CHAPTER 4

RESULTS AND DISCUSSION

This chapter comprehensively analyzes the proposed hybrid approach to secure VANET against DoS attacks and their different types. The efficacy of the integrated self-healing and immunization mechanisms in mitigating the impact of various DoS attacks is rigorously evaluated. The results obtained through extensive simulations and experiments are presented, along with a detailed discussion of their implications for VANET security.

This chapter primarily assesses the performance of the proposed approach by analyzing key metrics such as packet delivery ratio, delay, energy consumption, detection rate, false positive rate, packet loss, and routing overhead. Through comparative analysis with existing methodologies, this chapter seeks to prove that the proposed approach significantly enhances both the security and resilience of VANET. The hybrid approach proposed has been assessed based on its performance in mitigating DoS attacks and its types with self-healing trust based immunized approach with routing.

4.1 Experimental Setup and Results

The assumptions prevailed during the implementation of the proposed work are listed below:

i. The VANET area is partitioned into distinct domains (clusters), with each domain overseen by a dedicated Roadside Unit (RSU) responsible for managing group communication.

ii. In a V2I communication model where communication occurs solely through the RSU (Roadside Unit). Within each group, vehicles utilize the IEEE 802.11p standard for wireless access in vehicular environments to exchange communications with the designated RSU, employing the Ad-hoc On-demand Distance Vector (AODV) routing protocol.

iii. RSUs communicating using technologies can exchange information indirectly through a central entity known as the Regional Trusted Authority (RTA).

iv. It is assumed that all RSUs, RTAs, and the Trusted Authority (TA) are inherently resistant to attacks.

v. Furthermore, each node (vehicle or RSU) are dynamically updated based on security features on a regular basis.

The initial step considered the dataset CIC - IDS 2018 for the feature selection and for the enhanced mitigation with further steps, the dataset considered is CIC – DDoS2019. The CIC – DDoS2019 (The 2019 Canadian Institute for Cyber security – Intrusion Detection Systems Evaluation Dataset) focusing on cyber security aspects. The dataset likely contains information on the attack patterns through network traffic characteristics.

The CIC - IDS 2018 dataset included information of attacks relating to VANET communications like DoS, DDoS and Botnet. The network traffic characteristics are the features that differentiate malicious traffic from legitimate traffic.

The features included are:

i. Packet length
ii. Flow Lifetimes
iii. Endpoints IP
iv. Protocol information
v. Flags and timestamps

The performance of the VANET on implementing the hybrid approach is assessed in this environment. The following sections illustrate the datasets and the performance of the hybrid approach.

4.1.1 Dataset and Simulation

The dataset CIC-IDS 2018 is considered to include the traffic with attacks during the simulation of VANET. The three-phase methodology having the initial approach featuring phase 1 uses feature selection for malicious nodes detection. In phase 1, the proposed optimized feature selection technique, coupled with the classifier, was implemented within a simulated environment utilizing SUMO and OMNET++, and

validated using the CIC-IDS 2018 dataset. Approximately 1500 data points were collected and utilized in the proposed algorithm. DoS and Botnet attacks are considered for the detection. The simulation related to the CIC-IDS 2018 dataset is exhibited in the following subsection.

The enhanced feature selection for malicious nodes detection and mitigation against DoS attacks featuring phase 1 is implemented considering different types of DoS attacks from the CIC-DDoS2019 dataset. CIC-DDoS 2019 closely resembles real-world network traffic by including both benign traffic and up-to-date, common DDoS attacks (PCAPs). The analysis report on network traffic involved the categorization of network traffic flows. The dataset includes a diverse range of current reflective DDoS attacks encompassing PortMap, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag, SYN, NTP, DNS, and SNMP attacks. The 12 variants of DDoS attacks are considered for detection by the proposed approach.

The secondary objective 1 is to detect and classify DoS attacks with improved accuracy of detection and classification, recall, precision, minimum delay through optimizing the features. Contribution 1 successfully integrated the Glow-worm Swarm Optimization (GLW) technique with a Single Layer Feed Forward Neural Network (SLFN) classifier. Real-time scenarios were simulated using the SUMO software to evaluate the performance of this integrated approach. Microscopic traffic simulators model the movement of individual vehicles on a road network. By considering factors like vehicle characteristics and road conditions, these simulators determine the position of each vehicle at any given time ('t'). The obtained positional data can be effectively visualized through a graphical user interface (GUI) or alternatively recorded in a file (dump file) for later analysis. Figures 4.1 and 4.2 illustrate the diverse scenarios that can arise within vehicular systems.

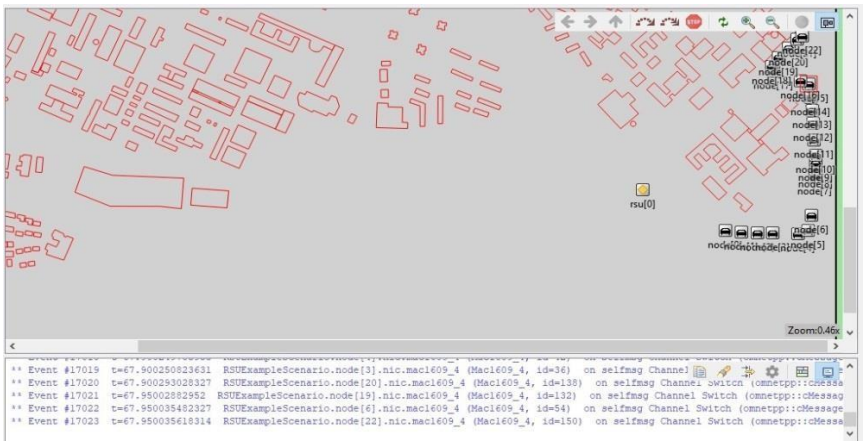

Figure 4.1: Distinct Scenarios of Vehicular Systems

SUMO combined with the OMNET collected data in real time under ordinary circumstances. Attack detection is considered by incorporating CIC-IDC2018 datasets. The collected data in the execution of the proposed algorithm included initial locations, characteristics of the vehicle namely, acceleration, maximum speed and direction, road network, ways, destination, and speed limit.

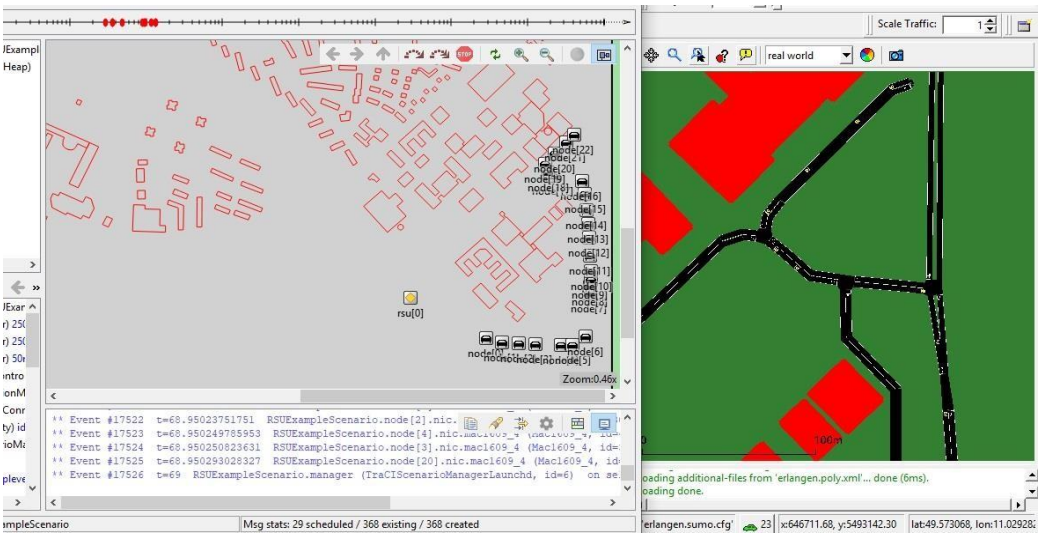

Figure 4.2: Four Lane /Two Lane Road System

SUMO (Lu S et al., 2016) is a simulator for car-following model (issue of Krauss, S et al, 1998, Wagner, P et al., 2003, Kerner, B.S et al., 2009, Treiber et al., 2000). The road side scenarios, created using SUMO, were subsequently simulated as nodes within the OMNET++ environment. The parameters created by SUMO is listed in Table 4.1.

