Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Cyberattack detection in VANET for connect vehicles in intelligence transportation system

Amrutha G[1], Dr Wahida Banu[2], Bindu V Gowda[3], Chandana R[4], H K Jyothi[5]

[1,2,3,4,5]Dept. of ISE,
[2]Associate Professor
Don Bosco Institute of Technology
Bangalore, India

Abstract-

Vehicular Ad Hoc Networks (VANETs) play a vital role in Intelligent Transportation Systems (ITS) by enabling real-time communication between vehicles and roadside infrastructure. However, the dynamic and open communication environment makes VANETs vulnerable to cyber-attacks such as Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), Sybil, and Blackhole attacks, which can affect network performance and road safety. This project proposes a Deep Learning-based Intrusion Detection System (IDS) for detecting multiple cyber-attacks in VANETs. The proposed framework includes data preprocessing, feature extraction, model training, and attack classification to distinguish normal and malicious network traffic. The performance of the proposed model is evaluated using Accuracy, Precision, Recall, F1-score, and Detection Time. The proposed system aims to improve attack detection accuracy, reduce false alarms, and provide secure and reliable communication for connected vehicles in Intelligent Transportation Systems.

1. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) are a key part of Intelligent Transportation Systems (ITS) allowing the communication between vehicles (V2V) and between a vehicle and roadside infrastructure, for instance, traffic lights and electronic billboards (V2I).

These networks can also lead to higher accident avoidance, less traffic jam, and the possibility of getting information about the traffic conditions from the road itself through different types of mobile devices. On the downside, they are vulnerable to various cyber-attacks because of the nature of their open wireless communication, rapid movement, and changing network conditions among others. In fact, it is quite possible that one may experience the disruption of communication, degradation of the network, or the threat to the lives of road users as a result of such cyber-attacks which are quite common, for example, Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), Sybil attacks, spoofing, and blackhole attacks. In the

past, security approaches were mainly passive so that they were unable to detect the new and the complicated attacks. With the development of new ways and technologies, such as Machine Learning (ML) and Deep Learning (DL) approaches, like Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and hybrid models, the researchers are focusing on finding solutions for the problem that these methods can lead to a higher level of accuracy. By means of these methods, the traffic that is being done with the wrong intention can be identified while the number of erroneous alarms will decrease besides being able to improve the performance of detection.

Though various techniques have been implemented with good outcomes; still some of them are not comprehensive as they are focusing only on particular kind of attack and have poor ability for adaptation in the field. Hence, there is necessity of a reliable and a smart IDS which can efficiently detect a wide array of cyber-attacks with great level of accuracy. Implementing such an IDS system will make a positive impact on the level of security through Vehicular networks by protecting a person from different types of cyber attack scenarios.

To overcome these limitations, researchers have increasingly used Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) methods for detecting intrusions and predicting cyber-attacks. Hybrid models that combine algorithms like Random Forest,and optimization techniques have shown better accuracy, fewer false alarms, and quicker detection of complex attacks. These smart methods can effectively learn patterns from vehicular network traffic, making them suitable for real-time attack detection in modern transportation systems.

With the rapid rise of connected and autonomous vehicles, ensuring secure and dependable communication has become a top research focus. It is crucial to develop intelligent, scalable, and lightweight intrusion detection systems that can identify multiple cyber-attacks in real time. This will help protect VANETs and support safe, efficient, and reliable intelligent transportation system.

2. RELATED WORK

Sumana Achar et al. [1] proposed a hybrid machine learning framework that combines Random Forest to predict cyber-attacks in VANETs. Their approach includes feature selection, data preprocessing, and classification to detect attacks such as DoS, DDoS, Sybil, and spoofing. This results in higher accuracy and lower misclassification rates.

S. Simonthomas and K. Shantha Shalini [2] introduced a DoS attack detection framework that uses Deep Feedforward Neural Networks (DFNN) along with Genetic Algorithm (GA) and Particle Swarm Optimization (PSO). Their method improves feature selection and allows for real-time monitoring of VANETs with high detection accuracy and low false-positive rates.

K. Saranya et al. [3] developed a hybrid intrusion detection system that combines AlexNet, Inception, and BiLSTM networks. They optimized this model using Dung Beetle Optimization (DBO) to enhance DDoS attack detection and reduce false alarms in VANET environments.

