International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2(2) (2026)

ijerst.editor@gmail.com

editor@ijerst.com

ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

Multivariate Attack Identification in High-Mobility Vehicular Communication interpreted through Hybrid Stacking

K. Chiranjeevi[1], B. Poojitha[1], K. Balakrishna[1], N. Siva Nagamani[2]
[1]Assistant Professor, [2]Associate Professor, [1,2]Department of Computer Science and Engineering (AI & ML)
[1,2]Geethanjali Institute of Science and Technology, Nellore-Bombay Highway, S.P.S.R, Andhra Pradesh 524137, India

ABSTRACT
Vehicular Adhoc Networks (VANET) play a critical role in intelligent transportation systems by enabling real-time communication among vehicles and infrastructure. However, due to their highly dynamic topology, decentralized architecture, and high node mobility, VANET environments are vulnerable to multiple security threats such as Distributed Denial of Service (DDoS), Sybil, and Blackhole attacks. Existing traditional systems primarily rely on individual machine learning models for attack detection, which often struggle to handle multivariate attack scenarios and fail to adapt effectively to rapidly changing network conditions. These approaches suffer from limitations such as high false alarm rates, poor generalization, and reduced detection accuracy under varying traffic patterns. To address these challenges, there is a strong need for a robust and adaptive detection framework that can accurately identify multiple attack types while maintaining consistency across dynamic environments. The proposed system introduces a hybrid stacking-based model and also baseline classifiers like Gaussian Naïve Bayes (GNB) and Support Vector Machine (SVM) and K-Nearest Neighbors (KNN). The model leverages a Stacked Tree Alternating Optimization (TAO) Tree along with EDA-driven feature optimization to enhance detection performance. A meta-learning layer combines the outputs of base models to improve overall prediction stability and reduce misclassification. The system is further implemented as a Flask-based web application to enable real-time attack detection, monitoring, and visualization through an interactive interface. The proposed approach demonstrates improved precision, reduced false alarms, and strong adaptability across diverse VANET traffic conditions. This work highlights the significance of hybrid stacking techniques in strengthening VANET security and provides a scalable solution for secure and efficient intelligent transportation systems.

Key words: VANET security, DDoS detection, Sybil attack detection, blackhole attack detection, hybrid stacking model, anomaly detection. Machine Learning

1. INTRODUCTION

VANET or Intelligent Vehicular Ad-Hoc Networking provides an intellectual way of using vehicular Networking. With the sharp increase of vehicles on roads in the recent years, driving becomes more challenging and dangerous. Collision warning messages, road signal arms and on-site traffic views will provide drivers with the necessary tools to decide the best path along the way. VANET or smart car Ad-Hoc network provides a smart way to use car network. In recent years, with the rapid increase of vehicles on the road, driving has become challenging and dangerous. Security maintenance in VANET is an important critical issue, which has resulted lots of research and studies. It makes secured data transmission, movement of vehicles and confidentiality of vehicles in a VANET. Dummy messages transmitted by DDoS attackers jam the channel thus reduces the performance and efficiency of the network. DDoS attacks have become common in internet today. Even the traditional Intrusion Detection System are ineffective in countering distributed DoS attack and Sybil attack. Countering DDoS attacks is complex as it contains various level of networks, needs cooperation and trust among various domains.

Figure 1 presents a chronological overview of several high-impact Distributed Denial of Service (DDoS) attacks, mapping their attack volumes (Gbps) against their periods of occurrence. The visualization highlights how attack intensity has progressively increased over the years, beginning with the XOR botnet in July 2014, which generated traffic volumes around 200 Gbps. Subsequent attacks, such as BillGates in December 2015 and Kalten between April and June 2016, show a noticeable rise in magnitude, approaching and surpassing the 300–400 Gbps range. These attacks reflect the early stages of large-scale botnet evolution, during which attackers experimented with new amplification techniques and leveraged vulnerable devices to expand their attack capacity. The figure's most striking insight is the dramatic escalation seen in late 2016, particularly with the Mirai botnet attacks in September 2016, which exceeded 600 Gbps and marked a turning point in IoT-fueled cyber warfare. This unprecedented surge demonstrates how compromised smart devices enabled attackers to launch massive, distributed traffic floods with minimal resources.