Table 4.1: Parameters List in SUMO

S.No.	List of Parameters	Specifications
1	No of vehicles	100
2	Speed	35-40 km/hr
3	Direction	Bi directional
4	Type of roads	Two-lane /Four Lane Roads
5	Network used	IPv6
6	No of attacks used	2

The node creation in OMNET++ Environment and the parameters are recorded in Table 4.2.

Table 4.2: List of the Features Calculated for the Vehicular Systems

S.No.	List of parameters	Specifications
1	No of TCP packets Transmitted	8 bytes
2	No of TCP Packets Received	8 bytes
3	Speed of the vehicles	35-40km/hr
4	Signal Strength	-10 to 25 dbm
5	Latency	2 ms
6	Direction	Omni direction
7	Throughput	40-80
8	Time Stamp	4 ms
9	Input Message ID	ID1
10	Layer ID	ID2

The above experimental set up has been established with the features optimized with the proposed algorithm. The algorithm considered the features calculated for the detection and prediction of DoS attack. The features considered are

- No. of TCP packets transmitted

  This feature identifies abnormal traffic patterns, such as a sudden high TCP packets transmitted from a particular IP address. This could be a sign of a DoS attack.

- No. of packets received

  This feature identifies abnormal traffic patterns, such as a sudden decline in the packets received by a particular IP address.

- Signal Strength

  This feature identifies areas with poor signal strength, which can lead to dropped packets and decreased performance. It can also be used to identify devices with weak signal strength, which may be more susceptible to attacks.

- Latency

  This feature identifies network congestion and used to identify devices with high latency more susceptible to attacks.

- Speed of the vehicles

  This feature identifies vehicles that are moving too fast or too slow for traffic conditions. This could be a sign of a reckless driver or a vehicle that has been stolen.

- Direction

  This feature identifies vehicles that are traveling in the wrong direction. This could be a sign of a lost driver or a vehicle that is trying to evade law enforcement.

- Throughput

  This feature identifies network bottlenecks and other performance problems. It can also be used to identify devices that are generating a lot of traffic, which may be a sign of an attack.

- Time stamp

  This feature identifies the time and date of network traffic events. This information can be used to correlate events from different sources and to track the progress of attacks.

- Input Message ID

  This feature recognizes the specific message that is being communicated over the network. This information can be used to identify the type of traffic and to track the progress of applications.

- Layer ID

  This feature identifies the layer of the network stack at which the traffic is being transmitted. This information can be used to identify the type of traffic and to troubleshoot network problems.

The ten features collected from the scenario are optimized on selection to five features by the fitness function. The features are the inputs to the SLFN classifier for attack detection and classification. A sample of five features with the values is listed with attacks in Table 4.3.

Table 4.3: Input Features of SLFN Classifier

No. of Packets Transmitted	No. of Packets Received	Throughput (Mbps)	Latency (ms)	Time of Arrival to OBU (ms)	Layer ID	Msg ID	Label	Label Details
5	5	48	0.7	0.45	186	457	0	Normal
5	5	62	0.8	0.458	174	427	0	Normal
5	5	25	0.3	0.459	60	138	0	Normal
5	5	60	0.5	0.45	66	153	0	Normal
5	5	46	0	0.45	30	63	0	Normal
5	5	49	0.1	0.45	42	93	0	Normal
5	5	8	3.2	0.78	36	78	2	Botnet
5	5	29	4	0.45	36	525	0	Normal
5	5	46	0	0.457	84	547	0	Normal
5	0	7	5	0.88	101	496	1	DOS
5	0	9	5.6	0.90	107	498	1	DOS
5	0	5	10	0.92	113	500	1	DOS
5	0	7	12	0.94	119	502	1	DOS
5	0	7	17	0.96	125	504	1	DOS
5	0	9	25	0.98	131	506	1	DOS
5	0	5	6.7	0.95	137	514	1	DOS
5	0	64	0.2	0.50	66	153	0	Normal

The features labeled as in Table 4.3 are fed as inputs to the classifier consisting of seven input layers and as the output is based on the normal traffic, botnet or DoS attacks, the output layers are fixed as three based on the detection and prediction of attacks. This setup implementedfor the DoS and Botnet attacks detection.

```
File  Edit  View  Search  Terminal  Help
Build commands will be stored in build/compile_commands.json
'build' finished successfully (7.043s)

0

Time+2.85714e+06ns

Number of Bits1.0752e+06

Deviation Loss-160

0
vehicle density-3.09658e+09
************************************
Total Sent Packet=10000
************************************
Total Received Packet=9990
************************************
Duration    : 0Seconds
************************************
transmitted bits : 1000000bits
************************************
received bits : 999000bits
************************************
Throughput    : 9.52721 Mbps
************************************
Avereage End to End Delay = -0.01001ms
************************************
Average Packet Delivery Fraction = 0.999
************************************
Percentage OF Packet loss = 0.0999987%
```

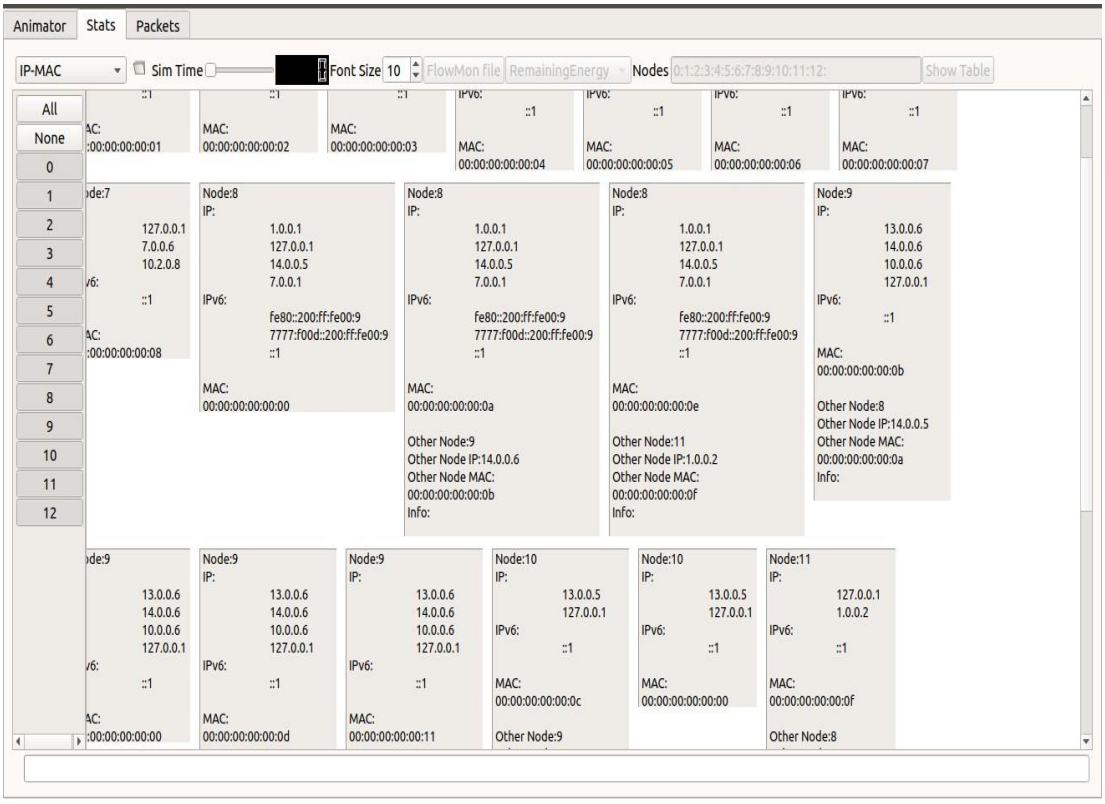

Figure 4.3: Simulation results of the proposed approach

The need to select the features based on various DoS attacks and to detect for further mitigation arises. Adaptive feature selection algorithms can adapt to the dynamic nature of VANET by continuously updating the selected feature subset as the network changes. Enhanced feature selection algorithms that use adaptiveness in feature selection are able to maintain accurate DDoS attack detection even in highly dynamic VANET.

