SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Intelligent Hybrid Machine Learning-Based Cyber Threat Detection and Network Performance Optimization Framework for Vehicular Ad Hoc Networks

Nazish Khan[1], Rahul Khokale[2], Mohammad Sharfoddin Khatib[3]

[1]Department of Computer Science & Engineering, G H Raisoni University, Saikheda, MP, India. E-mail: nazish.khan.cse@ghru.edu.in
[2] Department of Computer Science & Engineering, G H Raisoni University, Saikheda, MP, India. E-mail: rahul.khokale@ghru.edu.in
[3]Department of Computer Science & Engineering, Anjuman College of Engineering and Technology, MH, India.
E-mail: mskhatib@anjumanengg.edu.in

Abstract
The advent of Vehicular Ad Hoc Networks (VANETs) has enabled real-time communication between vehicles and the infrastructure on the road and has made it a crucial part of the intelligent transportation system. The special topology, mobility and diverse communication landscape, however, makes VANETs vulnerable to advanced cyber attacks which have the potential to severely impact network reliability, security and communication efficiency. For secure and efficient vehicular communication, this study presents an Intelligent Hybrid Machine Learning-Based Cyber Threat Detection and Network Performance Optimization Framework, which combines Deep feature Extraction, Ensemble learning, Anomaly Detection, and Adaptive network optimization. The framework utilizes extensive data pre-processing, intelligent intrusion detection and multi-class cyber threat classification to accurately detect malicious activity and dynamically optimize routing and communication performance. The proposed framework is an intelligent and adaptive cybersecurity solution that is scalable and usable for improving network performance and the detection capability for threats, making it an ideal solution for next generation intelligent transportation systems.

Keywords: Vehicular Ad Hoc Networks (VANETs), Cyber Threat Detection, Hybrid Machine Learning, Intrusion Detection System, Anomaly Detection, Network Performance Optimization.

I. Introduction

Vehicular Ad hoc Networks (VANETs) have become an important paradigm for communication in Intelligent Transport Systems (ITS), allowing for the exchange of information in real-time among vehicles, Road Side Units (RSUs) and traffic management infrastructure. VANETs enable many applications such as collision avoidance, traffic congestion management, route optimization, emergency response, autonomous driving and smart city transportation. Besides the fact that connected and autonomous vehicles are deployed in a very fast pace, the demand for secure, reliable and low latency communication networks that can support critical safety services has grown significantly [1]. The topology of VANETs is however highly dynamic, networks frequently disconnect, communication density varies, and there is a decentralized architecture, which poses significant challenges in order to ensure secure and efficient network operations. Although many technologies have been developed for vehicular network communications, VANETs are still highly exposed to a myriad of cyber attacks due to their open wireless communication environment and distributed architecture [2]. Denial-of-service (DoS), distributed Denial-of-Service (DDoS), blackhole attacks, wormhole attacks, Sybil attacks, spoofing, message tampering and false data injection can have a significant impact on the reliability of communications and on the safety of the vehicles. These attacks can diminish the performance of packet delivery and increase communication delay as well as compromise the integrity, authenticity and availability of important vehicular information. Thus, the creation of intelligent cybersecurity solutions that are capable of detecting and countering new attacks, while maintaining network performance, has become a critical research goal [3]. The traditional security measures like rule based intrusion detection systems, cryptographic protocols and signature based detection are not much effective against sophisticated and new cyberattacks. They rely on pre-defined attack signatures which means that they are ineffective in detecting zero-day attacks and adaptive attack behaviors that are frequently used in today's vehicular environment. Moreover, traditional machine learning algorithms fail to scale well in the case of the highly imbalanced network data, nonlinear traffic patterns, and dynamic network conditions, which results in more alarm rates and lower detection accuracy [4]. Hence, there is a

need to deploy more adaptive, intelligent and data-driven solutions to provide a more robust cybersecurity in future vehicular communication systems.

Recent breakthroughs in Artificial Intelligence and Machine Learning (AI/ML) highlight promising opportunities for AI/ML to improve intrusion detection by using automatic feature learning, anomaly detection and predictive threat analysis. Multi-modality learning paradigms can be combined to take advantage of complementary strengths in various feature extraction, classification and adaptive decision making tasks, in hybrid machine learning frameworks. These can help to improve the generalization, increase detection accuracy, decrease false alarms and increase the speed of responding to new threats, along with optimizing the network for the purposes of maximizing packet delivery ratio, minimizing communication delay, routing overhead and maximizing throughput under dynamic traffic conditions [5].

The Research in this paper aims to address these challenges with an Intelligent Hybrid Machine Learning-Based Cyber Threat Detection and Network Performance Optimization Framework for Vehicular Ad Hoc Networks (VANETs). The proposed framework include the intelligent data preprocessing, hybrid intrusion detection system based on machine learning, adaptive anomaly classification and network performance optimization in the single architecture [6]. The framework keeps a track of the traffic on the network, identifies discriminative features, detects malicious activities in real-time, and dynamically optimizes the communication performance using intelligent decision making mechanisms.

II. Related Work

In recent years, Vehicular Ad Hoc Networks (VANETs) have been the subjects of many studies with the aim of enhancing cybersecurity by adopting machine learning and deep learning methods. The traditional IDSs are mainly based on signature-based methods and used known classifiers like Decision Trees, Support Vector Machines and Random Forests to detect known attacks, such as Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS) and Probe [7]. These methods were able to give satisfactory performance for the predefined attack patterns, but they had poor adaptability to previously unseen attack patterns and highly dynamic vehicular environments. To address these issues, researchers presented deep learning architectures such as Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, Autoencoders and hybrid CNN-LSTM architectures that enhanced the feature extraction and intrusion detection performances [8]. More recently, ensemble learning, federated learning, reinforcement learning and explainable artificial intelligence have been explored to improve the robustness of detection, preservation of privacy and transparency of decisions [9].