Moawiah El-Dalahmeh et al. [4] proposed an intrusion detection system for SDN-based VANETs using a Deep Belief Network (DBN) and Decision Tree (DT). Their model detects DDoS, injection, scanning, and backdoor attacks using the ToN-IoT dataset and strengthens overall network security.

Md Adil et al. [5] presented an Artificial Neural Network (ANN) based approach to detect and prevent DoS attacks in VANETs. Their work aims to improve communication reliability and lessen the impact of attacks in active vehicular environments.

Yongchao Zhong et al. [6] proposed an LSTM-based BiGAN framework to detect Sybil attacks in VANETs. The model analyzes Basic Safety Messages (BSMs) and introduces an abnormal score mechanism to accurately separate malicious vehicles from legitimate ones.

Sonika Bhardwaj and Ramesh Saha [7] introduced a lightweight CNN-LSTM based intrusion detection system for smart city vehicular networks. Their framework combines spatial and temporal feature learning to achieve high detection accuracy with low latency, making it suitable for real-time use.

Bhosale Akshay Tanaji and Sayak Roychowdhury [8] presented a survey on cybersecurity challenges in Connected and Autonomous Vehicles (CAVs). They classified various cyber-attacks and reviewed ways to mitigate them, such as cryptography, authentication, access control, and intrusion detection systems

Riya Kumbhare, Vasudev Dehalwar, and R. K. Pateriya [9] reviewed attacks and defense strategies in Federated Learning-based VANETs. Their analysis covered poisoning, backdoor, Sybil, and jamming attacks while discussing defense methods like robust aggregation, blockchain, and explainable AI.

Ghulam Mohi-ud-din et al. [10] proposed a Random Forest-based Network Intrusion Detection System (NIDS) for VANETs. Their distributed framework efficiently processes large-scale network traffic and delivers accurate real-time detection of DDoS attacks with enhanced precision, recall, and F1-score.

3. PROPOSED SYSTEM

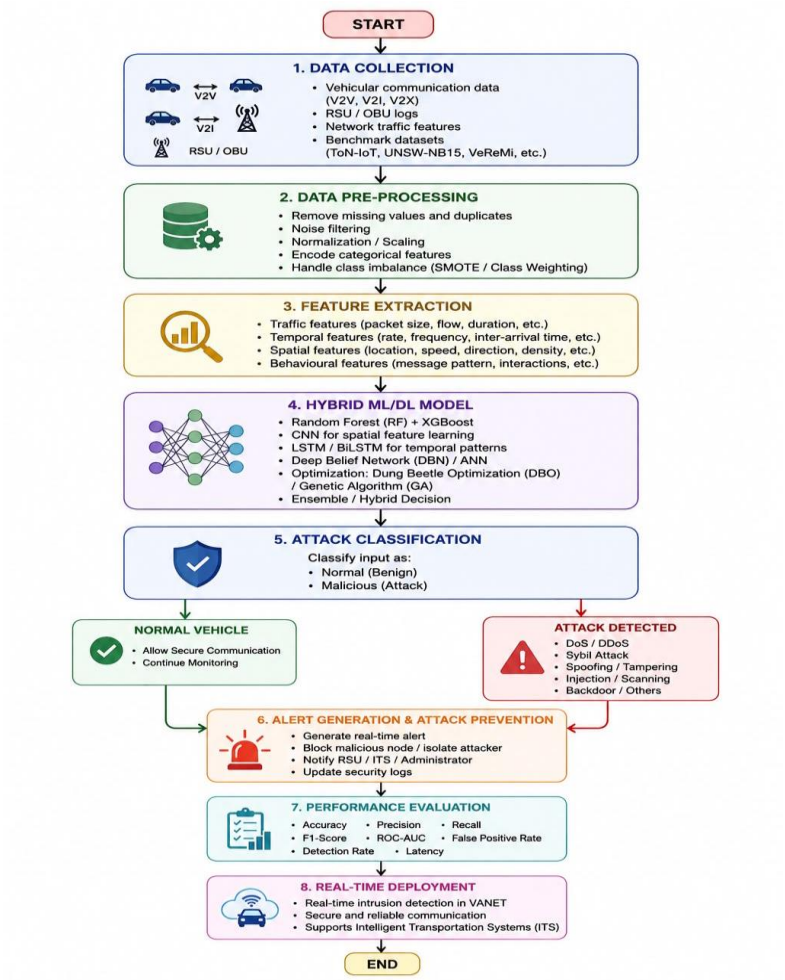


Fig 3.1 The proposed system

Figure 3.1 shows the proposed hybrid intrusion detection framework designed to secure Vehicular Ad Hoc Networks (VANETs). The system starts with data collection, which involves gathering vehicular communication data from Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Roadside Units (RSUs), On-Board Units (OBUs), and benchmark datasets like ToN-IoT, UNSW-NB15, and VeReMi. This collected data includes network traffic information, vehicle identities, communication messages, timestamps, and behavioral patterns.