The features considered in the enhanced proposed approach are 80 and the features are tabulated with their description. From the 80 features, the proposed approach selected the features pertaining to the DoS attacks as per the CIC-DDoS2019 dataset values and fed into the proposed methods for detecting and isolating the nodes with such maliciousness in the simulated VANET.

The integration of the proposed Response Feedback algorithm and micro-cluster outlier detection with linear regression is utilized for the identification of attacks during data communication. The model incorporates temporal information, considering a variable speed range influenced by factors such as data transmission delays, response times between the RSU and vehicles, packet deviation and loss rates, and the relative speeds and positions of vehicles. Figure 4.3 presents the simulation results encompassing metrics such as loss of deviation, density of vehicles, packet transmission, duration, throughput, average end-to-end delay, and node identifiers (IP and MAC addresses) within the RSU cluster communication network.

4.2 Evaluation Metrics:

Proposed model performance is assessed using evaluation metrics. Performance metrics for abnormality behavior detection based on DoS attacks can be divided into two categories: detection and prevention.

Detection metrics

- True positive rate (TPR): TPR represents the proportion of actual DoS attacks accurately detected and classified.
- False positive rate (FPR): FPR represents the normal traffic propotion that is erroneously detected and classified as a DoS attack.

- Accuracy: Accuracy represents the proportion of all traffic that is accurately classified, encompassing both DoS attacks and normal traffic.
- Precision: Precision represents the proportion of detected instances that are correctly classified as true DoS attacks.
- Recall: Recall indicates how effectively the system detects all the existing DoS attacks.

Prevention metrics

- Block rate: the proportion of DoS attacks that are blocked.
- False negative rate (FNR): The rate of DoS attack evasion
- Average time to detect: the average time taken to detect a DoS attack.
- Average time to block: the average time taken to block a DoS attack.

Computational Overhead Metric considered is the latency: the amount of time it takes for the detection and prevention mechanisms to process packets.

The effectiveness of the proposed methods is assessed by the performance evaluation metrics, namely: Accuracy, Recall, Precision and F-Measure are given with the formula.

Accuracy determines the ratio of the correctly classified sample count to the total number of instances evaluated by using equation (4.1)

$$Accuracy = \frac{tp+tn}{tp+fp+tn+fn} \tag{4.1}$$

Where tp stands for true positive, tn denotes true negative, fp denotes false positive, tn denotes true negative and fn denotes false negative. Precision is the fraction of predicted data instances as positive that are in fact positive. The evaluation metrics of precision for the proposed model is as follows:

$$Precision = \frac{tp}{tp+fp} \tag{4.2}$$

From equation (4.2); tp stands for true positive and fp signifies false positive. Recall, also known as the detection rate, proportionate the ransomware samples that are accurately identified, and is defined as follows:

$$detection\ rate = \frac{tp}{tp+fn} \tag{4.3}$$

From equation (4.3); tp stands for true positive and fn symbolizes false negative. F-Measure is the harmonic mean of precision and recall, and is defined as follows:

$$F - Measure = \frac{2*tp}{2*tp+fp+fn} \tag{4.4}$$

From equation (4.4), tp stands for true positive, fp denotes false positive, and fn denotes false negative. The suggested system employed a vehicle density metric to assess the RSU or cluster network's trustworthiness value. The nodes are designated as assault nodes if the vehicle density value exceeds the threshold value for vehicle density. The density of vehicles computed using equation (4.5),

$$vehicle\ density\ (VD) = n \times {}^{1000}/_{l} \tag{4.5}$$

Where, VD = vehicle density (per km), n = vehicles occupying the road, and l = road length occupied by vehicles (m). The proposed system assessed the trustworthiness of the RSU or cluster network by monitoring the packet delivery ratio and exceeding a predefined threshold, the system flagged the associated nodes as potential attack sources. The packet delivery ratio is defined using equation (4.4)

$$packet\ delivery\ ratio\ (PDR) = \frac{total\ no.of\ received\ packets}{total\ no.of\ send\ packets} \tag{4.4}$$

Where, PDR = packet delivery ratio. The proposed system takes into account of attack detection rate of the RSU or the cluster network. The attack detection rate was calculated by using equation (4.7);

$$Attack\ detection\ rate\ (ADR) = \frac{100\% \times (total\ no.of\ attacks)}{(\ total\ no.of\ detected\ attacks)} \tag{4.7}$$

If the detection rate surpasses the established threshold, the token value is incremented, resulting in an increase of the trust value by one. Conversely, if the detection rate fails to surpass the threshold, the token value is decremented, resulting in a decrease of the trust value by one.

The proposed system also takes the account the average latency of the packets transaction between node n to node m to detect the attacks. If the average latency exceeds the threshold, the proposed system determines the node as affected based on the trustiness. The average latency was calculated by using equation (4.8)

$$average\ latency\ (AL) = N\ /\ T \tag{4.8}$$

Where N is the number of packets on an average in the network and T gives total traffic entering the network. If the average latency value exceeds the threshold, the token value increases the trust value by one; otherwise, decreases by one.

Performance Metrics for Self – healing AIS trust based Mitigation Model

Evaluating the performance of a Self-healing Artificial Immune System (AIS) trust-based Denial of Service (DoS) attack mitigation model in VANET requires specific performance metrics tailored to the distinctive characteristics and requirements of VANET. The key performance metrics are highlighted for model evaluation.

- Packet Delivery Ratio (PDR): PDR indicates the percentage of data packets that successfully reach their destination within the VANET. It's crucial to ensure that legitimate communication is maintained despite DoS attacks.
- End-to-End Delay: This metric evaluates the duration for a packet to traverse end-to-end nodes. Low delays are essential in VANET for real-time applications.
- Trust Score Accuracy: Trust-based models rely on trust scores to assess the reliability of vehicles in the network. Evaluate the accuracy of trust scores in differentiating between trustworthy and malicious entities.
- False Positive Rate (FPR) and False Negative Rate (FNR): Assess the system's ability to distinguish between legitimate and malicious entities. A balance between FPR and FNR is important to avoid unnecessary blocking of legitimate vehicles.
- Scalability: Evaluate how well the model scales with the cumulative number of vehicles in the network. Ensure that it can handle growing VANET without a significant decrease in performance.

- Robustness against Emerging Attack Types: Evaluate the model's ability to adapt and protect against new and emerging DoS attack patterns in VANET.
- Latency and Overhead: Measure the additional latency and overhead introduced by the model to ensure it doesn't compromise the real-time nature of VANET applications.

Performance Metrics for Mapping and Optimized Routing Approach

To effectively strengthen access control and mapping in VANET through optimized clustering and routing, particularly in the context of security threats, it is crucial to evaluate various performance metrics to assess the system's effectiveness. The key performance metrics for assessing the access control, mapping, cluster optimization, and routing mechanisms in immunized VANET are given below.

Access Control Metrics:

- False positive rate (FPR): Authorized requests that are incorrectly denied in proportion.
- False negative rate (FNR): unauthorized requests that are falsely granted in proportion.

Mapping and Routing Metrics:

- End-to-end delay: The average duration taken for packet travelling end-to-end.
- Packet loss rate: Packets lost percentage during transit.
- Throughput: The total number of packets that can be delivered successfully per unit time.

4.3 Performance analysis

The proposed hybrid approach consists of three steps. The subsequent section presents a detailed performance analysis of the optimized feature selection approach, specifically the Glow Worm Swarm optimized Single Layer Feed forward Networks, implemented in phase 1. The performance analysis of the proposed techniques in phase 2 and phase 3 are continued. The overall performance of the proposed hybrid approach is evaluated using a set of relevant metrics and then compared to the performance of conventional approaches.