However, there are a number of issues about which more research needs to be done. The existing studies have focused mainly on cyber threat detection but neglected to consider other network performance metrics like packet delivery ratio, throughput, communication delay, routing overhead, and communication reliability. Likewise, the routing optimization methods typically target optimizing communication efficiency only and do not offer high level of security from cyberattacks [10]. Current systems also have high computational complexity, a high number of false-positive rates, low scalability in high-density environments and poor adaptability to new attack techniques. In addition, few existing solutions have investigated the use of automated response mechanisms and intelligent anomaly classification. To overcome these research challenges, the Intelligent Hybrid Machine Learning Based Cyber Threat Detection and Network Performance Optimization Framework is proposed, which combines the capabilities of deep feature learning, ensemble classification, adaptive anomaly detection, intelligent routing optimization and automatic decision making, and runs them within a single framework [11]. The proposed framework improves the network performance by adapting the routing policies dynamically, is capable of detecting multiple cyber threats, isolates malicious nodes, and updates routing policies dynamically while existing methods do not do all these things. In Table 1, existing VANET security methods are compared and strengths and weaknesses are highlighted as well as gaps in research. The integration approach brings together the advantages of more precise detection accuracy, reliable communication, scalability and resilience, achieving a more complete solution in the area of cybersecurity for next-generation intelligent transportation systems and very dynamic VANET environments.

Table 1. Analysis of Machine Learning-Based Cyber Threat Detection and Network Performance Optimization in VANETs

Method/Approach	Dataset	Cyber Threats Considered	ML/DL Technique	Limitations
Signature-Based IDS [13]	NSL-KDD	DoS, Probe	Decision Tree	Unable to detect unknown attacks
Deep Intrusion Detection [14, 15]	CICIDS2017	DoS, DDoS, Botnet	CNN	High computational complexity

Ensemble Learning IDS [16]	CICIDS2017	DDoS, Brute Force	Random Forest + XGBoost	Sensitive to imbalanced data
Secure VANET Routing [17]	VANET Simulation	Blackhole, Wormhole	Support Vector Machine	Poor scalability
Deep Hybrid IDS [18]	CSE-CIC-IDS2018	DoS, DDoS, Infiltration	CNN-LSTM	High training time
Intelligent Anomaly Detection [19]	CICIDS2017	Sybil, Spoofing	Autoencoder	Increased false positives
Federated IDS [20]	ToN-IoT	Multiple Cyber Attacks	Federated Learning	Large communication overhead
Explainable Intrusion Detection	CICIDS2017	Multi-class Attacks	XGBoost + SHAP	Computational overhead
Reinforcement Learning Routing [21]	SUMO-NS3	Blackhole, DoS	Deep Q-Network	Slow convergence
Hybrid Deep Learning Framework	CSE-CIC-IDS2018	Multi-class Attacks	CNN-BiLSTM	High inference latency
Edge-Assisted Secure VANET [22, 23]	CICIDS2017	DDoS, Spoofing	GRU + Attention	Limited scalability under dense traffic

III. System Model and Problem Formulation

In this section, the architecture of the VANET system, the cyber threat model, the communication performance metrics and the formulated problem are presented. It sets the operational context, introduces the key cybersecurity problems and lays the foundations for the mathematical development of an intelligent hybrid machine learning framework which can improve both intrusion detection and network performance optimization.

A. Vehicular Ad Hoc Network Architecture

The proposed architecture of Vehicular Ad Hoc Network (VANET) comprises connected vehicles, Roadside Units (RSUs), edge servers and centralized traffic management center, which work together to enable secure and intelligent vehicular communication. An On-Board Unit (OBU), Global Positioning System (GPS), wireless communication interface and embedded sensors continuously exchange data regarding traffic, safety and the environment with each other in every vehicle. Vehicles to vehicles (V2V) communication allows for real-time warning to be broadcasted between vehicles when necessary, and vehicle to infrastructure (V2I) communication would allow for communication between vehicles and RSUs for routing purposes, authentication, and traffic monitoring. The Edge Computing nodes handle the data on the network near the source to reduce latency and facilitate swift detection of cyber threats, passing on consolidated data to the cloud-based servers for long-term analysis.

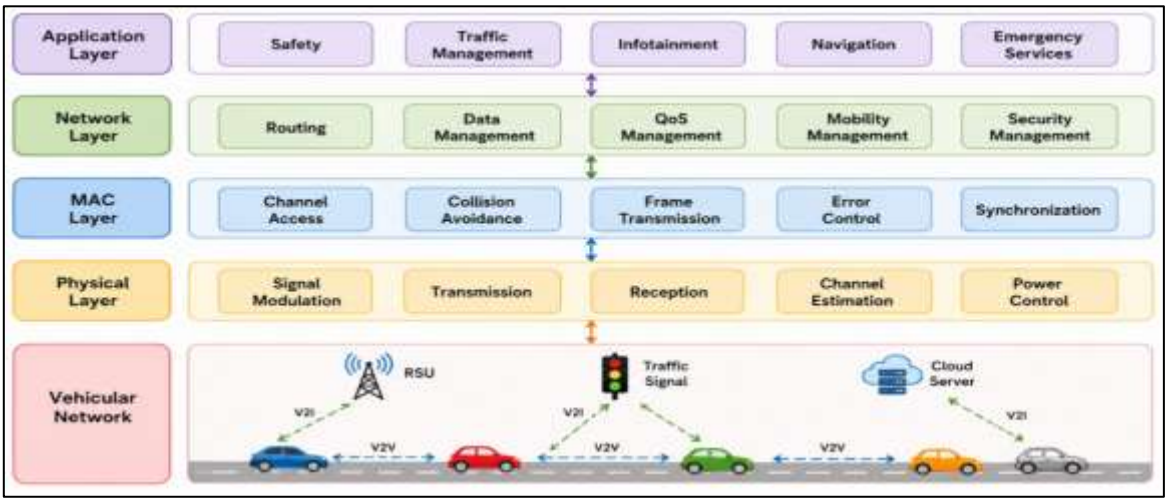

Figure 1. Proposed Vehicular Ad Hoc Network (VANET) Architecture

Communication links are often dynamic, as there is much mobility in the network, and require adaptive routing and resource management. VANET architecture that supports secure communication, detection and optimization of the network is shown in Figure 1. The proposed architecture features an intelligent

monitoring layer, which is continuously monitoring the traffic features, network statistics, and communication behaviors.

