNs) and external vehicular networks. IVNs involve an increasing number of electronic control units (ECUs) to adopt various functionalities. All ECUs in a vehicle are connected by a controller area network (CAN) bus to transmit messages and perform actions. 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. 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: 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. 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. 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. Thus, intrusion detection systems (IDSs) have become an essential component in modern IoV to identify malicious threats on vehicular networks. 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.

Machine learning (ML) and data mining algorithms have been recognized as effective models to design IDSs. In this paper, a multi-tiered hybrid intrusion detection system (MTH-IDS) is proposed to efficiently identify known and zero-day cyber-attacks on external networks using multiple ML algorithms. The proposed MTH-IDS framework consists of two traditional ML stages (data pre- processing and feature engineering) and four tiers of learning models. 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 MTH-IDS is evaluated on the CICIDS2017 dataset, representing the external network traffic data. 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 work are as follows:

1) It proposes a novel multi-tiered hybrid IDS that can accurately detect the various surveyed types of cyber- attacks launched on external vehicular networks;

2) It proposes a novel feature engineering model based on information gain (IG), fast correlation-based filter (FCBF), and kernel principal component analysis (KPCA) algorithms;
3) It proposes a novel anomaly-based IDS based on CL-k- means and biased classifiers to detect zero-day attacks;
4) It discusses the use of Bayesian optimization techniques to automatically tune the parameters of each tier in the proposed IDS for model optimization;
5) It evaluates the performance and overall efficiency of the proposed model on the state-of-the-art dataset CICIDS2017, and discusses its feasibility in real-world IoV devices.

II. LITERATURE SURVEY

Although various studies about vehicular network IDS development have been published, most of them are only designed for known attack detection on either intra-vehicle or external networks. Additionally, several papers only consider a specific type of attack, like Botnets or DoS attacks. However, in real-world applications, both intra-vehicle and external networks are vulnerable to various types of attacks with both existing and new patterns. The IDS proposed in is the only research that considers both CAN bus and external networks, and the IDS proposed in is the only technique that can detect both known and unknown attacks. Thus, there still should an IDS designed for the detection of both known and zero-day attacks on both intra-vehicle and external vehicular networks. Our proposed IDS aims to achieve this.

On the other hand, for the deployment of IDSs in real-world vehicle systems, vehicle-level model testing and real-time analysis should be performed to validate the feasibility of the IDSs. However, only five papers vehicle-level testing or real-time analysis, so the feasibility of other techniques in real-world IoVs is not proven. There- fore, our proposed IDS has been evaluated in a vehicle-level machine to verify whether it meets the real-time requirements of vehicular networks. An effective IDS should achieve a high detection rate and a low false alarm rate. Moreover, to meet the real-time requirements of IoV, an IDS should have low computational complexity and high efficiency. Thus, three important procedures, including data sampling, feature engineering, and model optimization, are implemented in our proposed MTH-IDS to improve the efficiency and accuracy of IoV attack detection.

However, only six existing techniques performed feature engineering and only one research work implemented model optimization. The use of efficiency and accuracy enhancement techniques enables our proposed MTH-IDS to outperform most existing research works in terms of detection rate, false alarm rate, and execution speed.

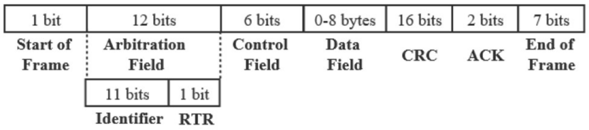

Fig. 1. CAN packet structure.

III. VEHICULAR NETWORKS, VULNERABILITIES, AND IDS DEPLOYMENT

A. Vulnerabilities of Intra-vehicle Networks

Modern vehicles often contain 70-100 ECUs that are in-vehicle components used to enable various functionalities. CAN is a bus communication protocol that defines an international standard for efficient and reliable intra-vehicle communications among ECUs. A CAN-bus is built based on differential signaling and comprises a pair of channels, CAN-High and CAN-Low, representing the two signals, 1 and 0, respectively. CAN is the most common type of IVN due to its low cost and complexity, high reliability, noise- resistance, and fault-tolerance properties. However, CAN is vulnerable to various cyber threats due to its broadcast transmission strategy, lack of authentication and encryption, and unsecured priority scheme.