4.3.1 Phase 1: Enhanced Feature Selection and Mitigation

Contribution 1: Optimized Feature Selection for Malicious Nodes Detection and Classification of DoS Attacks using Glow-worm (GLW) Single Layer Feed Forward Neural Network (SLFN)

Initially for the DoS attack detection and prevention using optimized feature selection approach, the performance of the proposed Glow Worm Swarm optimized Single Layer Feed forward Networks in the VANET is analyzed using the metrics and compared with the conventional feature selection approaches.

The features extracted from the Glowworm algorithm served as the input data for both the training and testing phases. For evaluation, 70% of the dataset was used to train the model, while the remaining 30% was reserved for testing. The model's performance was evaluated across different glow worm datasets using accuracy, sensitivity, and specificity as key metrics. To evaluate accuracy, the proposed algorithm was executed 100 trials, and the mean results were used as the accuracy score for classification of attacks. Algorithm was evaluated using different learning kernels, and results are presented in Table 4.4.

Table 4.4 shows that the proposed algorithm achieves its highest of 94.5% accuracy using the sigmoidal function with the CIC IDC dataset. Furthermore, Table 4.5 presents the results of the proposed GLW-SLFN algorithm, specifically when employing the Sigmoidal learning function, while varying the number of hidden neurons through random selection.

Table 4.4: Accuracy Comparison for different learning function used in Proposed Algorithm

Dataset details	Learning Kernel	Training Accuracy (%)	Testing Accuracy (%)
Five Feature Datasets	Sigmoid	95.5	95.4
	Sine	95.0	94.5
	Tanh	95.0	94.5

Table 4.5: Accuracy Comparison for the Different neurons used in GLW-SLFN Algorithm

Dataset Details	No. of Neurons	Training Accuracy (%)	Testing Accuracy (%)
Five Feature Datasets	10	93.5	93.0
	20	93.5	91.5
	50	92.5	92.5
	75	95.5	94.5
	100	91.5	92.4
	150	92.4	91.5
	200	91.5	92.5

As depicted in Table 4.5, the sigmoidal learning kernel, when utilized with 75 neurons, demonstrated the highest classification accuracy of 95.5% for various attacks within vehicular cyber-physical systems. To evaluate performance across various attack classifications, the highest accuracy achieved by the GLW-SLFN algorithm was compared with the accuracies of other learning algorithms. Different attack scenarios were considered for this comparative analysis.

Scenario – I Analysis

In the first scenario, DoS attacks were considered for classification and comparative analysis. Figures 4.4 and 4.5 clearly depict the training and testing accuracy of the proposed algorithm.

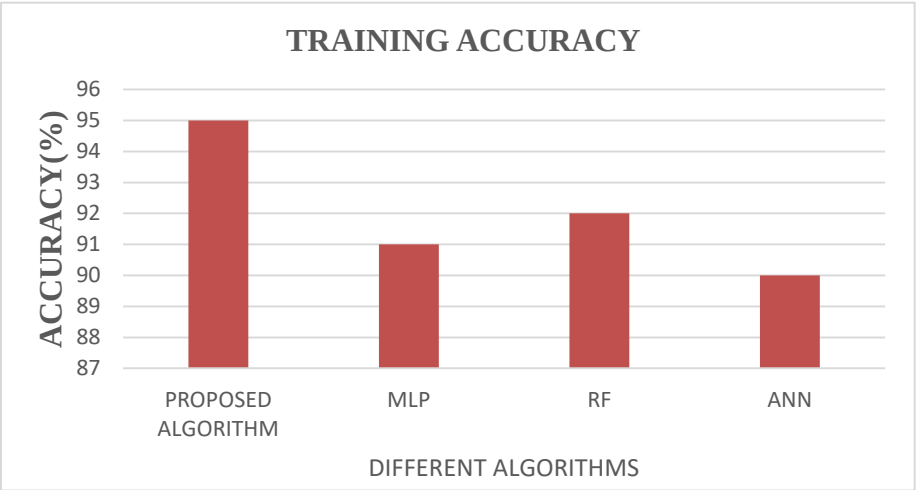

Figure 4.4: Training Accuracy Analysis for the different Algorithms in the DoS Attacks Classification

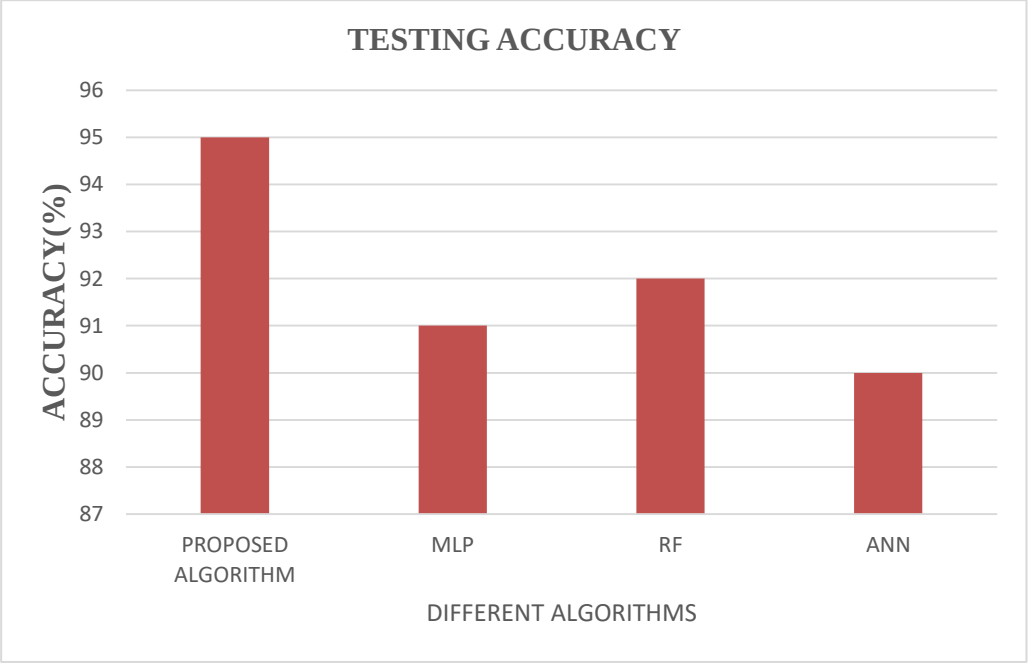

Figure 4.5: Testing Accuracy Analysis for the different Algorithms in the DoS Attacks Classification

The figures demonstrate that the proposed algorithm achieves an accuracy of 95.5%, surpassing other algorithms like Multilayer Perceptrons (MLP), Artificial Neural Networks (ANN), and Random Forest (RF). The learning kernel has improved the accuracy of the proposed GLW-SLFN.

Beyond accuracy, sensitivity (TPR) and selectivity (TNR) are crucial for evaluating classification algorithms. Sensitivity measures the algorithm's ability to correctly identify positive instances, while selectivity measures its ability to correctly identify negative instances. The subsequent subsection delves into a further analysis of the proposed algorithm's performance using these metrics.

Sensitivity and Selectivity Analysis

Neural networks are the best classification algorithm for classifying/predicting DoS attacks, based on sensitivity and selectivity analysis. However, random forests and support vector machines also have very good performance. Figure 4.6 shows the proposed GLW-SLFN approach provided performance exceeding random forests algorithm in sensitivity metric.