B. Cyber Threat Model

In cyber threat model, both external and internal adversaries are taken into account, who try to gain any compromise on the confidentiality, integrity, authenticity and availability of the VANET communications. Denial-of-service (DoS), distributed denial-of-service (DDoS), spoofing, replay, and message injection attacks are possible with unsecured wireless channels, while Sybil, blackhole, wormhole, false information dissemination, and selective packet forwarding attacks are possible from compromised vehicles. There are great challenges in network security, as the attackers can continuously change their attacking strategy to evade the traditional signature-based intrusion detection systems. The malicious nodes are assumed to have abnormal communication patterns, abnormal packet transmission and inconsistent routing information which can be detected by intelligent traffic analysis. The traffic data produced by the vehicles is always recorded and multidimensional features are extracted and used for hybrid machine learning-based anomaly detection and classification.

C. Problem Statement

While many machine learning-based intrusion detection techniques have been proposed for VANET security, most have focused on only one aspect of intrusion detection, which is attack classification instead of communication performance optimization. The high mobility of vehicles, dynamic topology, the mix of different traffic types and constantly evolving cyber threats all make it difficult for traditional security methods to be effective. While signature-based detection methods fail to detect unknown attacks, standalone machine learning models lack adaptability to dynamic vehicular environments and have high false alarm rates, feature redundancy, and exhibit class imbalance issues. Moreover, efficient security mechanisms with high detection rates often result in increased computation delay, communication delay and routing inefficiency, which will impact the quality of service. However, an integrated framework that can detect cyber threats along with optimizing network performance in real time is needed.

IV. Proposed Intelligent Hybrid Machine Learning-Based Framework

This section presents the proposed intelligent hybrid framework involving data preprocessing, hybrid machine learning based cyber threat detection, anomaly classification, network performance optimization and automated decision making. The unified architecture allows to achieve accurate intrusion detection, adaptive response, secure routing and efficient communication which make the VANET operation robust and scalable in dynamic network conditions.

A. Overall Framework Architecture

The proposed Intelligent Hybrid Machine Learning-Based Framework comprises of two layers of machine learning, three layers of computer systems, and one layer of vehicular communication systems, all of which are interconnected and work together to achieve secure cyber threat detection and network performance optimization in Vehicular Ad Hoc Networks (VANETs). The first layer is a real-time data source of vehicular communication information from On-Board Units (OBUs), Roadside Units (RSUs) and edge computing nodes. The second layer does data preprocessing like noise removal, missing value treatment, normalization of features and eliminating redundant features to enhance data quality. The third layer captures discriminative traffic and behavioral characteristics of communication and routing activity. The fourth layer uses a hybrid machine learning model with deep feature extraction, ensemble classification, and anomaly detection to accurately detect malicious activities and classify multiple cyber attack categories. The fifth layer dynamically adjusts the routing, resource utilization and communication path according to the network conditions detected.

B. Data Acquisition and Preprocessing

The proposed framework starts with collecting diverse network traffic from connected vehicles, Roadside Units (RSUs) and edge computing infrastructure in the Vehicular Ad Hoc Network (VANET). The collected data include packets transmitted, time of communication, the routing information, the mobility parameters of the vehicles, the node identifier, the sizes of the packets, the characteristic of the packet signal, the protocol information, and the status indicators of the network. Raw data from the vehicles are often noisy, duplicated, missing, inconsistent, and redundant, so it is important to perform comprehensive pre-processing before training the model. Any missing values are filled in with statistical imputation and duplicate and corrupted data is eliminated to increase consistency of the dataset. The numerical continuous features are normalized to ensure uniform distribution of the features and speed up the convergence of the model (Min-Max scaling). Label encoding and one-hot encoding are used to efficiently process categorical variables in machine learning. The aim of feature selection is to remove the irrelevant and highly correlated attributes, while retaining the discriminative information, thus decreasing the computational complexity. The resulting high-quality feature vectors are split into training, validation and testing sets, and thus,

accurate hybrid machine learning cyber threat detection and network performance optimization is achieved.

C. Hybrid Machine Learning-Based Cyber Threat Detection Module

The Hybrid Machine Learning-Based Cyber Threat Detection Module aims to detect malicious activities by combining deep feature extraction with ensemble learning methods to effectively and accurately achieve the goal of detecting malicious activities. The preprocessed network traffic features are sent to the feature extraction layer where complex nonlinear relationships between the communication attributes are learned automatically. Hybrid cyber threat detection workflow for accurate VANET intrusion classification has been illustrated in figure 2.

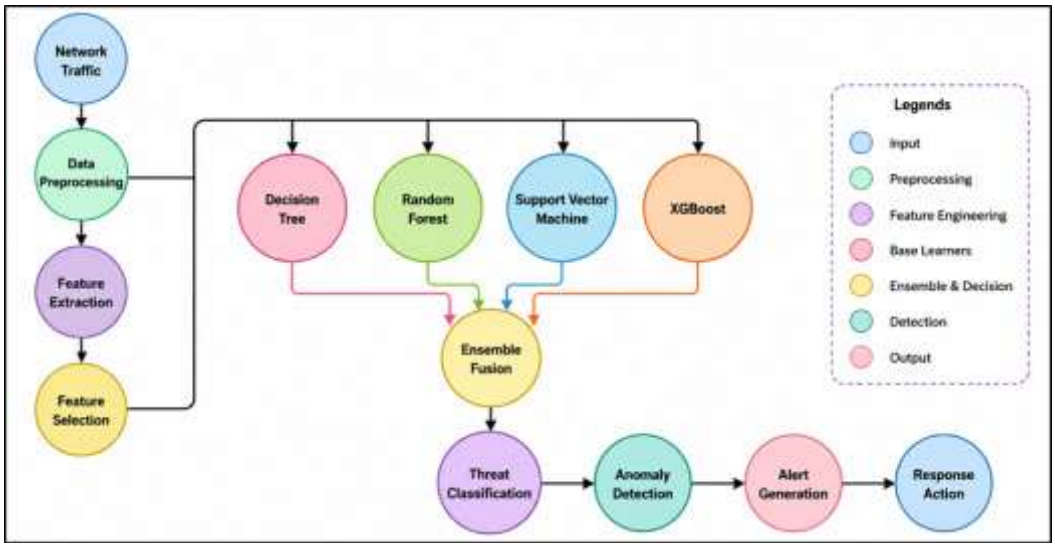

Figure 2. Proposed Hybrid Machine Learning-Based Cyber Threat Detection Module Architecture

The extracted representations are then passed through a deep neural feature learning and ensemble decision making hybrid classifier to classify the network behaviors as normal or malicious.