CAN messages, or packets, are transmitted via CAN-bus. The data frame is the most important type of CAN packet used to transmit user data. Fig. 1 shows the structure of a CAN packet, which consists of seven fields: start of frame, arbitration field, control field, data field, CRC (cyclic redundancy code) field, acknowledge (ACK) field, and end of frame. Among all fields, the data field with the size of 0-8 bytes is the most important and vulnerable one, since it contains the actual transmitted data that determines the node actions. An attacker can intrude or take control of a vehicle by injecting malicious messages into the data field of CAN packets, resulting in compromised nodes or vehicles; so-called message injection attacks.

Message injection attacks are the primary type of intra-vehicle attack and can be further classified as DoS attacks, fuzzy attacks, and spoofing attacks by their objectives. In DoS attacks, a CAN is flooded with massive high-priority messages to cause latencies or unavailability of other legitimate messages. Similarly, fuzzy attacks can be launched by injecting arbitrary messages with randomly spoofed identifiers or packets, causing compromised vehicles to exhibit unintended behaviors, like sudden braking or gear shift changes. Spoofing or impersonation attacks, such as gear spoofing and revolutions per minute (RPM) spoofing attacks, are launched by injecting messages with certain CAN identifiers (IDs) to masquerade as legitimate users and take control of the vehicles.

A. Vulnerabilities of External Vehicular Networks

In a similar fashion, V2X technology enables interactions and communications between vehicles and other IoV entities, including pedestrians, infrastructures, smart devices, and network systems. With the increasing connectivity ofmodern IoV, external vehicular networks are becoming large networks that involve various other networks and devices. Thus, external vehicular networks are vulnerable to various general cyber threats because each vehicle or device is apotential entry point for intrusions. Typical attacks in IoV include DoS, GPS spoofing, jamming, sniffing, brute-force, Botnets, infiltration, and web attacks. The description and IoV scenarios of these common external vehicular network attacks are summarized in Table II.

Paper	In-vehicle Network Attack Detection	External Network Attack Detection	Multiple Types of Known Attack Detection	Zero-Day Attack Detection	Vehicle-Level Model Testing or Real-time Analysis	Data Pre-Processing and Sampling	Feature Engineering	Model Optimization
Alshammari *et al.* [12]	✓		✓				✓	
Barletta *et al.* [13]	✓		✓					
Olufowobi *et al.* [14]	✓		✓		✓			
Olufowobi *et al.*[15]	✓		✓					
Lee *et al.* [16]	✓		✓		✓			
Lokman *et al.* [17]	✓		✓					
Song *et al.* [18]	✓		✓		✓			
Ashraf *et al.* [19]	✓	✓	✓				✓	
Alheeti *et al.* [20]		✓		✓			✓	
Rosay *et al.* [21]		✓	✓		✓		✓	
Aswal *et al.* [22]		✓					✓	
Aloqaily *et al.* [23]		✓	✓		✓			
Gao *et al.* [24]		✓						
Schmidt *et al.* [25]		✓	✓					
Min *et al.* [26]		✓	✓					
Yao *et al.* [27]		✓	✓					
Injadat *et al.* [28]		✓	✓				✓	✓
Proposed MTH-IDS	✓	✓	✓	✓	✓	✓	✓	✓

TABLE I. COMPARISON OF RECENT INTRUSION DETECTION TECHNIQUES FOR IOVS

TABLE II
COMMON ATTACK TYPES ON EXTERNAL VEHICULAR NETWORKS

Attack Type	Description and IoV Scenarios
DoS	Send a large number of requests to exhaust the compromised nodes' resources, causing vehicle unavailability or accidents.
GPS Spoofing	Masquerade as authorized IoV users to provide a node with false information, like false geographic information, therefore causing fake evidence, event delay, or property losses.
Jamming	Jam signals to prevent legitimate IoV devices from communicating with connected vehicles.
Sniffing	Capture vehicular network packets to steal confidential or sensitive information of vehicles, users, or enterprises.
Brute-force	Crack passwords in vehicle systems to take control of vehicles or machines and perform malicious actions.
Botnets	Infect multiple connected vehicles and IoV devices with Bot viruses to breach them and launch other attacks.
Infiltration	Traverse the compromised vehicle systems and create a backdoor for future attacks.
Web Attack	Hack IoV servers or web interfaces of connected vehicles to gain confidential information or perform malicious actions.