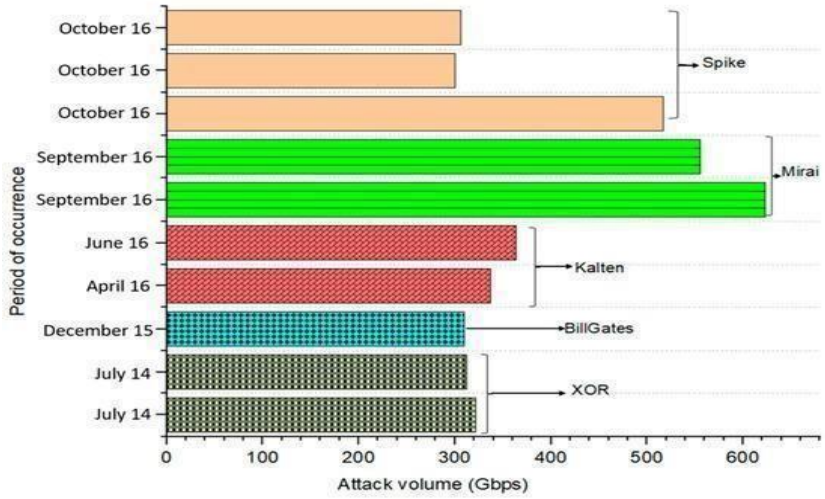


Figure 1: shows Timeline of majority of DDoS Attacks

Overall, the figure underscores the rapid evolution, sophistication, and amplification potential of modern botnets, emphasizing the urgent need for advanced detection and mitigation strategies in contemporary network infrastructures. In October 2016, the Spike botnet continued this trend, contributing multiple high-volume attacks that reinforced the growing severity of DDoS incidents.

2. LITERATURE SURVEY

Jayakrishna, et al. [1] proposed a hybrid selection strategy was introduced featuring an adaptive dragonfly algorithm (ADA) and an Enhanced grasshopper optimization algorithm (EGOA) for feature selection where the optimal features are determined. The experimental results show that VANET-DDoS Net++ surpasses other currently existing methodologies achieving 98.04% accuracy with 70% training data and 99.18% with 80% training data besides dramatically reducing false positive and negative rates as well as improving overall precision, F1-score, sensitivity, and specificity. The factor deals with the evolution of DDoS attacks whereas VANET networks offer a dynamic and secure intrusion detection and mitigation framework**.** Gayathri, et al. [2] proposed the Hybrid Deep Learning with Federated Learning (HDL-FL) framework, which leverages Convolutional Neural Networks (CNNs) to capture spatial and temporal traffic patterns. By utilizing Federated Learning, HDL-FL enables distributed, privacy-preserving training across RSUs and vehicles while reducing communication overhead. Experimental evaluations in simulated VANET environments show that HDL-FL achieves a 94% improvement in accuracy, a 30% reduction in false positives, and a 99% increase in attack detection rate while also reducing communication overhead by 6.5 s latency by 160 ms. Allafi, et al. [3] utilized the framework was designed specifically for edge-enabled VANET platforms. EXMAT combines the novel XGBoost classifier with custom-engineered behavioural features and post hoc explainability to provide accurate decisions directly at the vehicular edge. Experimental results show that the proposed model achieves an

overall classification accuracy of 95.78% with an almost perfect F1-score for standard behaviour samples of 99.98% and 94.36% for replay attacks. These results highlight EXMAT's ability to be applied in real-time vehicular networks, enhancing traffic safety and security against unknown cyberattacks. Anjali, et al. [4] Developed explainable Artificial Intelligence (XAI) techniques, particularly the Local Interpretable Model-Agnostic Explanations (LIME), were integrated to provide transparent and interpretable classification results. The model was trained and tested on approximately 400,000 real-time data traces, including both normal and attack scenarios, generated using simulation tools such as SUMO, OMNET+ +, and Python 3.19. Experimental results demonstrate that the proposed method significantly outperforms existing deep learning techniques, achieving a detection accuracy of 99.6%, a precision of 99.2%, and a recall of 99.4%. Nayak, et al. [5] Proposed a two-phase detection framework, in which the first phase utilizes cosine similarity and weighting factors to identify attack misbehaviour in vehicles. These metrics contribute to the calculation of effective node trust (ENT), which helps in further attack detection. In the second phase, deep learning (DL) models such as CNN and LSTM are employed for further granular classification of misbehaving vehicles into normal, fault, or Sybil attack vehicles. The proposed schemes demonstrate superior accuracy with an average of 94.49% to 99.94%, surpassing the performance of existing methods.

Ali, et al. [6] Proposed an innovative approach based on clustering and digital signature (CDS) to prevent black hole attack on reactive routing, i.e., ad-hoc on demand distance vector (AODV) and dynamic source routing (DSR) of VANET. The proposed approach was implemented and evaluated in SUMO-0.32.0 and NS-3.24.1 simulators. Elsadig, et al. [7] Utilized two layers of enhancements were applied—using a suitable feature selection technique and fixing the dataset imbalance problem. The results show that the proposed model, which is based on the Random Forest (RF) classifier, achieved excellent performance in terms of classification accuracy, computational cost, and classification error. It achieved an accuracy rate of 99.8%, outperforming all benchmark classifiers, including AdaBoost, decision tree (DT), K-nearest neighbours (KNNs), and multi-layer perceptron (MLP). To the best of our knowledge, this model outperforms all the existing classification techniques. In terms of processing cost, it consumes the least processing time, requiring only 69%, 59%, 35%, and 1.4% of the AdaBoost, DT, KNN, and MLP processing times, respectively. It causes negligible classification errors. Shobana, et al. [8] Proposed a novel hybrid model, GBiL, integrating gated recurrent unit (GRU) and bidirectional long short-term memory (BiLSTM) to detect and mitigate such attacks. At the core of this architecture, an intrusion detection system (IDS) is combined with a trust detection module to assess the trustworthiness of network nodes using real-time data. he proposed GBiL model achieves high performance, with an accuracy of 96.01% and a false alarm rate of just 0.04%. Hayouni, et al. [9] developed a HyDra-VANET, a novel hybrid security framework that integrates deep learning, federated learning, and homomorphic encryption for robust and privacy-preserving intrusion detection. At the vehicle level, a convolutional–recurrent neural network (CRNN) was employed to extract both spatial and temporal patterns from real-time vehicular communication and telemetry data, ensuring accurate anomaly detection. Shameer, et al. [10] utilized three models incorporating both internal and external hostile nodes. Using a deep learning-based Multilayer Perceptron (MLP) trust evaluation system, black hole assaults were detected through network metrics implementation, packet delivery ratio, latency, throughput, and power utilization. This study presents significant outcomes, including Packet Delivery Ratio (PDR) of 94.44% and throughput of 87,406.38 bps, comparable to scenario SII, which achieved a PDR of 69.23% and a throughput of 2,463.33 bps using a deep learningbased trust system concurrently with IoT network performance, particularly in the presence of core and outward blackhole occurrences.