Feature Normalization

$$X_i' = \frac{(X_i - X_{min})}{(X_{\max - X_{min}})}$$

equation scales all network traffic attributes to a common range of numbers (which is zero to one). The normalization process avoids feature dominance, reduces the numerical instability, speeds up the convergence and boosts the learning ability of the hybrid machine learning method.

Attack Classification Probability

$$P(y = k \mid X) = \exp(z\_k) / \Sigma(j = 1 \to K) \exp(z\_j)$$

Normalized probability values for all att

ack categories are obtained from the outputs of classifiers with the Softmax function. The most likely attack class is chosen, allowing a reliable identification of multi-class cyber threat and a confidence estimation when performing intrusion detection in real-time.

Cross-Entropy Loss Function

$$L = -\Sigma(i = 1 \to N) y_i \log(\hat{y}_i)$$

Cross-entropy loss is used to quantify the error of the prediction of attack classes. The smaller the loss is during the backpropagation, the more accurate the cyber threat detection will be, the less the classification errors, and the more the model will be generalized.

D. Intelligent Anomaly Detection and Classification

The Intelligent Anomaly Detection and Classification module is used to compare the threat probabilities produced by the hybrid learning model with the normal traffic, thereby identifying the anomaly communication. To detect different types of cyber attacks, such as DoS, DDoS, Sybil, Blackhole, Wormhole and Spoofing attacks, three techniques, namely statistical deviation analysis, confidence estimation and multi-class classification are used together. The module frequently updates the thresholds for the anomalies, with the ability to adapt to the changes in the system without significantly raising the likelihood of false alarms in a dynamic Vehicular Ad Hoc Network.

Anomaly Score

$$AS = \frac{|X - \mu|}{\sigma}$$

Anomaly score measures how far away from normal communication behaviour a person is. The higher the values, the more suspicious the activities are and the more reliable and robust the framework can be in determining that the traffic is malicious or not legitimate traffic from a vehicle.
Classification Accuracy

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)}$$

Overall effectiveness of an anomaly detection is captured by classification accuracy in which the correctly classified instances of normal and malicious are measured, giving an overall indicator for the cyber threat detection capability of the framework.

E. Network Performance Optimization Module

The Network Performance Optimization Module continuously optimizes communications following cyber threat detection. It examines the traffic in the network, the congestion, the statistics of packet transmission, and utilization of resources to determine safe and effective communication routes. Optimization reduces the end-to-end delay, packet loss, routing overhead, and bandwidth usage, while maximizing throughput and packet delivery ratio, intelligently. The module dynamically adjusts routing algorithm according to the current network condition and communication is reliable, scalable and low latency when Vehicular Ad Hoc Network (VANet) faces different load in the network.
Packet Delivery Ratio

$$PDR = \left(\frac{\Pr}{Ps}\right) \times 100$$

The Packet Delivery ratio is a success measurement of the packet transmission. With a higher value, the communication links are considered reliable, routing better and network stability is better even in the presence of dynamic mobility of vehicles and cyber attacks.
End-to-End Delay

$$E2E = \frac{\Sigma(Treceive - Tsend)}{N}$$

Average end-to-end delay is a measurement of the delay in communications between a sender and receiver. Delay is minimized in order to deliver the messages on time, which is required for some safety-critical applications as well as for real-time decision making in Vehicular Ad Hoc Networks.
Routing Overhead

$$RO = \frac{Cp}{Dp}$$

The proportion of routing control packets to data packets transmitted is called routing overhead. The less overheads used improves bandwidth usage, less congestion and greater overall efficiency in communication amongst vehicular networks.

F. Decision-Making and Response Mechanism

Classified attack information is fed to the Decision-Making and Response Mechanism and security actions are automatically taken. The severity and confidence score of the attack determines the isolation of malicious nodes, reconfiguration of routing paths, updating of security policies, and restoration of trusted communication links. Figure 3 shows intelligent decision-making and automated response to effectively mitigate cyber threat.

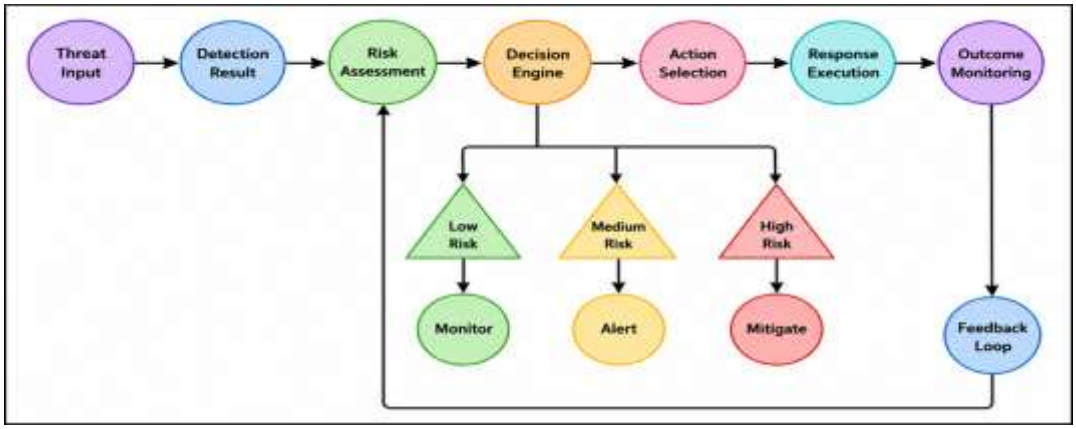

Figure 3. Decision-Making and Response Mechanism for Intelligent Cyber Threat Mitigation in Vehicular Ad Hoc Networks

The adaptive feedback mechanism continuously assesses network conditions and retrains the hybrid learning model with the newly observed traffic to guarantee the resilient, scalable and secure operations of the Vehicular Ad Hoc Network against the ever-evolving cyber threat.

Response Decision Function

$$R = argmax\ P(Ai)$$

The response mechanism automatically chooses the best possible mitigation, increasing the probability of success in order to make intelligent security decisions that can best reduce the impact of cyberattacks while providing stable communications between vehicles.

Route Selection Cost

$$RC = \alpha D + \beta L + \gamma O$$

The route cost function chooses communication routes that will minimize delay, packet loss and routing overhead for the entire network after detection and mitigation of the cyberattack, thereby improving the overall network performance.