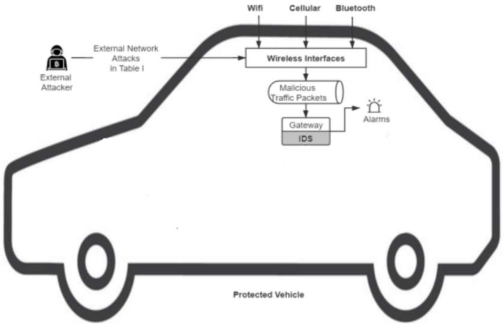

Fig. 2. The proposed IDS-protected vehicle architecture.

IV. PROPOSED MTH-IDS FRAMEWORK

A. *System Architecture*

The purpose of this work is to develop an IDS that can protect external networks from being breached by the various common attacks. In this paper, a novel multi-tiered hybrid IDS is proposed to detect both known and unknown cyber-attacks on vehicular networks with optimal performance. Fig. 3 demonstrates the architecture of the proposed system, comprising four main stages: data pre-processing, feature engineering, a signature-based IDS, and an anomaly-based IDS.

Firstly, external network traffic dataset is collected for the purpose of system performance evaluation on external vehicular networks. Data pre-processing consists of a k-means-based cluster sampling method used to generate a highly-representative subset, and a SMOTE method used to avoid class-imbalance. In the feature engineering process, the datasets are processed by information- gain-based and correlation-based feature selection methods to remove irrelevant and redundant features, and then passed to the KPCA model to further reduce dimensionality and noisy features. The proposed data pre-processing and feature engineering procedures can greatly improve the quality of the network data for more accurate model learning. The signature-based IDS is then developed to detect known attacks by training four tree-based machine learners as the first tier of the proposed MTH-IDS: DT, RF, ET, XGBoost. In the second tier, a stacking ensemble model and the BO-TPE method are used to further improve the intrusion detection accuracy by combining the output of the four base learners from the first tier and optimizing the learners. In the next stage, an anomaly-based IDS is constructed to detect unknown attacks. In the anomaly-based IDS, the suspicious instances are passed to a cluster-labeling (CL) k-means model as the third tier to effectively separate attack samples from normal samples. The fourth tier of the MTH-IDS comprises the BO-GP method and two biased classifiers used to optimize the model and reduce the classification errors of the CL-k-means. Ultimately, the detection result of each test sample is returned, which could be a known attack with its type, an unknown attack, or a normal packet. To summarize the rationale behind the algorithms used in the proposed IDS, the brief description and performance impact of each algorithm are presented in Table III.

B. *Data Pre-processing*

1) *Data Sampling by K-means Clustering:* In real life, training ML models on massive amounts of network traffic data is unrealistic and may cost a massive amount of time, especially in the hyper-parameter tuning process that needs to train a ML model multiple times. For model training efficiency improvement purposes, data sampling is a common technique that can generate a subset of the original data to reduce the training complexity of a model.

2) In the proposed system, to obtain a highly-representative subset, a k-means-based cluster sampling method is utilized. Cluster sampling is a common data sampling method by which the original data points are grouped into multiple clusters; then, a proportion of data is sampled from each cluster to form a representative subset. Unlike random sampling, which randomly selects every data sample with an equal probability, cluster sampling can generate a highly-representative subset because the discarded data points are mostly redundant data. Among all clustering algorithms, k-means is the most common one for data sampling due to its simple implementation and low computational complexity.

3) *Reduce Class-Imbalance by Oversampling*: Class-imbalance issues often occur in network traffic data, since the percentage of normal samples is often much larger than the percentage of attack samples in real-world network data, resulting in biased models and low detection rate. Class-imbalance problems are mainly solved by resampling methods, including random sampling and synthetic minority oversampling techniques (SMOTE), which can create new instances for the minority classes to balance the dataset. Unlike random sampling, which simply replicates the instances and may cause over-fitting, SMOTE can synthesize high quality instances based on the concept of KNN; thus, SMOTE is chosen in the proposed IDS to solve class-imbalance.