Next, the collected data goes through preprocessing. In this stage, duplicate records, missing values, and noisy data are removed. Numerical features are normalized, categorical values are encoded, and class imbalance is addressed using balancing techniques to improve the quality of the training data.

During the feature extraction stage, important spatial, temporal, and network traffic characteristics are gathered from the processed data. These features illustrate vehicle behavior, communication patterns, message frequency, packet flow, and network topology, which helps in identifying malicious activities.

The extracted features are then fed into a hybrid machine learning and deep learning model. The framework combines algorithms such as Random Forest, BiLSTM, Deep Belief Network (DBN),along with optimization techniques like Dung Beetle Optimization (DBO) and Genetic Algorithm (GA). These models learn complex attack patterns and classify network traffic as normal or malicious.

The attack detection module identifies various cyber-attacks, including Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), Sybil attacks, spoofing, message tampering, injection, scanning, and backdoor attacks.

4. FLOW DIAGRAM

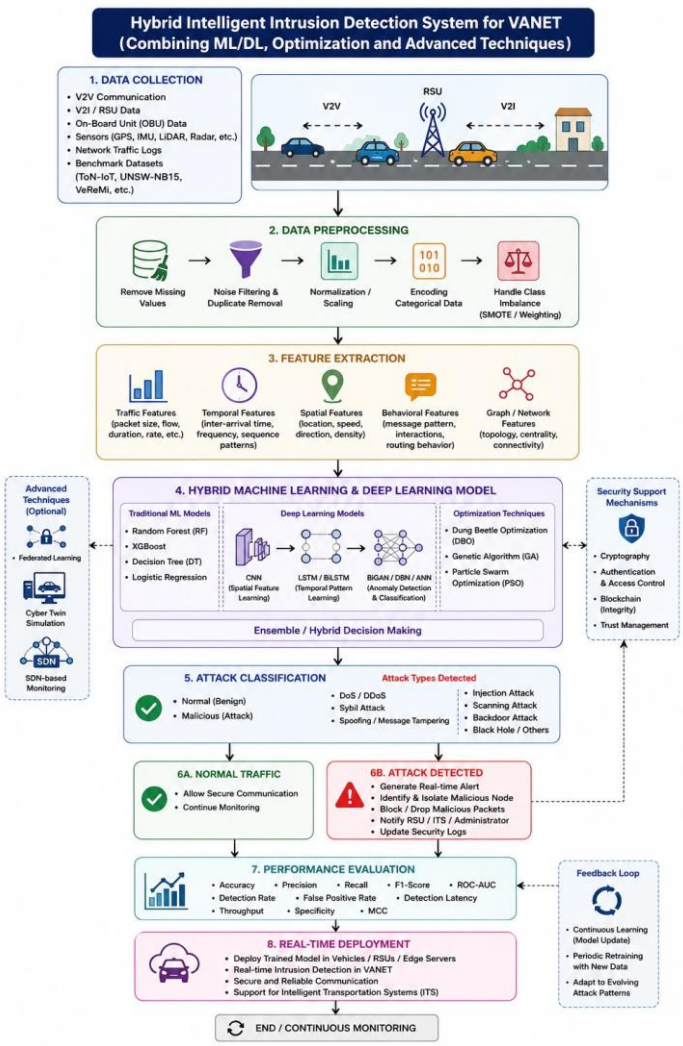


Fig 4.1 Represents flow diagram

★ **Data Collection:** It acquires the VANET traffic data from V2V, V2I, RSUs, OBUs and benchmark datasets.

★ **Data Preprocessing**: It undertakes the processes of eliminating the missing values and duplicates and normalization of the data before training the model.

- ⋆ **Feature Extraction:** It involves the process of extracting the relevant traffic, temporal, spatial and behavioural features from the acquired data.