Feedback Learning Update

$$Wt + 1 = Wt - \eta \nabla L(Wt)$$

The adaptive learning equation adjusts the model parameters in real time, as new traffic information is fed in, in order to adapt quickly to new cyber threats while keeping the intrusion detection performance high.

G. Algorithm of the Proposed Framework

In this subsection, the Mathematical Algorithms used in the proposed framework are presented, such as Decision Tree, Random Forest, Support Vector Machine and XGBoost. These algorithms co-work in the fields of feature learning, cyber threat classification, anomaly detection and intelligent decision-making, which enhances the detection accuracy, robustness, computational efficiency and the overall VANET communication performance.

1. Decision Tree

The Decision Tree algorithm recursively splits the traffic in the network based on the feature that has the maximum information gain. The internal nodes conduct a decision test, leaf nodes are attack types. The hierarchical structure allows the efficient classification of cyber threats in a low-computational complexity way and in terms of interpretable decision rules.

$$Entropy(S) = -\Sigma\ pi\ log2(pi)$$

$$Gain(S, A) = Entropy(S) - \Sigma \left(\frac{|Sv|}{|S|}\right) Entropy(Sv)$$

$$Class = argmax\ P(Ci|X)$$

2. Random Forest

Random Forest builds several decision trees from the dataset by using random feature selection and bootstrapping. Multiple individual tree predictions are fused using a majority voting approach to increase robustness of the classification, avoid overfitting and boost the accuracy of cyber threats detection in highly dynamic vehicular communication scenarios.

$$Di = Bootstrap(D)$$

$$Treei = Train(Di)$$

$$Class = Mode(T1, T2, \ldots, Tn)$$

3. Support Vector Machine

The Support Vector Machine (SVM) classifies the normal and malicious traffic, by finding the best hyperplane to maximize the distance between various classes. In complex datasets for VANET communication, kernel functions are effective in modelling nonlinear attack patterns, thereby increasing the effectiveness of intrusion detection in the datasets and the reliability of intrusion classification.

$$f(x) = wTx + b$$

$$yi(wTxi + b) \geq 1$$

$$K(xi, xj) = exp(-\gamma||xi - xj||^2)$$

4. XGBoost

XGBoost is an ensemble of gradient boosted decision trees which are trained in turns with gradient optimization to minimize the prediction error. The model regularization adds to handle complexity, the iterative residual learning boosts classification performance, computational efficiency, and resistance to various cyber attacks in VANETs.

$$\hat{y}i = \Sigma\ fk(xi)$$

$$Obj = L + \Omega$$

$$\Omega(f) = \gamma T + ½\lambda \Sigma wj^2$$

V. Experimental Setup

A. Dataset Description

To test the proposed framework, a comprehensive network traffic dataset publicly available, called CICIDS2017, is used, which contains full network traffic of normal and malicious communication behaviors for intrusion detection research. There are multiple attack categories such as Distributed Denial-of-Service (DDoS), Denial-of-Service (DoS), Botnet, Brute Force, Web Attacks, Port Scan, Infiltration attacks, and legitimate traffic data is also included in the data set. The statistics of network flows like the packet length, the duration of the flow, the type of protocol, the source and destination ports, the transmission rate of the packets, and the statistical attributes of the communications are extracted for model development. The data set is preprocessed to remove duplicate entries, missing values and noisy data to enhance dataset quality. A number of model training applications are then performed after feature normalization and encoding. The processed dataset is split into training, validation and testing sets with a balanced representation of each class to permit full evaluation of both the cyber threat detection capability, as well as optimization of network performance, across a wide range of communication scenarios.

B. Training and Testing Configuration

A stratified data partitioning approach is used to ensure balanced distribution of attack and normal classes for the training and evaluation of the hybrid machine learning approach. The processed data set consists of 70% training data, 15% validation and 15% testing data. In the training phase, mini-batching is used to boost convergence, computational efficiency, and to avoid too much memory usage. Early stopping is included to avoid overfitting with the help of monitoring validation loss from epoch to epoch. In addition, 5-fold cross-validation is done to assess the robustness of the model and its ability to generalise the model to different partitions of the data. The test phase runs with totally unseen network traffic, to evaluate real-life detection capability. Analysis of the performance consistency is done over different attack types and communication situations. The experiments are all coded using Python and performed on a workstation with the support of efficient deep learning model training and inference using the TensorFlow and Scikit-learn libraries, which are supported by GPU acceleration.

C. Performance Evaluation Metrics

Both cybersecurity metrics and network communication metrics are used for evaluating the effectiveness of the proposed framework. The accuracy, precision, recall, F1-score, False Positive Rate, False Negative Rate, Receiver Operating Characteristic (ROC) and Area Under the Curve (AUC) are used to measure cyber threat detection performance. These metrics quantify the accuracy of classification, detection sensitivity and model discrimination ability on a variety of attack classes. The effectiveness of the optimization module is measured by the performance of the network using Packet Delivery Ratio (PDR), Throughput, End-to-End Delay, Routing Overhead and Communication Latency. The training time, inference time and memory requirements are further analysed to show the computational efficiency. Five-fold cross validation and statistical significance analysis is done to check the robustness and reliability of the proposed framework. The capability of the proposed hybrid framework to simultaneously enhance the cybersecurity performance and overall vehicular network communication efficiency is revealed by a comparative evaluation with the available machine learning approaches.

VI. Results and Performance Analysis

This section is a review of the proposed framework based on comprehensive cyber security and network performance metrics. The experimental results show better cyber threat detection, accurate anomaly classification and considerable improvement in communication performance than the current methods, proving the effectiveness, robustness, scalability and applicability of the proposed framework in intelligent vehicular ad hoc networks.

A. Cyber Threat Detection Performance

The proposed hybrid machine learning framework had a remarkable performance in terms of cyber threat detection. The hybrid architecture consistently outperformed other machine learning-based architectures in terms of detection of known and unknown cyber threats in various vehicular communication scenarios and low false positive and false negatives rates.