Yadav, et al. [11] developed a model within Black hole attack, the attacker vehicle, at the time of routing represents itself with the smallest and most desired route to the destination and hence communication with other legitimate nodes starts with this attacker node. Now the attacker vehicle can drop all the packets or send the information to other malicious vehicles. In Sybil attack the malicious vehicle sends

fake alert message of high traffic to RSU and then RSU alerts other vehicles on the road of false high traffic with the intention of a malicious vehicle. Abdallah, et al. [12] introduced to create a method for identifying blackhole attacks through anomaly detection techniques utilizing Support Vector Machines (SVM). Our detection system looks at node activity to scan network traffic for irregularities. In blackhole scenarios, the attackers exhibit distinct behavioural characteristics that distinguish them from other nodes. This can be efficiently detected by the proposed SVM-based detection system. The proposed detection system is designed to analyse network traffic and identify anomalies by examining node behaviours. The results indicate that ADS-SVM outperforms the other methods with a detection accuracy of 99.96%, surpassing the 99.2% achieved by J48 classifier and the 96.5% achieved by NB classifier. Jasim Mohammed, et al. [13] introduced a new approach to detect black hole attacks through anomaly detection techniques using response generation time and machine learning models is proposed. It continuously monitors the activities of nodes and examines and analyzes realtime network traffic, and uses machine learning algorithms to identify behavioural characteristics, irregularities, and abnormal activities and differentiate them from other nodes. Analysis of the results of the nightshades shows increased accuracy in detecting black hole attacks and ensuring the security of mobile Ad-hoc networks. This approach not only helps to detect attacks faster, but also increases the overall efficiency of the system. Sumit, et al. [14] proposed seeks to achieve the goal of ensuring safe and effective interaction between vehicles participating in VANETs by dynamically determining the optimal path for the exchange of data. A chaotic protect multi-verse optimization approach is used to generate several random sequences from which the most secure route may be selected. This is done to enhance the security of the VANET transmission network during transmission. The results of the trials indicate that the suggested technique is more successful in avoiding MITM and improving the functioning of VANET connections in settings that are characterized by intelligent cities. Ravindran, et al. [15] utilized Fuzzy Logic-based Intrusion Detection System with Hidden Markov Model (FIDS-HMM) is proposed to identify the malicious nodes and mitigate the black hole attack. Moreover, an HMM is employed in the proposed protocol to monitor the energy levels of the nodes in order to detect the malicious nodes effectively. The implementation of the proposed protocol is carried out by using NS2 simulator. Simulation results justify the proposed protocol namely FIDS-HMM provides an efficient detection mechanism for black hole attacks in the network. Moreover, the proposed protocol improves the Quality of Service (QoS) parameters, namely packet delivery ratio, delay, and throughput in the network with efficiency.

3. PROPOSED SYSTEM

The proposed system as illustrated in Figure 2 introduces a hybrid stacked Tao Tree classifier for multivariate detection of DDoS, Sybil, and Blackhole attacks in high-mobility VANETs by utilizing a comprehensive vehicle-level dataset containing network, mobility, trust, and attack-related attributes. The system begins with structured data collection from nodes, followed by advanced preprocessing to clean, normalize, and prepare the data for analysis. Through EDA, key behavioural patterns and anomalies are observed, and data balancing is achieved using SMOTE-Tomek to handle class imbalance. Existing baseline models such as KNN, GNB, and SVM are implemented for comparison, while the proposed stacked Tao Tree classifier combines strengths of multiple learners to improve detection accuracy and robustness. The model is then evaluated through performance comparison, integrated with a Flask interface for real-time classification, and finally provides attack category predictions from test data for efficient VANET security monitoring.