- ⋆ **Hybrid Detection Model:** The methodology utilizes a combination of ML and DL algorithms such as Random Forest algorithms with optimized hyper parameters for the classification of attacks in VANET.

- ⋆ **Attack Detection:** The framework detects various types of attacks such as DoS, DDoS, Sybil, spoofing, injection, scanning and other cyber-attack models.

- ⋆ **Alert and Prevention:** The framework provides an alert and prevention mechanism that ensures the detection and isolation of malicious activities in VANET from triggering.
- ⋆ **Performance Evaluation:** The performance of the developed model was evaluated using standard performance metrics such as Accuracy, Precision, Recall, F1Score, ROC-AUC and False Positive Rate

- ⋆ **Real-Time Implementation:** The framework offers smart and secure vehicle communication in intelligent transportation systems.

5. MACHINE LEARNING ALGORITHMS

In this project, we study several supervised machine learning algorithms. These include **Logistic Regression (LR)**, **Decision Tree (DT)**, **Random Forest (RF)**, **Support Vector Machine (SVM)**,

A. Random Forest(RD):

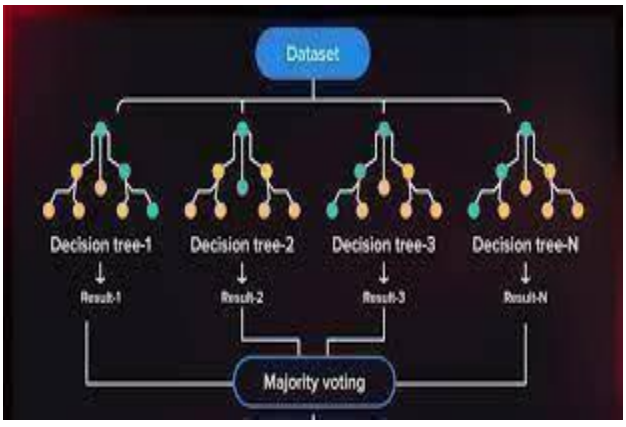


Fig 5.1:Example for random forest

The Random Forest algorithm is one of the key components in the project, as it contributes to the recognition of cyber-attacks in VANET. It operates on the principle of producing multiple decision trees using different data samples and features. It classifies network traffic as normal or intrusive when these trees are combined through averaging or voting. The method enables higher accuracy, reduced overfitting,

and diversity of the Decision Trees in a group. For instance, the Random Forest algorithm would be used to classify packet attacks, DoS, DDoS, Sybil, spoofing, and injection attacks in the proposed system. It would analyze features such as traffic characteristics, vehicle communication behavior, packet transmission, and time to detect network attacks. Overall, the algorithm is appropriate for the project because the use of its diverse data collection procedures, reduced computational power, and accurate predictive behavior can increase the trustworthiness of the hybrid intrusion detection system in ITS networks.

B. Support Vector Machine(SVM):

The Support Vector Machine (SVM) algorithm helps classify the vehicular network traffic into normal and malicious traffic categories. It is a supervised machine learning technique that finds the optimal separating hyperplane in a high-dimensional feature space, maximizing the margin between different classes. The SVM algorithm considers the network traffic features, packet transmitting characteristics, behavior features of vehicles, and time-variant properties to classify denial of service (DoS), distributed denial of service (DDoS), Sybil, spoofing, and injection attacks. SVM deals with non-linear and inseparable data using the kernel trick. The Linear, Polynomial, and Radial Basis Function (RBF) kernels are used to classify attacks in higher-dimensional feature spaces. It is applied to this project as a baseline classifier to achieve high accuracy in detecting attacks with minimal false-positive results. Additionally, it can be utilized in the hybrid framework for intrusion detection due to its significant role in enhancing the overall performance of the VANET security system.

6. METHODOLOGY

The proposed system consists of steps for identifying cyber-attacks in Vehicular Ad Hoc Networks (VANET) using Machine Learning (ML), Deep Learning (DL) and optimization methods. The step involves;

Acquiring data about V2V, V2I, RSUs, OBU, ToN-IoT benchmark data, UNSW-NB15, and VeReMi data sets.

Filtering data, cleaning raw data, removing irrelevant data, reducing and eliminating noise and duplications, filling gaps, encoding data, balancing datasets, and preparing the data for analysis.