4) *Data Normalization*: After implementing the k-means and SMOTE methods to obtain a representative and balanced dataset, several additional data pre-processing steps are completed for the next steps. Firstly, the network traffic datasets are encoded with a label encoder used to transform categorical features into numerical features to support the inputs of ML algorithms, because many ML algorithms cannot support string features directly. After that, the network datasets are normalized by the Z-score algorithm since the collected features in network traffic data often have largely different ranges, and ML models often perform better on normalized datasets. An unnormalized dataset with largely different feature scales may result in a biased ML model that only lays emphasis on large-scale features. Through the Z-score method, the features can be normalized to have a mean of 0 and a standard deviation os. Through the Z-score method, the features can be normalized to have a mean of 0 and a standard deviation of 1.

C. *Feature Engineering*

A high-quality and highly representative dataset can be generated after data pre-processing. On the other hand, obtaining an optimal feature list by appropriate feature engineering can also improve the quality of datasets for more accurate and efficient model learning. A comprehensive feature engineering method that consists of IG, FCBF, and KPCA, is implemented before ML model

D. *Feature Engineering*

A high-quality and highly representative dataset can be generated after data pre-processing. On the other hand, obtaining an optimal feature list by appropriate feature engineering can also improve the quality of datasets for more accurate and efficient model learning. A comprehensive feature engineering method that consists of IG, FCBF, and KPCA, is implemented before ML model training to remove irrelevant, redundant, and noisy features while retaining the important features.

1)*Feature Selection by Information Gain:*

As a common feature selection (FS) method, the information gain (IG) method is used to select important features. IG, the amount of information gained or the changes in entropy,

TABLE III: RATIONALE AND PERFORMANCE IMPACT OF EACH COMPONENT OF THE MTH-IDS

Stage	**Algorithm**	**Rationale and Description**	**Performance Impact**
Data pre-processing	K-means cluster sampling	Network traffic data is often large, while IoV devices often have limited computational power and resources. The k-means sampling method can generate highly representative subsets for more efficient training because the removed data is mostly redundant data.	Improve model training efficiency.
	SMOTE	Network traffic data is often imbalanced data because most data samples are collected under normal conditions in real-world vehicle systems. SMOTE can create high-quality samples for minority classes to avoid class-imbalance and ineffective classifiers.	Improve detection rate.
	Z-score	Different features often have different ranges, which can bias the model training. The Z-score method can normalize features to a similar scale and handle outliers.	Improve model accuracy and training efficiency.
Feature engineering	IG	For certain tasks like intrusion detection, many collected features can be irrelevant, causing additional training time. The IG method can remove those unimportant features.	Improve model training efficiency.
	FCBF	Certain features are redundant because they contain very similar information. FCBF can remove redundant features by calculating the correlation between each pair of features.	Improve model accuracy and training efficiency.
	KPCA	The anomaly-based IDSs are sensitive to the quality of features. KPCA can further extract the most relevant features to reduce dimensionality and noisy information.	Improve model accuracy and training efficiency.
The signature-based IDS	DT, RF, ET, and XGBoost	Tree-based ML algorithms often perform better than other ML algorithms on complex tabular data to which IoV data belong. Four tree-based supervised algorithms are used to train base classifiers for known intrusion detection.	Detect various types of known attacks.
	BO-TPE	The default hyper-parameters of ML algorithms often cannot return the best model. BO-TPE can optimize the models' hyper-parameters to obtain the optimized base classifiers.	Improve accuracy of known attack detection.
	Stacking	Ensemble models can often achieve higher accuracy than any single model. Stacking ensemble can combine the base classifiers to obtain a meta-learner with better performance.	Improve accuracy of known attack detection.
The anomaly-based IDS	CL-k-means	For unknown attack detection, CL-k-means can generate a sufficient number of normal and attack clusters to identify zero-day attacks from the newly arriving data.	Detect unknown attacks.
	BO-GP	CL-k-means has an important hyper-parameter, the number of clusters, *k*. BO-GP is an effective HPO method to optimize *k* and obtain the optimized CL-k-means model.	Improve accuracy of unknown attack detection.
	Two biased classifiers	CL-k-means may return many errors when detecting complex unknown attacks. Two biased classifiers are trained on the FPs and FNs of CL-k-means to reduce the errors.	Improve accuracy of unknown attack detection.