Step 1: Dataset: The dataset is constructed using node-level features that reflect mobility, communication behaviour, and trust characteristics of vehicles in VANETs. Each record contains node id, position coordinates, speed, direction, acceleration, packet transmission statistics, packet drop ratio, latency, retransmission count, signal strength, trust metrics, and recorded attempts of blackhole, Sybil, and denial-of-service attacks. These attributes provide a multivariate representation that supports accurate classification of different attack types.

Step 2: Data Preprocessing: Data preprocessing begins with cleaning missing values, handling null trust scores, correcting inconsistent node positions, and removing impossible values such as negative speeds or abnormal coordinates. Scaling is applied to mobility and network features to maintain uniformity. Categorical fields are encoded using suitable encoding techniques, and noise is removed through outlier detection using statistical thresholds. The dataset is reorganized into feature matrices and target labels that support supervised classification for multiple attack behaviours.

Step 3: Exploratory Data Analysis (EDA): EDA is performed to study distributions, correlations, and behavioural deviations across all features. Scatter plots of position, histograms of packet drop ratio, heatmaps of trust metrics, and trend analysis of signal strength help identify hidden patterns. Attack attempts are examined to understand frequency and relation with node behaviour. This analysis highlights key discriminating features for later model performance improvement.

Step 4: SMOTE Tomek Data Balancing: Due to highly imbalanced attack categories, SMOTE Tomek is applied to generate synthetic minority samples while removing Tomek links that cause overlap between classes. This technique ensures a clean decision boundary and balanced class distribution. The resulting dataset becomes more suitable for training robust models and avoids bias toward majority attack types.

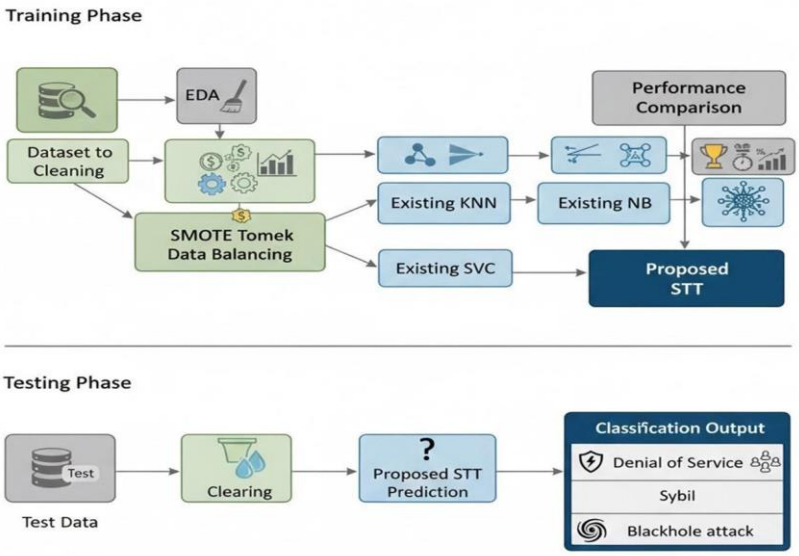


Figure 2 System Architecture

Step 5: Existing KNN Classifier: The KNN classifier is trained using the balanced dataset where each instance is classified based on the k-nearest neighbours in feature space. Distancebased voting determines the final predicted attack label. KNN serves as a baseline algorithm to measure effectiveness of the proposed stacked model.

Step 6: Existing Naive Bayes: Naive Bayes is applied under the assumption of conditional independence among features. Probabilistic distributions of mobility, trust, and packet features are used to compute class likelihood. Despite its simplicity, Naive Bayes provides a fast and interpretable benchmark for attack detection experiments.

Step 7: Existing Support Vector Machine: SVM is trained with nonlinear kernels to identify complex boundaries between normal and attack classes. It separates the high dimensional feature space using margins and support vectors. This existing model acts as another comparison point for evaluating improvement achieved by the proposed classifier.

Step 8: Proposed Stacked Tao Tree Classifier: The proposed model integrates multiple decision-tree-based learners in a stacked architecture, where predictions from base learners are fed into a meta-level Tao Tree classifier. This stacking strategy combines strengths of diverse trees, captures nonlinear interactions among network and mobility features, and improves multivariate attack detection.

The final model offers enhanced accuracy, reduced false alarms, and stronger generalization in high-mobility environments.

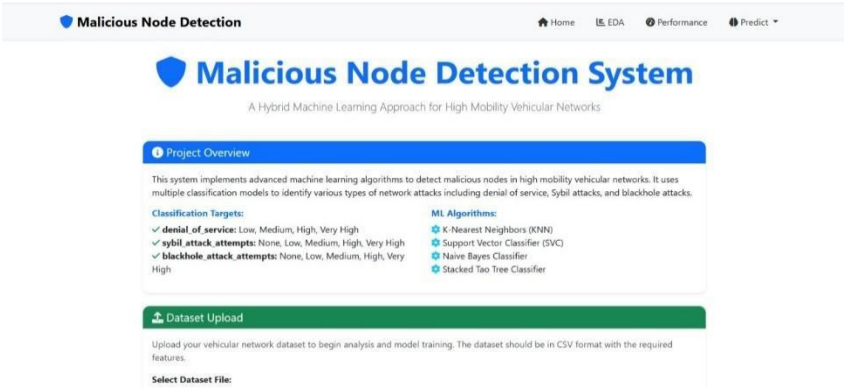
Step 9: Performance Comparison: All classifiers including KNN, Naive Bayes, SVM, and the proposed stacked Tao Tree model are evaluated using accuracy, precision, recall, F1-score, and confusion matrices. Comparison demonstrates that the hybrid stacked model outperforms existing methods by achieving better detection for blackhole attack attempts, sybil attack attempts, and denial of service events.