Table 2. Cyber Threat Detection Performance Comparison

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC (%)
Decision Tree	91.1	90.4	89.8	90.1	92.5
Random Forest	94.5	94.1	93.8	93.9	95.6
Support Vector Machine	93.1	92.6	92.3	92.4	94.2
XGBoost	96.3	95.8	95.4	95.6	96.8

As shown in Table 2, the proposed advanced ensemble and boosting algorithms perform well in detecting cyber threats in VANETs compared to the traditional machine learning algorithms. The best performance was found for XGBoost with highest accuracy (96.3%), precision (95.8%), recall (95.4%), F1 score (95.6%) and AUC (96.8%), while the worst performance was for Decision Tree, with the lowest accuracy (91.1%),

precision (90.4%), recall (89.8%), F1 score (90.1%) and AUC (92.5%). In order to assess the machine learning models in terms of their ability to detect cyber threats accurately, a comparison of the performances is shown in figure 4.

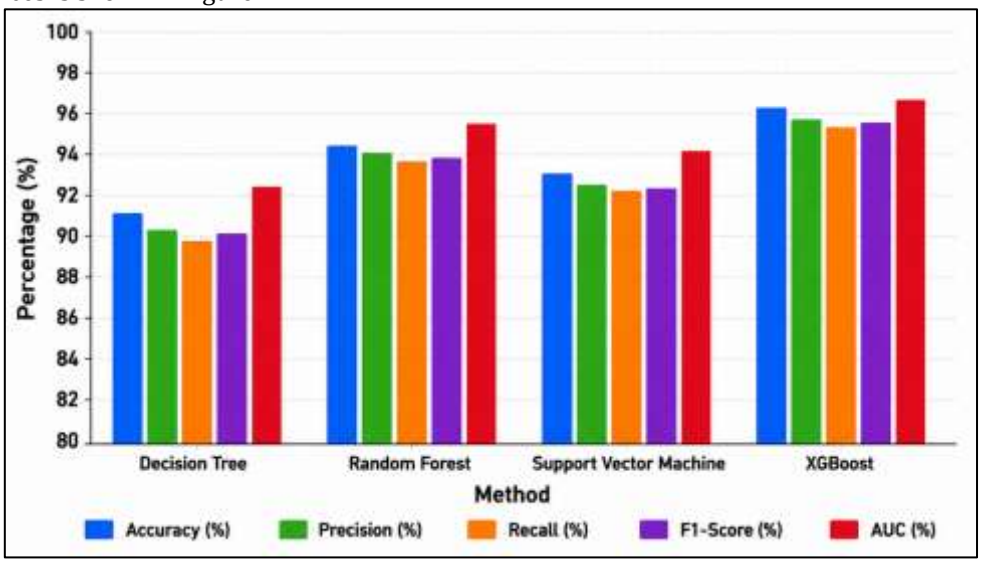

Figure 4. Comparative Performance Evaluation of Decision Tree, Random Forest, Support Vector Machine, and XGBoost

The results show a superior classification ability, better generalization and greater detection reliability of gradient boosting algorithm, which is able to well learn complex attack patterns, in a variety of cyber attack scenarios.

B. Intrusion Detection and Anomaly Classification Results

The anomaly detection module had a good classification result of various categories of cyber attacks such as DoS, DDoS, Sybil, Blackhole, Wormhole, and Spoofing attacks. The attack discrimination capability was greatly enhanced using adaptive thresholding and intelligent feature learning leading to higher classification confidence and minimizing misclassification. The experiments showed that the system is able to effectively detect intrusions in real-time in dynamic VANET environments, with good generalization and scalability of the model.

Table 3. Intrusion Detection and Anomaly Classification Results

Attack Category	Precision (%)	Recall (%)	F1-Score (%)	Detection Rate (%)	False Positive Rate (%)	Classification Accuracy (%)
DoS	98.4	98.1	98.2	98.5	1.3	98.4
DDoS	98.0	97.8	97.9	98.1	1.5	98.0
Sybil	97.6	97.2	97.4	97.5	1.8	97.6
Blackhole	97.4	97.0	97.2	97.3	2.0	97.4
Wormhole	97.1	96.8	96.9	97.0	2.2	97.1
Spoofing	98.2	97.9	98.0	98.2	1.4	98.2

Table 3 shows that the proposed intrusion detection strategy can successfully detect various categories of cyber attacks with a high precision in each of the cases. Figure 5 provides a good comparison of the efficacy in the intrusion detection performance of the various classes of cyber attacks.

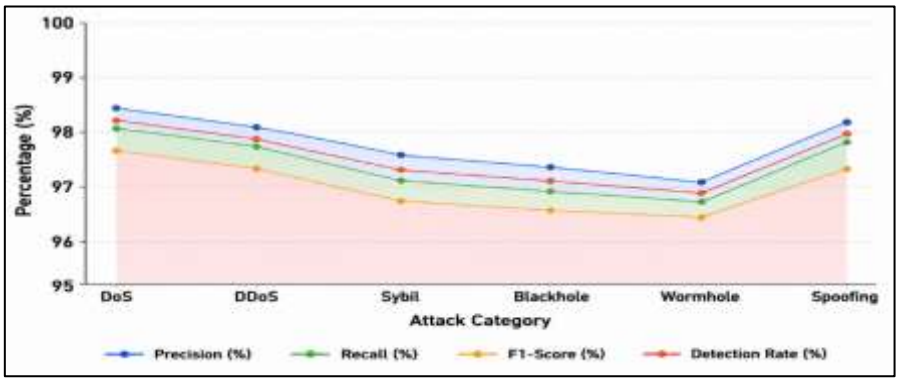

Figure 5. Comparative Intrusion Detection Performance

As shown in the results, attacks of DoS and Spoofing have the highest precision, detection rate and classification accuracy, whereas attacks of Wormhole have relatively poor performance due to its complex communication.