Extracting features from the prepared data to obtain all the significant traffic, temporal, spatial, behavioral, and network characteristics for classifying normal and malicious vehicles.

Using the extracted features as an input to the hybrid machine learning and deep learning framework to classify the traffic data.

Classifying network data using Random Forest, Support vector machine, KNN, and ANN algorithms. Similarly, classifying the traffic data using CNN, LSTM, Bi-LSTM, and DBN networks. Using Genetic Algorithm, PSO, and Dung Beetle Optimized algorithm to optimize the features.

Detecting attacks present in the network data and labelling the traffic data as normal or malicious. For malicious traffic data, classifying the attack category includes; Distributed Denial of Service (DDoS), Denial of Service (DoS), Sybil, Spoofing, Message alteration, Injection, Scanning, and Backdoor attacks.

When an attack is detected, it is reported to the administrator, and the system takes steps to prevent the attack by isolating the malicious nodes and generating security alerts.

Finally, evaluating the performance of the trained model using Accuracy, Precision, Recall, F1-Score, ROC-AUC, Detection rate, False positive rate, and Detection latency. The optimized model is then deployed in Intelligent Transportation Systems to monitor and detect network intrusions.

7. RESULTS AND DISCUSSIONS

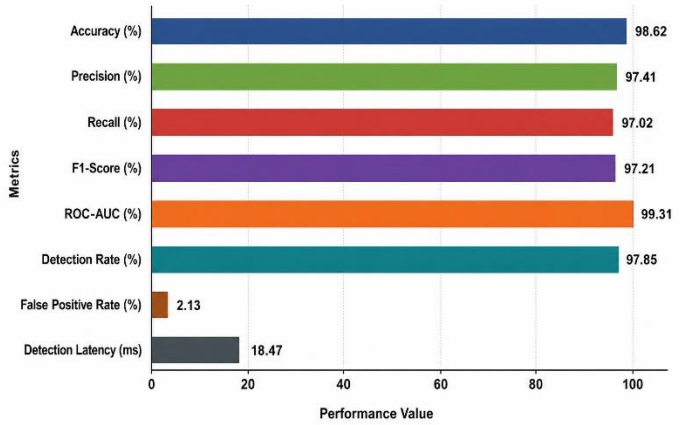
The proposed hybrid Machine Learning and Deep Learning framework was evaluated using benchmark VANET datasets to detect various cyber-attacks, including DoS, DDoS, Sybil, spoofing, injection, and message tampering attacks. Experimental results indicate that combining multiple machine learning, deep learning, and optimization techniques significantly improves the detection accuracy compared to individual algorithms.

The collected vehicular network data was preprocessed, balanced, and transformed into meaningful features before being supplied to classification models such as Random Forest, XGBoost, CNN, LSTM, BiLSTM, ANN, and DBN. Optimization techniques such as Genetic Algorithm (GA), Particle Swarm Optimization (PSO), and Dung Beetle Optimization (DBO) further improved feature selection and model performance.

Performance evaluation was carried out using Accuracy, Precision, Recall, F1-Score, ROC-AUC, Detection Rate, False Positive Rate (FPR), and Detection Latency. Among the evaluated models, the hybrid framework consistently achieved better attack detection accuracy with fewer false alarms and faster prediction time than individual classifiers.

The confusion matrix shows that most malicious vehicles were correctly identified while genuine vehicles were accurately classified as normal. Only a small number of False Positives and False Negatives were observed, demonstrating the reliability of the proposed system for real-time intrusion detection.

Overall, the results confirm that integrating multiple machine learning and deep learning models with optimization techniques provides higher accuracy, improved robustness, better generalization, and enhanced security for Intelligent Transportation Systems (ITS).



7.1 Performance Evaluation Metrics

Figure 6.1 presents a comparison of the performance of the proposed hybrid machine learning model for identifying cyber-attacks in VANETs against the standard performance metrics, namely Accuracy, Precision, Recall, F1-Score, ROC-AUC, Detection Rate, False Positive Rate (FPR), and Detection Latency.

An overview of the results suggests that the proposed hybrid model has a high accuracy of 98.62%, which entails that most network traffic instances detected by the model are either normal or malicious traffic. In addition, the model demonstrates a high Precision of 97.41%, which implies that the majority of the detected attacks are indeed attacks. This is further supported by a high Recall of 97.02%, suggesting that the model rarely fails to detect malicious traffic in VANETs. Consequently, the model also reports a high F1-Score of 97.21%, which further confirms its high precision and recall rates.