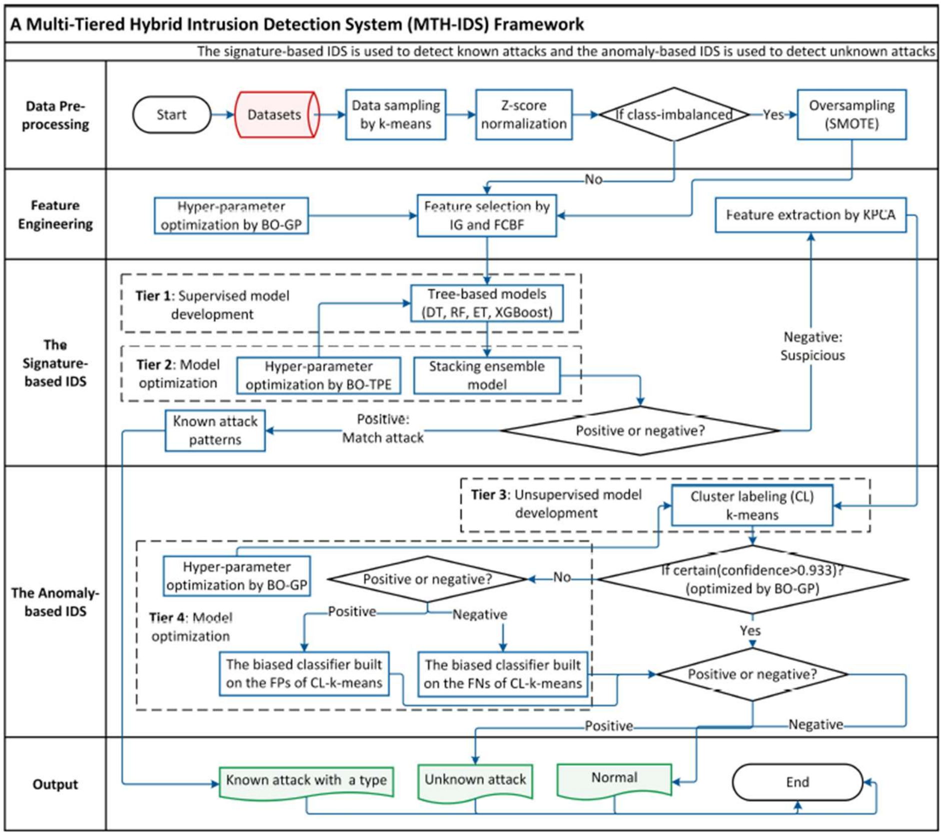
A Multi-Tiered Hybrid Intrusion Detection System (MTH-IDS) Framework
The signature-based IDS is used to detect known attacks and the anomaly-based IDS is used to detect unknown attacks
Data Pre-processing
Start
Datasets
Data sampling by k-means
Z-score normalization
If class-imbalanced
Yes
Oversampling (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. 3. The framework of the proposed MTH-IDS.

can be used to measure how much information a feature can bring to the targeted variable. IG is chosen in the proposed system since it can obtain an importance score for each feature at a fast speed due to its low computational complexity of O(n).

2) *Fast Correlation Based Filter (FCBF):* Although the IG-based FS method eliminates the unimportant features to reduce time complexity, many redundant features still exist. Among the correlation-based FS algorithms, the fast correlation-based filter (FCBF) algorithm is selected since it has shown great performance on high dimensional datasets by effectively removing redundant features while retaining important features, and has a low time complexity of O(log n).

3) *Kernel Principal Component Analysis (KPCA):* Although utilizing IG-FCBF can return a better feature set than only using IG, FCBF has a major limitation that it only calculates the correlation between pairs of features, but does not consider correlations among three or more different features, resulting in undiscovered noisy features. On the other hand, the unsupervised learning models in the anomaly-based IDS are more sensitive to appropriate features than supervised learning models since they rely on the changes of feature values instead of the ground truth labels to process data. Hence, kernel principal component analysis (KPCA) is utilized after implementing the IG-FCBF method for the anomaly-based IDS.

V. Proposed hybrid IDS

IDSs are mainly classified as signature-based IDSs and anomaly-based IDSs. Signature-based IDSs are designed to detect the known attack patterns by training supervised ML models on labeled datasets. However, they often lack the capacity to detect new attack patterns that are not previously stored in the databases. On the other hand, anomaly-based IDSs can distinguish unknown attack data from normal data by unsupervised learning algorithms based on the assumption that new attack data are more statistically similar to the known attack data than normal data, but they often return many false alarms. Thus, a hybrid IDS that consists of a signature- based IDS and an anomaly-based IDS is proposed in this paper to effectively detect both known and zero-day attacks.