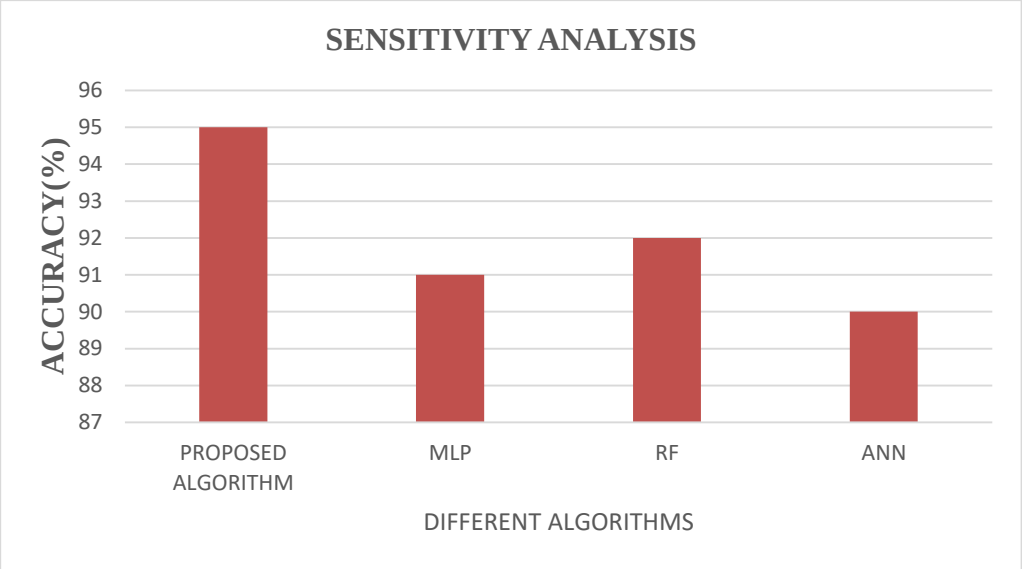

Figure 4.6: Sensitivity Analysis for the different Algorithms in the DoS Attacks Classification

The selectivity analysis performed based on the metric is revealed in the Figure 4.7 for the proposed GLW-SLFN approach providing the performance exceeding random forests algorithm in sensitivity metric.

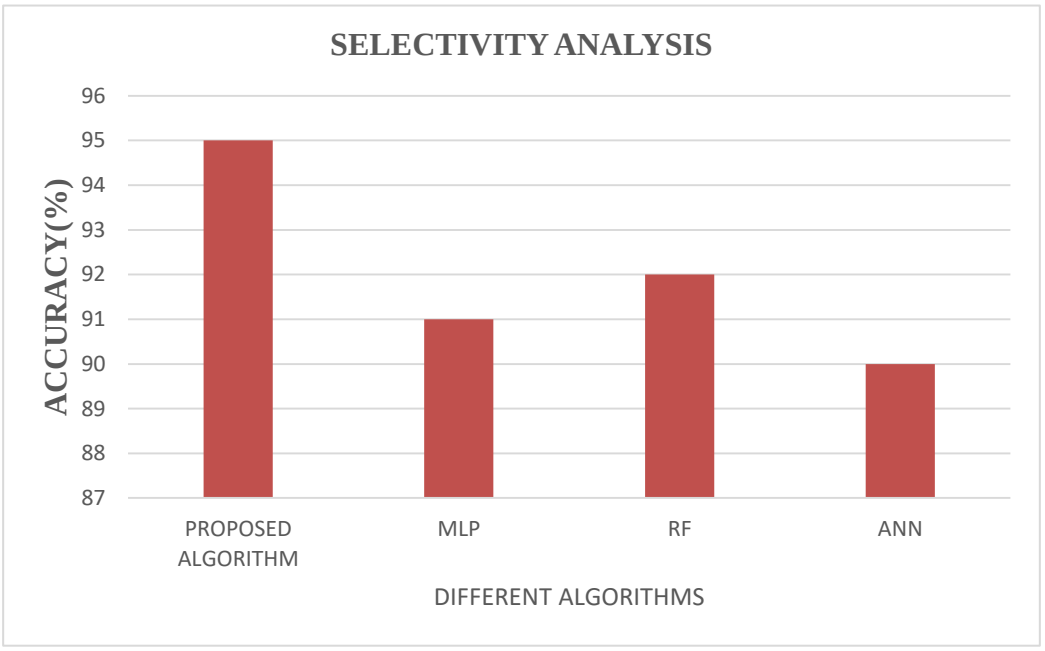

Figure 4.7: Selectivity Analysis for the different Algorithms in the DoS Attacks Classification

Scenario – II Analysis

The second scenario encompassed the classification and evaluation of Botnet attacks. A comparative analysis of the proposed algorithm with other approaches is presented in Table 4.6.

Table 4.6: Comparative Analysis between the different learning algorithms in classifying the Botnet attacks

Type of Attacks	Algorithms	Training Accuracy (%)	Testing Accuracy (%)	Sensitivity (%)	Selectivity (%)
Botnet Attacks	ANN	88.5	88.0	89.0	89.0
	RF	92	91.5	92	91.5
	MLP	91	90	91	90.5
	Proposed algorithm GLW-SLFN	95.5	95.0	94.0	95.0

An analysis of Table 4.6 reveals that the proposed algorithm surpasses existing learning algorithms in terms of key performance metrics, including accuracy, sensitivity, and selectivity.

Time Analysis

The training and testing times associated with the proposed GLW-SLFN were calculated and subsequently compared with the corresponding times for other existing algorithms. Tables 4.7 and 4.8 provide a detailed comparison of training and testing times for different networks, considering various attack scenarios.

Table 4.7: Training Time Comparison of the Proposed GOF-SLFN Model in Detection of Attacks

Types of Attacks	**Training Time (secs)**				
	GLW-SLFN	**SLFN**	**MLP**	**RF**	**ANN**
DoS attacks	0.233	0.345	0.1269	0.298	4.56
Botnet attacks	0.231	0.3300	0.1278	0.288	4.67

Table 4.8: Testing Time Comparison of the Proposed GOF-SLFN Model in Detection of Attacks

Types of Attacks	Testing Time (secs)				
	GLW-SLFN	SLFN	MLP	RF	ANN
DoS attacks	0.109	0.108	0.1117	0.118	2.39
Botnet attacks	0.112	0.111	0.121	0.121	2.78

An analysis of Tables 4.7 and 4.8 reveals a reduction in time complexity for the proposed algorithm on comparison with machine learning algorithms in the context of real-time vehicular attack detection. Furthermore, to substantiate the performance of the proposed algorithm, a comparative analysis was conducted against Single Feedforward Networks employing alternative optimization algorithms.

A comparative analysis was performed between the proposed SLFN classifier and classifiers employing existing optimization algorithms. Table 4.9 provides a detailed presentation of the comparative analysis results for the proposed SLFN classifier optimized through the utilization of the GLW algorithm.

Table 4.9: Testing Time Comparison of the Proposed GLW-SLFN Model in Detection of Attacks

S.No.	Type of Attacks	Algorithm used	Training Accuracy (%)	Testing Accuracy (%)	Sensitivity (%)	Selectivity (%)
1	DoS Attacks	Swarmfly-SLFN	87.5	87.0	86.0	85.0
		BAT-SLFN	93	92.5	92	91.5
		LDA-SLFN	94	93	90	90.5
		Proposed algorithm GLW-SLFN	95.5	95.0	94.0	95.0
2	Botnet Attacks	Swarmfly-SLFN	86.45	86.0	84.0	83.0
		BAT-SLFN	92	91.0	91	90.5
		LDA-SLFN	94	93	90	90.5
		Proposed algorithm GLW-SLFN	95.5	95.0	94.0	95.0

From the above Table 4.9, it is clear that Glowworm optimization SLFN has more efficiency than the other optimization techniques thus finding itself more suitable for the detection of attacks in the VANET scenario considered.

Phase 1 with Contributions 2, 3 and 4:

The enhanced feature selection approach has the proposed methods for the malicious nodes detection with isolation and prevention steps. During the process, an enhanced feature selection approach was implemented, which incorporated the Response Feedback Algorithm. Subsequently, adaptive nodal attack detection and reliance node estimation approaches were implemented to detect, isolate, and prevent malicious nodes arising from DoS attacks. The performance of the proposed contributions for the malicious nodes detection with isolation and prevention steps is provided in this section.