Step 10: Prediction from Test Data: Test data is passed through the trained pipeline where preprocessing, scaling, and model inference are applied to generate predictions. The final classification output identifies the attack category based on input node behaviour patterns, providing results in the form of attack labels for each test instance.

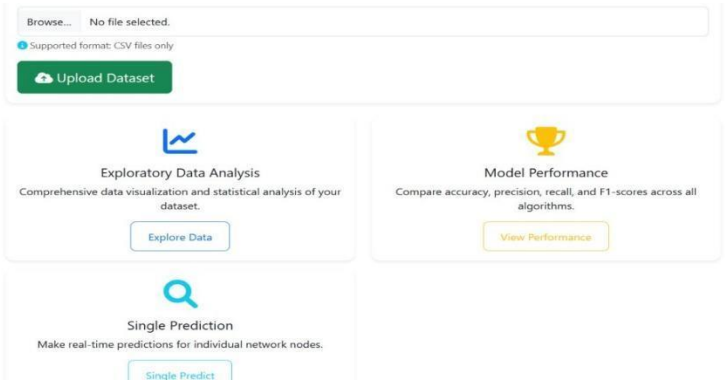
Step 11: Integration with Flask: The trained hybrid stacked model is deployed into a Flask web application enabling real-time detection. User input or uploaded test files are processed through API routes, and the application displays the final attack classification. This integration allows practical use of the model in a simulation dashboard or VANET security interface.

4. Result Analysis

Figure 3 shows the images depict the home dashboard of a Malicious Node Detection System. It is a web-based platform designed to detect malicious nodes in vehicular networks using machi ne learning. The interface highlights a project overview explaining attack types like DoS, Sybil, and blackhole attacks. Multiple ML algorithms such as KNN, SVC, Naive Bayes, and ensemble models are listed. A dataset upload section allows users to submit CSV files for analysis and training. Dedicated cards provide access to exploratory data analysis and model performance evaluation. A single prediction feature enables real-time prediction for individual nodes. A "Getting Started" section guides users through uploading data, training models, and making predictions.



(a)



(b)

Figure 3 Home Page (a) primary (b) secondary

Figure 4 presents the confusion matrix for DDoS attack detection using the STT model, showing perfect classification performance across all classes. All samples are correctly positioned along the diagonal, indicating zero misclassification. The model accurately detects 406 Normal, 201 Medium, 193 High, and 200 Very High instances without any errors. This reflects exceptional accuracy and strong class discrimination capability. The absence of false positives and false negatives highlights the reliability of the model. It also indicates that the learned features effectively capture variations in attack intensity. Such performance demonstrates the model's robustness in handling multi-class attack scenarios.

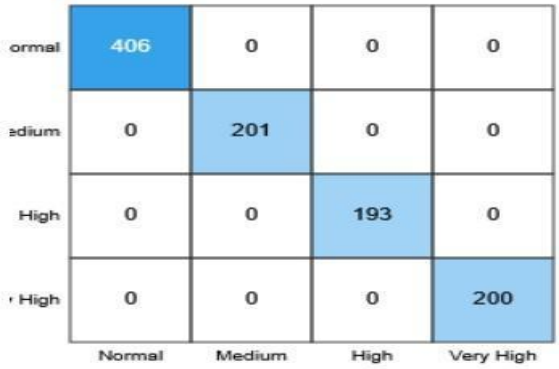


Figure 4: DDoS Confusion Matrix for STT Model

Figure 5 illustrates the confusion matrix for Sybil attack detection, showing near-perfect classification performance. The model correctly identifies 333 Normal, 334 Low, and 332 Medium samples with high accuracy. Only one Normal instance is misclassified as Low, while all other predictions are correct. This minimal error indicates strong precision and recall across the classes. The confusion matrix shows clear separation between different attack levels. It also reflects the model's ability to generalize effectively across similar patterns. The low misclassification rate demonstrates stable and reliable performance.

Figure 6 shows the All instances are correctly classified along the diagonal with values of 195 (Normal), 207 (Low), 195 (Medium), 201 (High), and 202 (Very High), while all offdiagonal elements are zero. This indicates zero misclassification across all attack levels, demonstrating the superior capability of the Stacked Tao Tree (STT) model in learning discriminative features and accurately identifying Blackhole attacks with 100% precision and recall.