1) *The Signature-based IDS:* After the data pre-processing and feature engineering procedures, the obtained labeled datasets are trained by an ensemble learning model to develop a signature-based IDS. In the proposed signature-based IDS, four tree-based ML algorithms — decision tree (DT), random forest (RF), extra trees (ET), and extreme gradient boosting (XGBoost) — are selected as the base learners. DT is a common ML algorithm that uses a tree- structure to fit data and make predictions. DT algorithms have multiple hyper-parameters that require tuning, including
2) *The Anomaly-based IDS:* The proposed signature-based IDS can detect multiple types of known attacks effectively. However, attackers can still carry out zero-day attacks that are not included in the known attack patterns and can be misclassified as normal states. Therefore, the instances labelled “normal” by the signature-based IDS will be considered suspicious instances because some of them can be unknown attack

samples. A novel anomaly-based IDS architecture is then developed to identify zero-day attacks by processing the suspicious instances. After feature engineering, the optimized dataset obtained from the output of the IG-FCBF-KPCA method is used to trainthe anomaly-based IDS. The first tier of the proposed anomaly-based IDS comprises the cluster labeling (CL) k-means developed by improving the k-means model.

VI. Performance Evaluation

A. Experimental Setup

The experiments are divided into two parts, one for the known intrusion detection by evaluating the signature-based IDS component on the labeled datasets and one for unknown intrusion detection by evaluating the anomaly-based IDS component on the unlabeled datasets.

B. Data Description

For external network IDS development, there is a shortage of public IoV benchmark datasets due to popularization, privacy, and commercialization issues. Among the various cyber-security datasets, CICIDS2017 is the most representative dataset of current external networks because it is the most state-of-the-art dataset and contains more features, instances, and cyber-attack types than other datasets. Thus, the network traffic flow data in the CICIDS2017 dataset is chosen in the proposed MTH-IDS to represent the complex external vehicular network data.

Moreover, to better relate the CICIDS2017 dataset to IoV applications, we have associated each type of attack in the CICIDS2017 dataset with the external vehicular network threats described in Table II based on the detailed analysis of the CICIDS2017 dataset. The specifics of the CICIDS2017 dataset and the corresponding external vehicular attack types are shown in Table V. Since the Bot, brute-force, infiltration, and web attack classes are minority classes with small numbers of samples (from 36 to 13,835), the SMOTE method described was implemented to synthesize more samples to enable the minority classes to have at least 100,000 samples. Addressing class-imbalance can avoid obtaining biased models with low attack detection rates.

TABLE III
Class Label, Attack Type, and Size of The CICIDS2017 Dataset

Class Label	**Corresponding Attack Type in Table II [78]**	**Original Number of Samples**	**Number of Training Set Samples After Balancing**	**Number of Test Set Samples**
BENIGN	-	2,273,097	1,591,168	681,929
Bot	Botnets	1,966	100,000	590
DDoS	DoS	380,699	266,489	114,210
DoS GoldenEye				
DoS Hulk				
DoS Slow-httptest				
DoS Slowloris				
Heartbleed				
Port-Scan	Sniffing	158,930	111,251	47,679
SSH-Patator	Brute-Force	13,835	100,000	4,150
FTP-Patator				
Infiltration	Infiltration	36	100,000	11
Web Attack – Brute Force	Web Attack	2,180	100,000	654
Web Attack – Sql Injection				
Web Attack – XSS				

C. Performance Analysis of Known Intrusion Detection

The experimental results on the CICIDS2017 dataset are shown in Table IV. By implementing the proposed IG-FCBF method with the optimized correlation threshold (alpha = 0:9) to select 20 features from 80 original features and using HPO methods to obtain optimized ML models, the F1-score of the proposed IDS has improved from 99.861% to 99.879%, and the execution time has decreased by 70.2%, as shown in Table IV. This justifies the proposed FS method and the BO- TPE method can greatly improve the system efficiency and slightly improve the model accuracy. In addition to the multi-classification results used to evaluate the IDS's capacity to detect various types of attacks, the IDS is also implemented to train a binary classification model that can distinguish between normal and abnormal network traffic data and return one of these two labels. As shown in Table IV the proposed IDS reaches 99.895% accuracy and saves 69.4% of the execution time by training the binary classification model. Binary classifiers and multi-classifiers can be chosen according to the specific needs of users.