The performance values of the proposed Step 1, which are derived from Contributions 2, 3, and 4, are tabulated for a range of performance metrics in Table 4.10. The performance metrics associated with the proposed enhanced feature selection approach, which integrates a Self-healing AIS, an Entropy-based SVM, and a Bayesian Aggregate Model for the detection, isolation, and prevention of malicious nodes arising from DoS attacks, are graphically illustrated.

Table 4.10: Performance of the Proposed Phase 1

Network Size (No. of Nodes)	Number of Packets (p/sec)	Energy Consumption (EC) (J)	Latency (ms)	Detection Rate (%)	Throughput (Mbps)	Packet Loss (%)
50	9000	8	7	85	9.23	0.92
100	10000	15	10	86	10.23	0.9
150	11000	25	20	89	12.56	0.85
200	11000	38	30	97	15.03	0.78

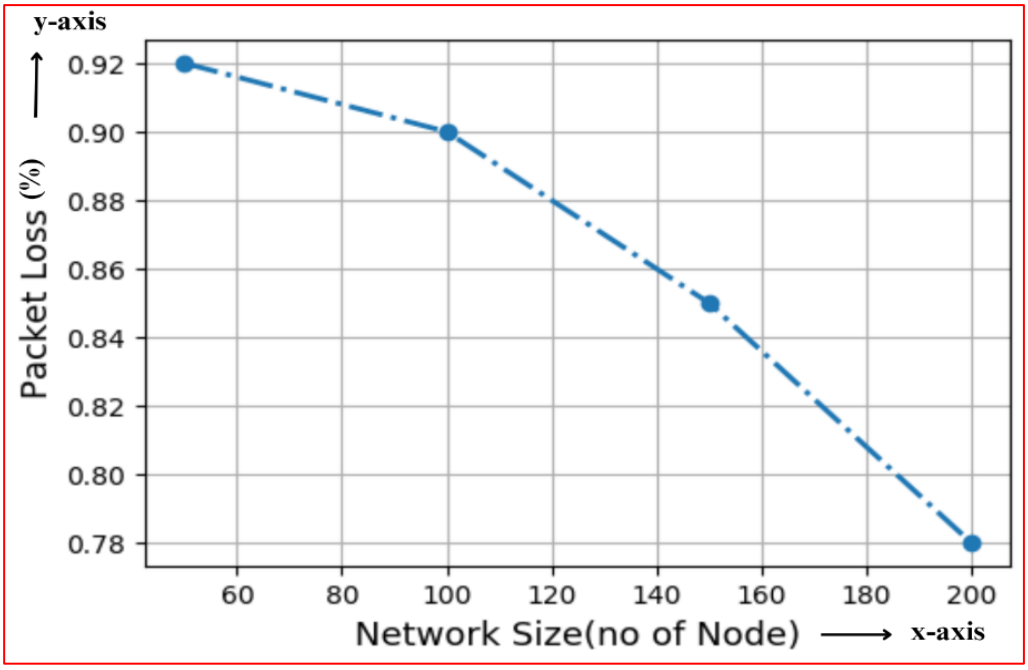

Figure 4.8: Packet loss

Figure 4.8 provides a clear depiction of the loss of packets a trend where an increase in network size, from 40 to 200 nodes, corresponds to a decrease in the packet loss experienced is demonstrated. The proposed Self-healing AIS with Entropy-based SVM demonstrates a reduction in packet loss by effectively managing node mobility through the implementation of the Response Feedback Algorithm. The identification of attacks is facilitated by the integration of micro-cluster outlier detection with linear regression, which incorporates factors such as temporal information with variable speed ranges, data transmission and response times between the RSU and vehicles, packet deviations and losses, relative vehicle speeds and positions, and other pertinent factors. Thereby this proposed model minimizes the packet loss to 0.78 when the network size is 200 but there is a need to further reduce the packet loss with enhancing security for more number of nodes.

The throughput of the proposed Self-healing AIS with Entropy-based SVM model is shown in Figure 4.9. The throughput of the proposed system was improved to 15 Mbps over 200 nodes and over 40 nodes, the throughput of the proposed model is 9.5 Mbps.

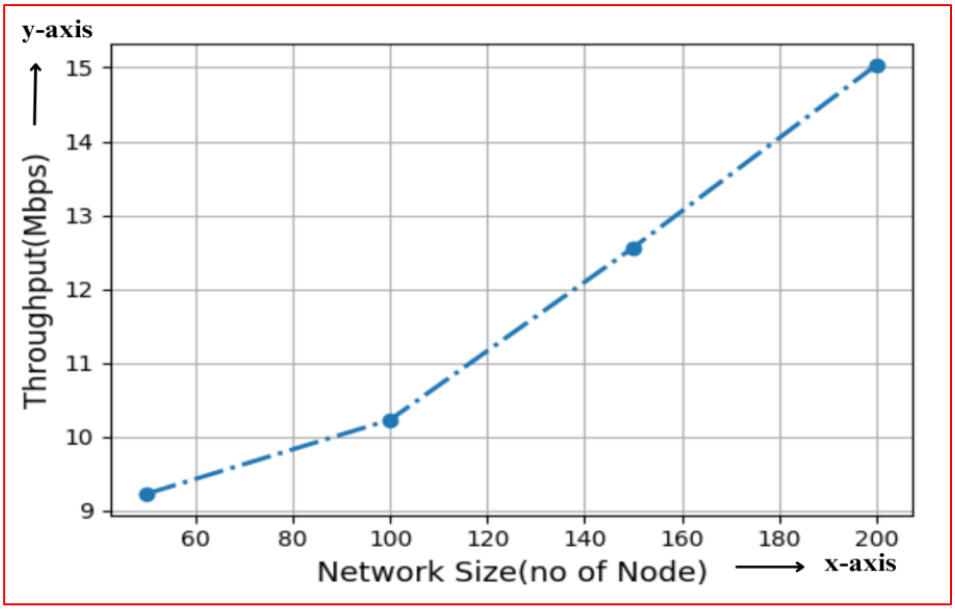

Figure 4.9: Throughput

It follows that throughput exhibited an increase with a corresponding scalability. The throughput of the proposed model is significantly enhanced through the utilization of an entropy-based SVM classifier, which leverages kernel density estimation within the framework of the Adaptive Nodal Attack Detection Approach for the identification of malicious attacks based on their respective trustworthiness values. However, there is a further need to enhance the throughput with considering more number of nodes.

As depicted in Figure 4.10, the detection rate of the proposed system exhibits a significant increase, rising from 85% to 94%, as the network size expands from 40 to 200 nodes. This notable detection rate can be attributed to the implementation of a novel adaptive nodal attack detection approach within the proposed system, wherein an entropy-based SVM classifier effectively categorizes maliciousness based on the trustworthiness of nodes. Nevertheless, further enhancements are required to ensure the detection of all twelve variants of DDoS attacks.

The performance evaluation of the proposed system, which incorporates an enhanced feature selection approach, a Self-healing AIS, an Entropy-based SVM, and a Bayesian Aggregate Model, demonstrates effective handling of DoS attacks. This comprehensive approach encompasses:

Detection: Enhanced feature selection facilitates accurate detection of malicious activity.

Isolation: The Self-healing AIS mechanism effectively isolates compromised nodes.

Prevention: The system actively prevents the spread of attacks.

This multi-faceted approach provides a robust solution for mitigating the impact of DoS attacks within the network.

The model exhibiting the performance is further considered to provide long-term availability of the VANET services by detecting further attacks and classifying the attacks with optimized routing on mapping.