Figure 7 shows the test data input interface used for attack detection, where node-specific parameters related to position, movement, and network behaviour are provided. In this example, the node ID is 1, with position coordinates X = 374.54 and Y = 393.64, a speed of 11.21, direction 179.88°, and acceleration 1.38. Network metrics include 459 packets sent, 227 packets received, a packet drop ratio of 0.51, latency of 83.30 ms, and a message retransmission count of 9, representing realistic node activity conditions used for evaluating attack behaviour.

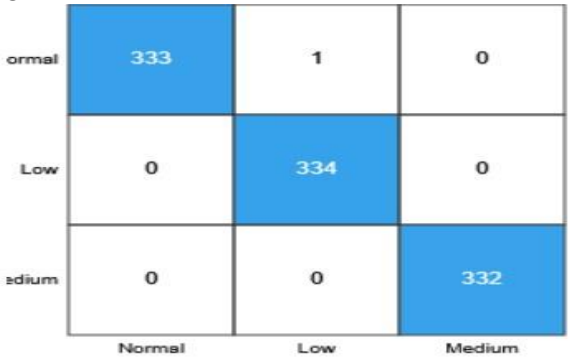


Figure 5: Sybil Confusion Matrix for STT Model

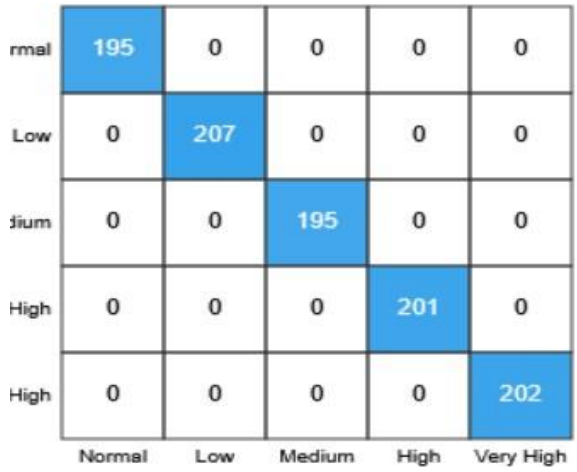


Figure 6: Black hole Confusion Matrix for STT Model

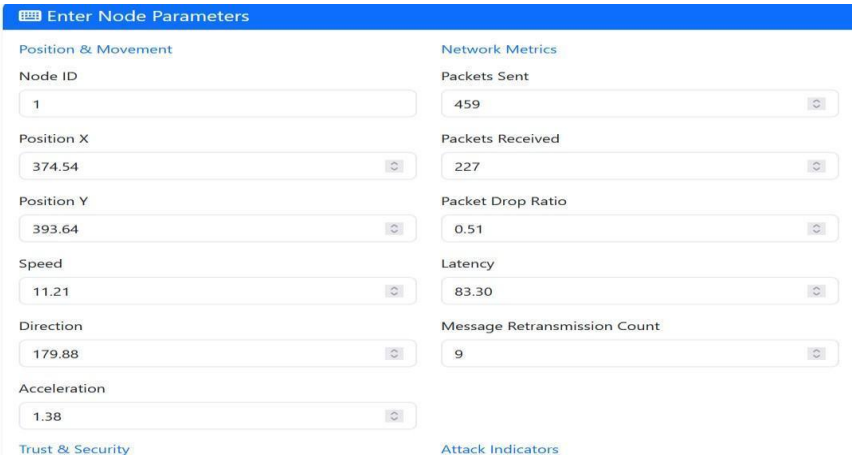


Figure. 7: Test Data Input

Figure 8 shows the corresponding prediction results generated by different classifiers for the given test input. For Denial of Service (DoS) detection, KNN predicts Level 0, SVC predicts Level 1, while NB and STT classify the attack as Level 2. In the case of Sybil attack attempts, KNN and NB identify Level 1, whereas SVC reports Level 2 and STT confirms Level 1. For Blackhole attack attempts, KNN indicates Level 1, while SVC, NB, and STT consistently detect a higher severity at Level 3. These results demonstrate how the stacked model aligns closely with stronger attack severity predictions compared to individual classifiers.

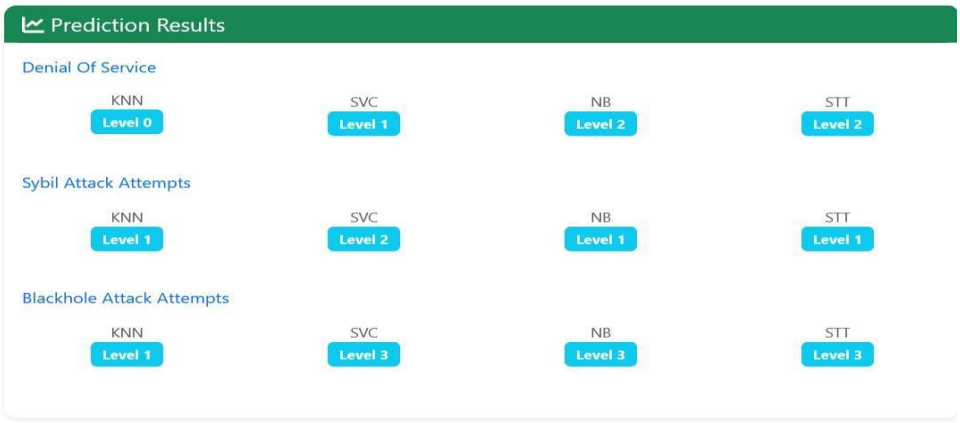


Figure 8: Prediction Results

Table 1 shows the image presents the Denial of Service (DoS) classification results comparing four machine learning algorithms: K-Nearest Neighbours (KNN), Support Vector Classifier (SVC), Naive