Therefore, the experimental results show that the proposed IDS can efficiently separate normal and malicious network traffic data and effectively detect various types of known cyber-attacks in vehicle systems.

TABLE IV
Performance Evaluation of Classifiers on The CICIDS2017 Dataset

Method	**Acc (%)**	**DR (%)**	**FAR (%)**	**F1**	**Execution Time (S)**
MTH-IDS (Without FS & HPO)	99.861	99.753	0.110	0.99860	5238.4
MTH-IDS (Multi-Class Model)	**99.879**	**99.818**	**0.101**	**0.99879**	**1563.4**
MTH-IDS (Binary Model)	**99.895**	**99.806**	**0.084**	**0.99895**	**478.2**

D. Performance Analysis of Unknown Intrusion Detection

At this stage, all the models in the anomaly-based IDS are trained for binary classification by labeling the instances of all attack types as "attack" and normal instances as "normal". In the proposed system, after being evaluated by the signature-based IDS, all data samples of known attack types will be returned, and other normal instances will be labeled "suspicious" and passed to the anomaly-based IDS to determine whether any unknown attacks exist.

Several experiments were conducted on the CICIDS2017 dataset that contains data samples of 14 different common cyber-attacks types to illustrate potential attacks launched on external vehicular networks. In each experiment of the validation process, each type of attack is regarded as an unknown attack, and the results are shown in Table IX.

From Table V, it can be seen that the proposed system exhibits different performances when applied to the experiments of different types of unknown attacks. By implementing the proposed methods, the false alarm rates for most of the attack types are at a low level of less than 20%. The detection rates for the "Heartbleed", "Port-Scan", "SSH-Patator", "Web Attack – Brute Force", and "Web Attack – Sql Injection" attacks are high (from 89.516% to 100%), while the detection rates for other types of attacks are relatively lower (from 51.298% to 83.931%). The F1-scores for most of the attack types are larger than 0.80. The only type of attack that the proposed system cannot detect effectively is the "Web Attack – XSS" whose results show a very low F1-score (0.062), because their data distribution is very similar to normal data distributions. The average F1-score of the proposed MTH-IDS on all the attacks is 0.80013, which is higher than the CL-k- means model without biased classifiers (0.77305).

Thus, the proposed IDS can detect most of the previously-unseen types of attacks with a relatively high detection rate and a relatively low false alarm rate. Nevertheless, there is still some room for improvement since effectively detecting zero- day attacks is still an unsolved research problem.

TABLE V
PERFORMANCE EVALUATION ON EACH TYPE OF UNKNOWN ATTACK OF
THE CICIDS2017 DATASET

Attack Type	Validation Instances	DR (%)	FAR (%)	F1
Bot	3,932	63.276	21.669	0.68426
DDoS	256,054	62.697	11.698	0.71902
DoS GoldenEye	20,586	83.931	20.461	0.82127
DoS Hulk	462,146	67.440	11.806	0.75248
DoS Slow-httptest	10,998	76.687	19.094	0.78339
DoS Slowloris	11,592	83.834	7.902	0.87447
FTP-Patator	15,876	51.298	12.686	0.62564
Heartbleed	22	100.0	18.182	0.91667
Infiltration	72	72.222	5.556	0.81250
Port-Scan	317,860	98.962	17.849	0.91288
SSH-Patator	11,794	95.828	23.351	0.87443
Web Attack – Brute Force	3,014	89.516	17.319	0.86558
Web Attack – Sql Injection	42	95.238	23.810	0.86957
Web Attack – XSS	1,304	3.681	14.417	0.06233
Average (MTH-IDS)	**1,115,292**	**75.943**	**13.882**	**0.80013**
Average (CL-k-means)	1,115,292	72.682	15.357	0.77305

The experimental results on the test sets are shown in Table VI. As shown in Table VI, the F1-scores of the proposed IDS on the 30% test sets of the CICIDS2017 dataset is 99.88%. Moreover, the confusion matrices of evaluating the proposed method on the test sets of the CAN-intrusion-dataset and CICIDS2017 dataset are shown in Fig. 3