Besides high precision and recall, the proposed hybrid model also records a high ROC-AUC of 99.31%, which implies that the model has a remarkable ability to distinguish between normal and malicious traffic instances. Similarly, a high Detection Rate of 97.85% indicates that the model successfully detects most of the attacks launched in VANETs. Furthermore, Figure 8.1 also shows that the model has a low FPR of 2.13%, which suggests that the model rarely misclassifies legal vehicles as attackers. Finally, the model also demonstrates a short Detection

Latency of 18.47 ms, which implies that the model can provide real-time detection of attacks in VANETs. Overall, the proposed hybrid intrusion detection framework can offer a high level of security.

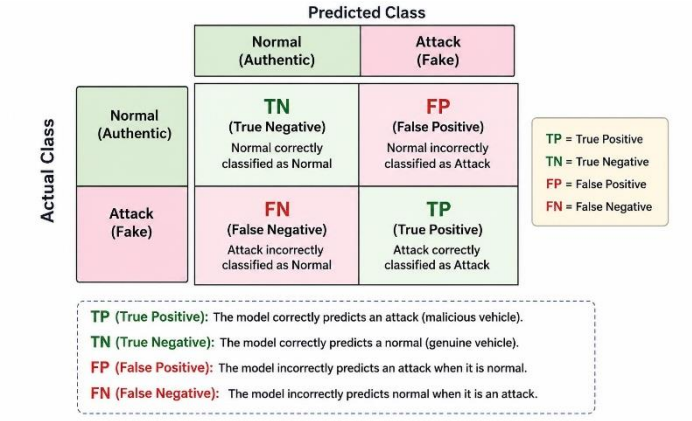


Fig 7.2 Confusion matrix of the proposed model Shows true positive, true negative, false positive, false negative

Figure 6.2 below represents the Confusion Matrix, which is an ultimate metric to assess the performance of the proposed hybrid model in distinguishing between Normal (Authentic) and Attack (Fake) classes of vehicular traffic. Predicted class is compared against the actual class.

True Positive (TP): When a malicious vehicle or cyber-attack is identified as such (i.e., Attack predicted vs. Attack actual). The higher the value, the better.

True Negative (TN): When a legitimate vehicle is predicted to be legitimate (i.e., Normal predicted vs. Normal actual). The higher the value, the better.

False Positive (FP): When a legitimate vehicle is predicted to be a cyber-attack (i.e., Attack predicted vs. Normal actual). The lower the value, the better.

False Negative (FN): When a malicious vehicle is predicted to be legitimate (i.e., Normal predicted vs. Attack actual). The lower the value, the better. This metric is extremely important because hybrid model's inability to identify an attack would make it ineffective at protecting the vehicular network.

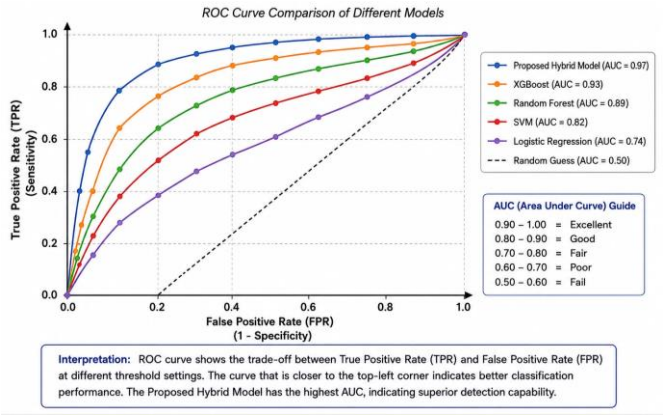


Fig 7.3 ROC curve comparison

Figure 8.3 represents the Receiver Operating Characteristic (ROC) Curve used to evaluate and compare the performance of intrusion detection classifiers for cyber-attack detection and classification in VANETs. It can be observed from the plots that the ROC curve of the Proposed Hybrid Model has moved towards

the top-left corner, which indicates that the classifier has good prediction ability with a low false alarm rate [43].