Bayes (NB), and the Stacked Tao Tree (STT) classifier. The traditional classifiers—KNN, SVC, and NB—exhibit relatively low and comparable performance, with accuracies ranging from 26.20% to 29.00%, precision between 28.58% and 29.81%, recall from 26.20% to 29.00%, and F1-scores below 30%, indicating limited effectiveness in DoS attack detection. In contrast, the proposed Stacked Tao Tree classifier significantly outperforms all others, achieving 100% accuracy, precision, recall, and F1-score, clearly demonstrating its superior capability and robustness for reliable and accurate DoS attack detection

Table 1: DDoS Classification Results

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
K-Nearest Neighbours	26.20	29.14	26.20	26.70
Support Vector Classifier	29.00	29.81	29.00	29.27
Naive Bayes	26.20	28.58	26.20	26.53
Stacked Tao Tree Classifier	100.00	100.00	100.00	100.00

Table 2 illustrates the Sybil attack attempts classification results for four algorithms: KNearest Neighbours (KNN), Support Vector Classifier (SVC), Naive Bayes (NB), and the Stacked Tao Tree (STT) classifier. Among the conventional methods, KNN achieves an accuracy of 35.70%, precision 35.39%, recall 35.70%, and F1-score 34.65%, while SVC shows slightly lower performance with 33.80% across accuracy, recall, and F1-score. Naive Bayes performs marginally better than KNN with 35.60% accuracy, 35.93% precision, 35.60% recall, and 35.05% F1-score. In contrast, the proposed Stacked Tao Tree classifier demonstrates nearperfect performance, achieving 99.90% accuracy, precision, recall, and F1-score, clearly highlighting its effectiveness and robustness in accurately detecting Sybil attack attempts compared to traditional classifiers.

Table 2: Sybil Attack Classification Results

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
K-Nearest Neighbours	35.70	35.39	35.70	34.65
Support Vector Classifier	33.80	33.84	33.80	33.80
Naive Bayes	35.60	35.93	35.60	35.05
Stacked Tao Tree Classifier	99.90	99.90	99.90	99.90

Table 3 presents the blackhole attack attempts classification results using four different algorithms: K-Nearest Neighbours (KNN), Support Vector Classifier (SVC), Naive Bayes (NB), and the Stacked Tao Tree (STT) classifier. The traditional classifiers show relatively low detection performance, with KNN achieving 19.90% accuracy, 19.80% precision, 19.90% recall, and an F1-score of 19.43%, while SVC performs similarly with 19.40% accuracy, 19.51% precision, 19.40% recall, and 19.37% F1-score. Naive

Bayes shows a slight improvement, reaching 21.70% accuracy, 21.66% precision, 21.70% recall, and a 20.08% F1score. In contrast, the proposed Stacked Tao Tree classifier significantly outperforms all other models, achieving a perfect 100% accuracy, precision, recall, and F1-score, clearly demonstrating its superior capability in accurately detecting blackhole attack attempts.

Table 3: Blackhole Attack Classification Results

Algorithm	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1 Score (%)**
K-Nearest Neighbours	19.90	19.80	19.90	19.43
Support Vector Classifier	19.40	19.51	19.40	19.37
Naive Bayes	21.70	21.66	21.70	20.08
Stacked Tao Tree Classifier	100.00	100.00	100.00	100.00

5. Conclusion

The experimental analysis demonstrates the effectiveness of the proposed attack detection framework using multiple classifiers and a Stacked Tao Tree (STT) model. Based on the test input values (Node ID 1 with position X = 374.54, Y = 393.64, speed 11.21, packet drop ratio 0.51, latency 83.30 ms, and 9 message retransmissions), the system was able to clearly identify and classify different network attacks. For Denial-of-Service detection, the individual classifiers produced varying severity levels (KNN: Level 0, SVC: Level 1, NB: Level 2), while the STT model consistently identified Level 2, indicating a more reliable aggregation of predictions. Similar trends were observed for Sybil and Blackhole attacks, where STT aligned with higher and more consistent severity levels, particularly detecting Level 3 for Blackhole attacks, highlighting its robustness in capturing malicious behaviour under adverse network conditions. Furthermore, the comparative performance evaluation across DoS, Sybil, and Blackhole attack scenarios confirms that traditional classifiers such as KNN, SVC, and Naive Bayes exhibit limited detection capability, with accuracy and F1-scores often below 40% for complex attacks like Blackhole and Sybil. In contrast, the STT classifier achieved near-perfect or perfect performance, with 99.9%–100% accuracy, precision, recall, and F1-score across all attack types. These results validate the effectiveness of the hybrid stacking approach in handling multivariate network data and improving attack detection accuracy, making it suitable for deployment in dynamic and security-critical network environments.