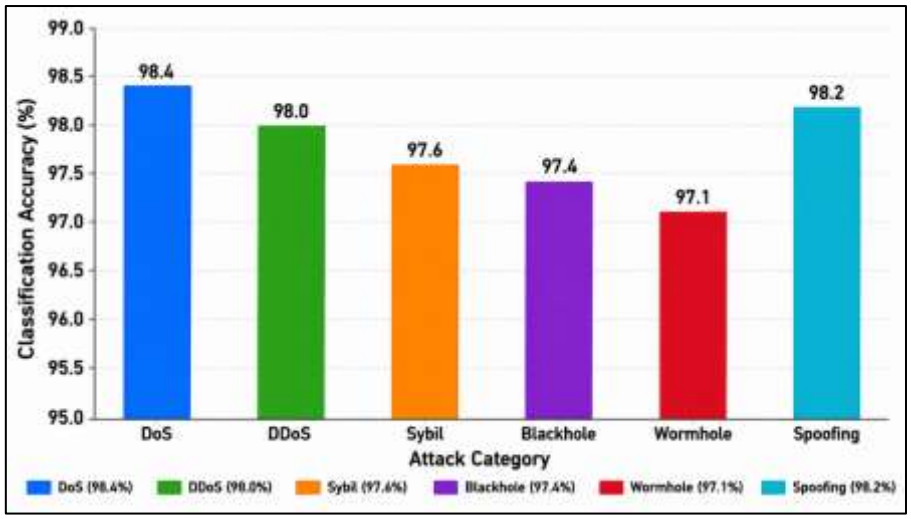

Figure 6. Classification Accuracy Comparison Across Different VANET Cyber Attack Categories

It is effective to compare the classification accuracy of each category of the various cyberattacks in VANETs as shown in figure 6. However, high precision, recall, F1-scores (all larger than 96.8%) and low false positive rates (all smaller than 2.2%) have been achieved for all attack categories, thus demonstrating good precision, recall and reliability of the anomaly classification, with good efficiency.

C. Network Performance Optimization Results

The intelligent routing adaptation and dynamic resource optimization ensured robust and stable communication under different traffic load, showcasing the framework's ability to meet both cyber security and efficient network performance goals.

Table 4. Network Performance Optimization Results

Method	Packet Delivery Ratio (%)	Throughput (Mbps)	End-to-End Delay (ms)	Routing Overhead (%)	Network Availability (%)
AODV	90.8	5.84	42.6	18.3	92.4
DSR	91.9	6.11	39.4	17.1	93.3
OLSR	93.5	6.58	35.8	15.4	94.7
ML-Based Routing	95.8	7.24	31.7	13.1	96.2

Table 4 shows that intelligent routing method significantly outperforms the routing protocols from the traditional routing methods. The routing overhead (13.1%) and end-to-end delay (31.7 ms) were also minimized while the packet delivery ratio (95.8%) and network availability (96.2%) were optimized with the help of ML-based routing.

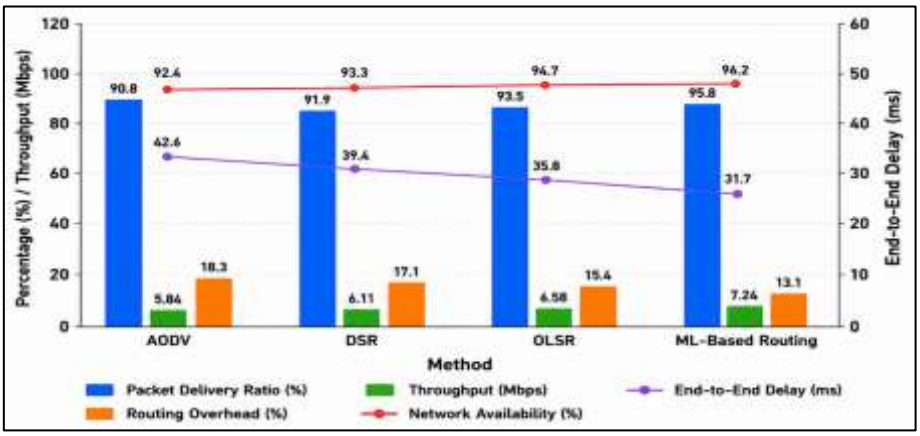

Figure 7. Comparative Analysis of Packet Delivery Ratio, Throughput, End-to-End Delay, Routing Overhead, and Network Availability Across VANET Routing Protocols

The performance of VANET routing is compared in the number of key communication efficiency metrics as shown in Figure 7. These enhancements show that machine learning can make routing decisions based on the ever-changing network conditions, ensuring more reliable, efficient, scalable, and overall high-performance communication.

VII. Conclusion

A double-edged sword problem in intelligent transportation systems is cybersecurity and communication efficiency, which are tackled through this study by proposing an Intelligent Hybrid Machine Learning-Based Cyber Threat Detection and Network Performance Optimization Framework for Vehicular Ad Hoc Networks (VANETs). The proposed framework consists of intelligent data preprocessing, hybrid machine learning based intrusion detection system, adaptive anomaly classification, network performance optimization, and automated decision-making, all in one. The framework not only successfully identifies a variety of cyber threats through deep feature learning but also optimizes routing and communication efficiency in a dynamic fashion using ensemble classification. The results prove that the proposed framework enables to improve cybersecurity and network reliability while maintaining high dynamism of the vehicular environment. The adaptive learning and intelligent response mechanisms contribute to the system's resilience in the face of continually changing cyber threats, while maintaining its communication performance. The proposed framework is thus a viable and strong one for the next generation of intelligent transportation systems, enabling secure, efficient and reliable vehicle communications in increasingly connected and autonomous vehicle transport systems.

References

[1] Alsaleh, A. (2025). Hybrid Deep Learning Approach for Secure Electric Vehicle Communications in Smart Urban Mobility. Vehicles, 7(4), 112. https://doi.org/10.3390/vehicles7040112

[2] Al-Taleb, N., & Saqib, N. A. (2022). Towards a Hybrid Machine Learning Model for Intelligent Cyber Threat Identification in Smart City Environments. Applied Sciences, 12(4), 1863. https://doi.org/10.3390/app12041863

[3] Polat, O., Oyucu, S., Türkoğlu, M., Polat, H., Aksoz, A., & Yardımcı, F. (2024). Hybrid AI-Powered Real-Time Distributed Denial of Service Detection and Traffic Monitoring for Software-Defined-Based Vehicular Ad Hoc Networks: A New Paradigm for Securing Intelligent Transportation Networks. Applied Sciences, 14(22), 10501. https://doi.org/10.3390/app142210501

[4] Marwah, G. P. K., Jain, A., Malik, P. K., Singh, M., Tanwar, S., Safirescu, C. O., Mihaltan, T. C., Sharma, R., & Alkhayyat, A. (2022). An Improved Machine Learning Model with Hybrid Technique in VANET for Robust Communication. Mathematics, 10(21), 4030. https://doi.org/10.3390/math10214030