TABLE VI
PERFORMANCE EVALUATION ON THE UNTOUCHED TEST SET

Dataset	Acc (%)	DR (%)	FAR (%)	F1
CICIDS2017	99.88	99.77	0.10	0.9988

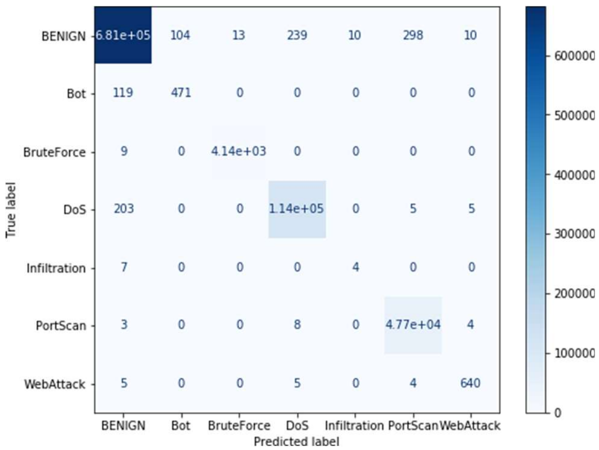

Fig. 3. Confusion matrix for the test set of CICIDS2017 dataset.

VII. CONCLUSION

To enhance IoV security, this work proposed a multi-tiered hybrid intrusion detection system (MTH-IDS) model that can detect various types of known and zero-day cyber-attacks on external-vehicular networks for modern vehicles. The proposed MTH-IDS consists of two traditional ML stages (data pre-processing and feature engineering) and four main tiers of learners utilizing multiple machine learning algorithms. Through data pre-processing and feature engineering, the quality of the input data can be significantly improved for more accurate model learning. The first tier of the proposed system consists of four tree-based supervised learners used for known attack detection, while the second tier comprises the BO-TPE and stacking models for supervised base learner optimization to achieve higher accuracy. The third tier consists of a novel CL-k-means unsupervised model used for unknown/zero-day attack detection. Lastly, BO-GP and two biased classifiers are used to construct the fourth tier for unsupervised learner optimization. The four tiers of learning models enable the proposed MTH-IDS to achieve optimal performance for both known and unknown attack detection in vehicular networks.

Through the performance evaluation of the proposed IDS on the public dataset that represent external vehicular network data, the proposed system can effectively detect various types of known attacks with accuracy of 99.88% on the CICIDS2017 dataset. Moreover, the proposed system can detect various types of unknown attacks with average F1-scores of 0.800 on the CICIDS2017 dataset. The experimental results on a vehicle-level machine also show the feasibility of the proposed system in real-time environments. In future work, the proposed anomaly-based IDS framework can be further improved by doing research on other unsupervised learning and online learning methods.

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 Detection 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 oppor- tunities," *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.

[12] A. Alshammari, M. A. Zohdy, D. Debnath, and G. Corser, "Classifica- tion Approach for Intrusion Detection in Vehicle Systems," *Wirel. Eng. Technol.*, vol. 09, no. 04, pp. 79–94, 2018.

[13] V. S. Barletta, D. Caivano, A. Nannavecchia, and M. Scalera, "A Kohonen SOM Architecture for Intrusion Detection on In-Vehicle Com- munication Networks," *Appl. Sci.*, vol. 10, no. 15, 2020.

[14] H. Olufowobi, C. Young, J. Zambreno, and G. Bloom, "SAIDuCANT: Specification-Based Automotive Intrusion Detection Using Controller Area Network (CAN) Timing," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 1484–1494, 2020.

[15] H. Olufowobi et al., "Anomaly Detection Approach Using Adaptive Cumulative Sum Algorithm for Controller Area Network," *AutoSec 2019 - Proc. ACM Work. Automot. Cybersecurity, co-located with CODASPY 2019*, pp. 25–30, 2019.

[16] H. Lee, S. H. Jeong, and H. K. Kim, "OTIDS: A novel intrusion detection system for in-vehicle network by using remote frame," *Proc. - 2017 15th Annu. Conf. Privacy, Secur. Trust. PST 2017*, pp. 57–66, 2018.

[17] S. F. Lokman *et al.*, "Stacked Sparse Autoencoders-Based Outlier Discovery for In-Vehicle Controller Area Network (CAN)," *Int. J. Eng. Technol.*, vol. 7, no. 4.33, pp. 375-380, 2018.

[18] H. M. Song, J. Woo, and H. K. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," *Veh. Commun.*, vol. 21, p. 100198, 2020.