REFERENCES

[1] Jayakrishna, Naramalli, and N. Narayanan Prasanth. "A hybrid deep learning model for detection and mitigation of DDoS attacks in VANETs." Scientific Reports 15, no. 1 (2025): 34170.

[2] Gayathri, T., S. Uma Maheswari, S. Ponni Alias Sathya, T. Satyanarayana Murthy, and Pramoda Patro. "Machine Learning-Enhanced DDoS Attack Detection and Mitigation in VANET Infrastructure." Transactions on Emerging Telecommunications Technologies 36, no.10 (2025): e70262.

[3] Allafi, Randa, Amnah Alshahrani, Munya A. Arasi, Hussain Alshahrani, Mohammed A. AlAqil, Rana Alabdan, Ibrahim Zalah, and Rowida Mohammed Alharbi. "Explainable Machine Learning Framework for Real-Time Multi-Attack Threat Detection in EdgeEnabled VANET Environments." Transactions on Emerging Telecommunications Technologies 36, no. 10 (2025): e70283.

[4] Anjali, Thuvva, Rajeev Goyal, and G. N. Balaji. "X-GEVON-a novel explainable intelligent network to detect the multiple attacks in vanet systems." Discover Computing 28, no. 1 (2025): 185.

[5] Nayak, Rajendra Prasad, Sourav Kumar Bhoi, Kshira Sagar Sahoo, Srinivas Sethi, Subasish Mohapatra, and Monowar Bhuyan. "Unveiling Sybil Attacks Using AI-Driven Techniques in Software-Defined Vehicular Networks." Security and Privacy 8, no. 1 (2025): e487.

[6] Ali, Shahjahan, Parma Nand, and Shailesh Tiwari. "An innovative approach based on clustering and digital signature to prevent black hole attack from vehicular ad-hoc network." International Journal of Communication Networks and Distributed Systems 31, no.2 (2025): 221-249.

[7] Elsadig, Muawia A., Abdelrahman Altigani, Yasir Mohamed, Abdul Hakim Mohamed, Akbar Kannan, Mohamed Bashir, and Mousab AE Adiel. "Connected Vehicles Security: A Lightweight Machine Learning Model to Detect VANET Attacks." World Electric Vehicle Journal 16, no. 6 (2025): 324.

[8] Shobana, G., A. Thillai Nathan, Dhev Sabharish Sivakumar, and R. Arockia Xavier Annie."GBiL: A hybrid gated recurrent units (GRU) and bidirectional long short-term memory (BiLSTM) model with Particle Swarm Optimization for a Robust VANET IDS." EURASIP Journal on Wireless Communications and Networking 2025, no. 1 (2025): 57.

[9] Hayouni, Haythem. "Enhancing VANET Security Using a Hybrid Model of Deep Learning and Homomorphic Encryption." Security and Privacy 8, no. 6 (2025): e70109.

[10] Shameer, M., and P. Rutravigneshwaran. "Impact Analysis of Malicious IoT Node Placement for Blackhole Attack Detection and Mitigation using Deep LearningBased Trust Evaluation." Indian Journal of Science and Technology 18, no. 32 (2025): 2581-2593.

[11] Yadav, Dhananjay, and Nirbhay Kumar Chaubey. "Detection and Prevention of Black Hole Attack and Sybil Attack in Vehicular Ad Hoc Networks." In International Conference on Computing Science, Communication and Security, pp. 176-189. Cham: Springer Nature Switzerland, 2024.

[12] Abdallah, Ashraf Abdelhamid, Mahmoud S. Abdallah, Heba Aslan, Marianne A. Azer Abdallah, Young-Im Cho, and Mohamed S. Abdallah. "Enhancing Mobile Ad Hoc Network Security: An Anomaly Detection Approach Using Support Vector Machine for Black-Hole Attack Detection." International Journal of Safety & Security Engineering 14, no. 4 (2024).

[13] Jasim Mohammed, Fatimah, Azam Andalib, Hossein Azgomi, and Seyed Ali Sharifi. "Enhancing the Security of Mobile Ad-hoc Networks: A Black Hole Attack Mitigation Approach Using Response Time and Machine Learning Models." Journal of Industrial and Systems Engineering 17, no. 1 (2025): 204-216.

[14] Sumit, Rajender Singh Chhillar, Sandeep Dalal, Surjeet Dalal, Umesh Kumar Lilhore, and Sarita Samiya. "A dynamic and optimized routing approach for VANET communication in smart cities to secure intelligent transportation system via a chaotic multi-verse optimization algorithm." Cluster Computing 27, no. 5 (2024): 7023-7048.

[15] Ravindran, Selvi. "Intelligent fuzzy logic based intrusion detection system for effective detection of black hole attack in WSN." Peer-to-Peer Networking and Applications 17, no. 4 (2024): 1813-1829.