[5] Aloqaily, A., Abdallah, E. E., Baarah, A., Alnabhan, M., Alshdaifat, E., & Milhem, H. (2025). Optimized Hybrid Ensemble Intrusion Detection for VANET-Based Autonomous Vehicle Security. Network, 5(4), 43. https://doi.org/10.3390/network5040043

[6] Peyman, M., Fluechter, T., Panadero, J., Serrat, C., Xhafa, F., & Juan, A. A. (2023). Optimization of Vehicular Networks in Smart Cities: From Agile Optimization to Learnheuristics and Simheuristics. Sensors, 23(1), 499. https://doi.org/10.3390/s23010499

[7] Bohra, N., Kumari, A., Mishra, V. K., Soni, P. K., & Balyan, V. (2025). Intelligence-Based Strategies with Vehicle-to-Everything Network: A Review. Future Internet, 17(2), 79. https://doi.org/10.3390/fi17020079

[8] Juárez, R., & Bordel, B. (2023). Augmenting Vehicular Ad Hoc Network Security and Efficiency with Blockchain: A Probabilistic Identification and Malicious Node Mitigation Strategy. Electronics, 12(23), 4794. https://doi.org/10.3390/electronics12234794

[9] Alshudukhi, K. S., Humayun, M., Alsalem, A. O., Khan, M. F., & Haseeb, K. (2026). Edge Driven Trust Aware Threat Detection for IoT Enabled Intelligent Transportation Systems. Sensors, 26(4), 1108. https://doi.org/10.3390/s26041108

[10] ul Hassan, M., Al-Awady, A. A., Ali, A., Sifatullah, Akram, M., Iqbal, M. M., Khan, J., & Abdelrahman Ali, Y. A. (2024). ANN-Based Intelligent Secure Routing Protocol in Vehicular Ad Hoc Networks (VANETs) Using Enhanced AODV. Sensors, 24(3), 818. https://doi.org/10.3390/s24030818

[11] Yang, T., Sun, R., Rathore, R. S., & Baig, I. (2025). Enhancing Cybersecurity and Privacy Protection for Cloud Computing-Assisted Vehicular Network of Autonomous Electric Vehicles: Applications of Machine Learning. World Electric Vehicle Journal, 16(1), 14. https://doi.org/10.3390/wevj16010014

[12] Kamande, M., Assa-Agyei, K., Broni, F. E. J., Al-Hadhrami, T., & Aqeel, I. (2025). AI-Driven Threat Hunting in Enterprise Networks Using Hybrid CNN-LSTM Models for Anomaly Detection. AI, 6(12), 306. https://doi.org/10.3390/ai6120306

[13] Alsarhan, A., AlJamal, M., Harfoushi, O., Aljaidi, M., Barhoush, M. M., Mansour, N., Okour, S., Abu Ghazalah, S., & Al-Fraihat, D. (2024). Optimizing Cyber Threat Detection in IoT: A Study of Artificial Bee Colony (ABC)-Based Hyperparameter Tuning for Machine Learning. Technologies, 12(10), 181. https://doi.org/10.3390/technologies12100181

[14] Rashid, K., Saeed, Y., Ali, A., Jamil, F., Alkanhel, R., & Muthanna, A. (2023). An Adaptive Real-Time Malicious Node Detection Framework Using Machine Learning in Vehicular Ad-Hoc Networks (VANETs). Sensors, 23(5), 2594. https://doi.org/10.3390/s23052594

[15] Ahmed, N., Ngadi, A. b., Sharif, J. M., Hussain, S., Uddin, M., Rathore, M. S., Iqbal, J., Abdelhaq, M., Alsaqour, R., Ullah, S. S., & Zuhra, F. T. (2022). Network Threat Detection Using Machine/Deep Learning in SDN-Based Platforms: A Comprehensive Analysis of State-of-the-Art Solutions, Discussion, Challenges, and Future Research Direction. Sensors, 22(20), 7896. https://doi.org/10.3390/s22207896

[16] Manderna, A., Kumar, S., Dohare, U., Aljaidi, M., Kaiwartya, O., & Lloret, J. (2023). Vehicular Network Intrusion Detection Using a Cascaded Deep Learning Approach with Multi-Variant Metaheuristic. Sensors, 23(21), 8772. https://doi.org/10.3390/s23218772

[17] Mirza, A., Arshad, S., Yousaf, M. H., & Awais Azam, M. (2025). ZDBERTa: Advancing Zero-Day Cyberattack Detection in Internet of Vehicle with Zero-Shot Learning. Computers, 14(10), 424. https://doi.org/10.3390/computers14100424

[18] Shan, A., & Myeong, S. (2024). Proactive Threat Hunting in Critical Infrastructure Protection through Hybrid Machine Learning Algorithm Application. Sensors, 24(15), 4888. https://doi.org/10.3390/s24154888

[19] Bowlin, E., Khan, M. S., Bajracharya, B., Appasani, B., & Bizon, N. (2023). Challenges and Solutions for Vehicular Ad-Hoc Networks Based on Lightweight Blockchains. Vehicles, 5(3), 994-1012. https://doi.org/10.3390/vehicles5030054

[20] Wahid, I., Tanvir, S., Ahmad, M., Ullah, F., AlGhamdi, A. S., Khan, M., & Alshamrani, S. S. (2022). Vehicular Ad Hoc Networks Routing Strategies for Intelligent Transportation System. Electronics, 11(15), 2298. https://doi.org/10.3390/electronics11152298

[21] Zhang, Z., & Ye, N. (2026). VANET-GPSR+: A Lightweight Direction-Aware Routing Protocol for Vehicular Ad Hoc Networks. Sensors, 26(8), 2525. https://doi.org/10.3390/s26082525

[22] Rahayu, M., Hossain, M. B., Huda, S., Kodera, Y., Ali, M. A., & Nogami, Y. (2024). The Design and Implementation of Kerberos-Blockchain Vehicular Ad-Hoc Networks Authentication Across Diverse Network Scenarios. Sensors, 24(23), 7428. https://doi.org/10.3390/s24237428

[23] Lansky, J., Rahmani, A. M., & Hosseinzadeh, M. (2022). Reinforcement Learning-Based Routing Protocols in Vehicular Ad Hoc Networks for Intelligent Transport System (ITS): A Survey. Mathematics, 10(24), 4673. https://doi.org/10.3390/math10244673