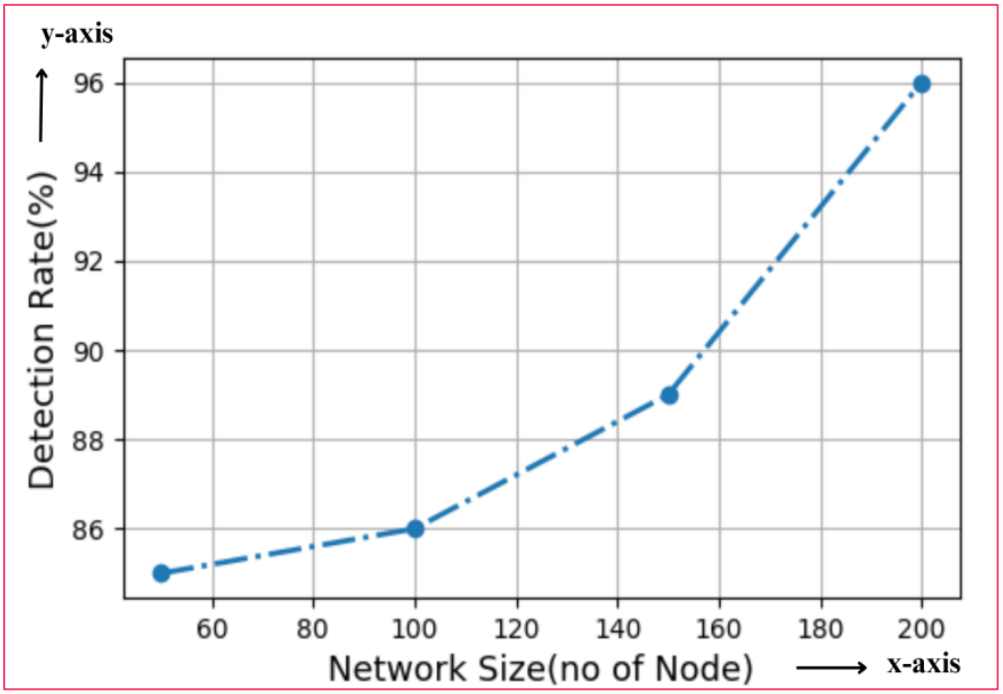

Figure 4.10: Detection rate

The following section provides the performance of the proposed steps 2 and 3 with the metrics and comparison.

Performance Comparison of Contributions 2, 3 and 4:

The state of the proposed contributions 2, 3 and 4 fulfilling the secondary objective 1 has been compared with the existing approaches. Compared with AODV,

Firecol technique and Trust-based framework (Poongodi et al., 2019) and the comparative analysis proved the performance of the proposed contributions 2, 3 and 4 outperformed the existing approaches.

Existing approaches in VANET often employ Trust-Based Evaluation Systems, frequently combined with clustering methods. These systems typically consider trust values derived from factors such as message frequency, overall trust, residual energy, trust policies, and data factors. The deterrence design identified the attacker, segregated the malicious nodes and optimized the utilization of a bandwidth without compromising the nodes security.

The proposed system effectively addresses DoS attacks in VANET by combining:

Enhanced Feature Selection: This approach refines the input data for improved attack detection.

Self-healing AIS: This mechanism provides inherent resilience and adaptability to the system.

Entropy-based SVM: This classifier accurately categorizes nodes as malicious or benign.

Bayesian Aggregate Model: This model enhances the system's ability to assess and trust information from different sources.

Furthermore, the system incorporates:

Micro-cluster Outlier Detection with Linear Regression: This technique analyzes data transmission and response times to identify abnormal behavior and detect potential attacks.

This multi-layered approach ensures robust detection, isolation, and prevention of DoS attacks within the VANET environment.

This approach leverages trust-based mechanisms, employing kernel density estimation on metrics such as vehicle density, energy consumption, average latency, packet delivery ratio, and detection rate. An entropy-based SVM classifier is then used to categorize and predict the maliciousness of nodes within the cluster network. The Pearson

correlation coefficient is utilized to assess the quality of the RSU cluster communication network. Furthermore, a Bayesian aggregate model, coupled with the self-healing effect of the Artificial Immune System (AIS), effectively isolates malicious nodes.

Figure 4.11 shows energy consumption of four methods (AODV, Firecol, Trust Based Framework, and Proposed Method) with varying network sizes. AODV is most efficient at 50 nodes but less as size increases. Firecol has high energy consumption across all sizes. Trust Based Framework improves efficiency with larger networks. The Proposed phase 1 is most efficient at 200 nodes, despite higher consumption at smaller scales.

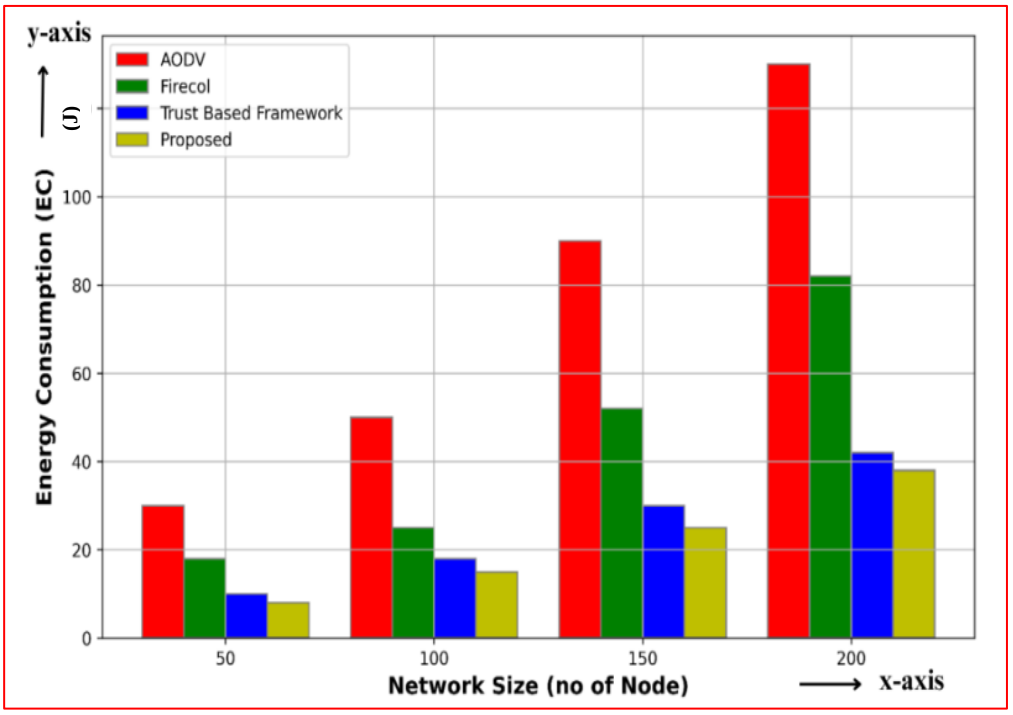

Figure 4.11 Energy Consumption

The proposed system significantly reduced latency by 25% compared to existing approaches. Specifically, it outperformed AODV (95% latency), the trust-based framework (27% latency), and Firecol (58% latency). This demonstrates that the proposed system achieves the lowest latency among these solutions, as visually depicted in Figure 4.12.

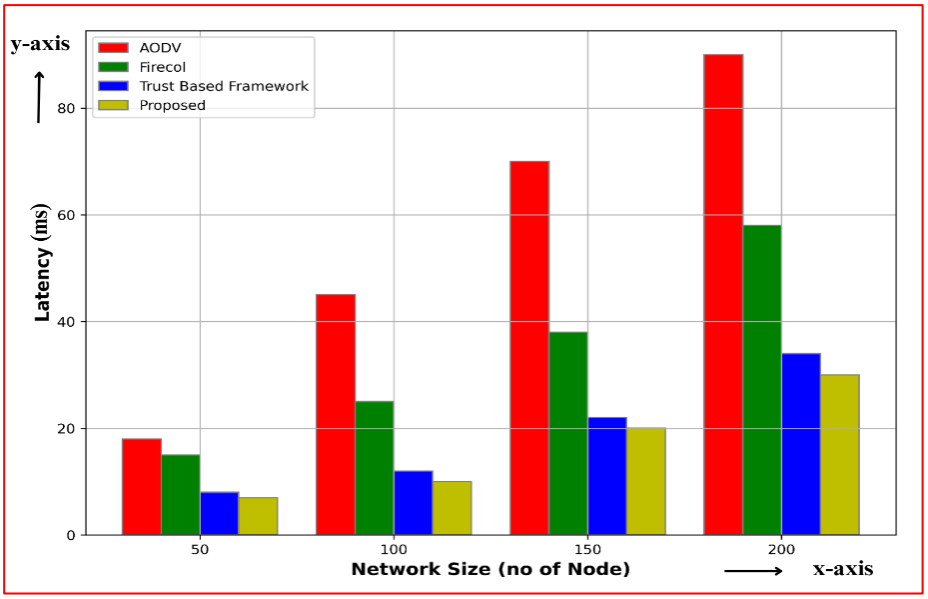

Figure 4.12: Latency

The proposed system significantly reduces latency by incorporating a novel approach. This approach leverages a Response Feedback Algorithm that integrates micro-cluster outlier detection techniques with linear regression. This combination effectively monitors anomalous behavior, providing valuable feedback based on temporal information and enabling rapid identification of attacks. This proactive approach leads to a substantial reduction in latency.