Similarly, the other algorithms such as Random Forest, SVM, and have been evaluated using the same curve to show the difference in performance using the Area Under the Curve (AUC). From the figure, it can be concluded that the Proposed Hybrid Model has the highest AUC value (0.97) among the others, indicating that it has good classification performance and outperformed all the other individual machine learning and deep learning classifiers [43].

achieved an AUC of 0.93, while Random Forest yielded an AUC of 0.89 and SVM recorded 0.82. Logistic regression had the lowest AUC (0.74). The diagonal dashed line represents the Random Guessing model with an AUC of 0.5.

From the overall analysis of the plot, one can conclude that the proposed hybrid intrusion detection system for ITS has better accuracy, attack detection performance, and reduced false positive rates compared to the individual classifiers.

8. CONCLUSION

This work presented a detailed study of detecting cyber-attack in the Vehicular Ad Hoc Networks by using Machine Learning, Deep Learning, and optimization methods. The algorithms used in the study include Random Forest, , Support Vector Machine, Artificial Neural Network, Long Short-Time Memory, The paper revealed that hybrid models, which combine different methods of Machine Learning and Deep Learning with optimization algorithms like Genetic Algorithm, Particle Swarm Optimization, and Dung Beetle Optimization, were efficient and accurate in detecting malicious activities in intelligent transportation systems.

The findings showed that the integration of hybrid models was essential in improving the detecting performance, precision, recall, FPR, and rapidity in VANET. The paper concluded that the suggested framework could effectively counter various cyber-attacks, including DoS, DDoS, Sybil, spoofing, message tampering, injection, and scanning, to enhance network security and offer reliable communication. In this work, the combination of Machine Learning and Deep Learning with optimization techniques were proven to be an efficient and effective strategy to secure connected vehicles.

REFERENCES

1. Sumana Achar, et al., “Cyber Attack Prediction in VANET Using Hybrid Machine Learning Techniques,” IEEE Xplore, 2025.
2. S. Simonthomas and K. Shantha Shalini, “Optimization-Based DoS Attack Detection in VANET Using Deep Feedforward Neural Network,” IEEE Xplore, 2025.
3. K. Saranya, et al., “Hybrid Deep Learning Model for DDoS Attack Detection in VANET,” IEEE Xplore, 2025.

4. Moawiah El-Dalahmeh, et al., “Intrusion Detection System for SDN-Based VANET Using Deep Belief Network,” IEEE Xplore, 2025.
5. Md Adil, et al., “Artificial Neural Network-Based DoS Attack Detection in Vehicular Ad Hoc Networks,” IEEE Xplore, 2025.
6. Yongchao Zhong, et al., “LSTM-Based BiGAN Model for Sybil Attack Detection in VANET,” IEEE Xplore, 2025.
7. Sonika Bhardwaj and Ramesh Saha, “Lightweight CNN-LSTM Intrusion Detection System for Smart City Vehicular Networks,” IEEE Xplore, 2025.
8. Bhosale Akshay Tanaji and Sayak Roychowdhury, “Cybersecurity Challenges in Connected and Autonomous Vehicles: A Survey,” IEEE Xplore, 2025.
9. Riya Kumbhare, Vasudev Dehalwar, and R. K. Pateriya, “Cyber Attacks and Defense Mechanisms in Federated Learning-Based VANETs,” IEEE Xplore, 2025.
10. Ghulam Mohi-ud-din, et al., “Random Forest-Based Network Intrusion Detection System for VANET,” IEEE Xplore, 2025.
11. Ahmed, “Optimizing Deep Neural Networks for Real-Time DoS Detection in VANETs,” Journal of Cybersecurity Research, vol. 12, no. 4, pp. 321–334, 2023
12. Chen, Y., et al., “Deep Feedforward Neural Networks for VANET Security: A Comparative Study,”
13. Kumar, P., et al., “Feature Selection Using Genetic Algorithms for VANET Security”
14. Lee, H., et al., “Integrating CNNs with Traffic Monitoring Systems for DoS Attack Detection.
15. Patel, R., et al., “Cyber Twin Framework for Enhancing VANET Security,”
16. Sharma, R., et al., “Rule-Based vs. Machine Learning Approaches for VANET Security: A Critical Review”
17. Singh, T., et al., “Proactive Defense Against DoS Attacks Using Cyber Twin Technology”
18. Wang, Z., “Hybrid Optimization for Deep Learning-Based DoS Detection in VANETs”
19. Zhao, L., et al., “Scalability of Cyber Twin-Based Security Systems in Large-Scale VANETs”