Furthermore, the system incorporates kernel density estimation to continuously monitor crucial parameters within the RSU cluster communication, including vehicle density, energy consumption, average latency, packet delivery ratio, and detection rate. By analyzing these parameters, the system accurately assesses the trustworthiness of each node.

To further enhance performance, the system integrates an entropy-based Support Vector Machine classifier. This classifier effectively categorizes nodes as malicious or benign using trust values, significantly improving the system's detection rate.

Compared to existing approaches, the proposed system demonstrates a significant improvement in detection rate. While AODV exhibits a detection rate of 60%, the trust-based framework achieves 65%, and Firecol reaches 77%, the proposed system achieves a

remarkable 97% detection rate. Notably, Figure 4.13 demonstrates that the proposed system consistently achieves the highest detection rate, outperforming AODV, especially in scenarios with a larger number of nodes.

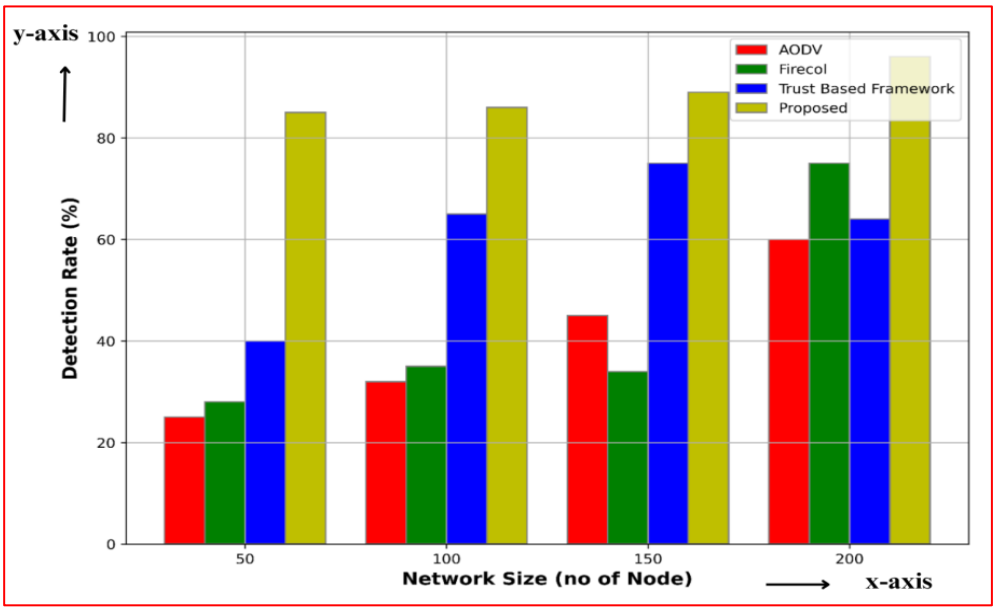

Figure 4.13: Detection Rate

Consequently, the proposed system demonstrated the capability to successfully identify, classify, and isolate attacks. This resulted in significant performance improvements, including a 97% detection rate, a 38% reduction in energy consumption, and a 25% reduction in latency, surpassing the performance metrics achieved by conventional methods.

4.3.2 Phase 2: Strengthening the Access Control and Mapping and

Phase 3 – Immunization of Clusters and Routing

Contributions 5 and 6:

The proposed steps 2 and 3 focused on enhancing the performance of the proposed approach through Triple Random Hyperbolic Encryption with Hex-Tuple Matched Mapping using Deep Auto Sparse Impasse Neural Network and Stable Automatic Optimization using Deep Trust Factorization Neural Network with Moth Flame Optimization algorithm. The metrics for the performance are provided with the graphs in this section.

Stable Automatic Optimization using Deep Trust Factorization Neural Network with Moth Flame Optimization algorithm is proposed to further reduce the packet size resulting in reduced packet loss. The proposed model's packet loss graph is shown in Figure 4.14. Packet loss is extremely low in the suggested model. The graph displays the amount of packet loss across the 300 nodes that make up the VANET. The packet loss for 50 nodes is 0.9, and when the number of nodes increased to 300, the packet loss is reduced to 0.5 and when the number of nodes is 200, packet loss is 0.7. Before attack the packet loss is 0.9 and after the attack the packet loss has been decreased to 0.48.

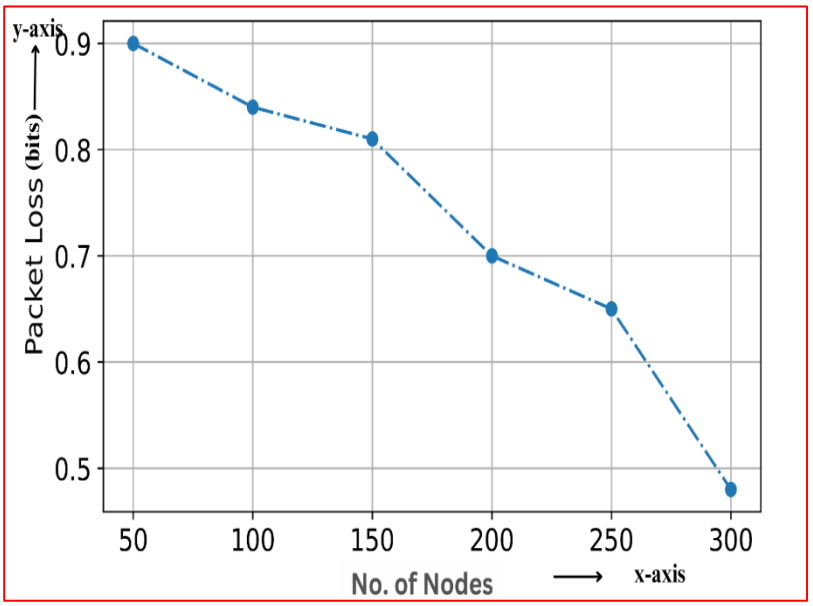

Figure 4.14: Packet loss

It has been decreased due to the proposed Encrypted Access Mapping in a Distinctly routed Optimized Immune System has low packet loss by using triple random hyperbolic encryption that perform random encoding three times and map all the same IP addresses in a symmetrically matching hex-tuple value thereby eliminate the packet loss associated with security concerns.

A novel approach, combining Stable Automatic Optimization with a Deep Trust Factorization Neural Network and the Moth Flame Optimization algorithm, is proposed to significantly enhance throughput during data transmission. Throughput, defined as the amount of information processed by the system within a given timeframe, is crucial for efficient network operation.

The performance based on throughput, is visually represented in Figure 4.15. This figure graphically illustrates the relationship between network size and the achieved throughput, demonstrating the significant performance gains achieved by the proposed approach. The throughput of proposed model is 10 Mbps when the number of nodes is 50; throughput is 17 Mbps and 21 Mbps when the number of nodes is 200 and 300 respectively. The number of nodes in the proposed model increases the throughput of the amount of data the network takes to transfer also increases. The throughput of the proposed model is increased by using Stable Automatic Optimized Cache Routing in which circular link state routing is used to adopt time and frequency synchronization channel hopping to get a high delivery ratio.

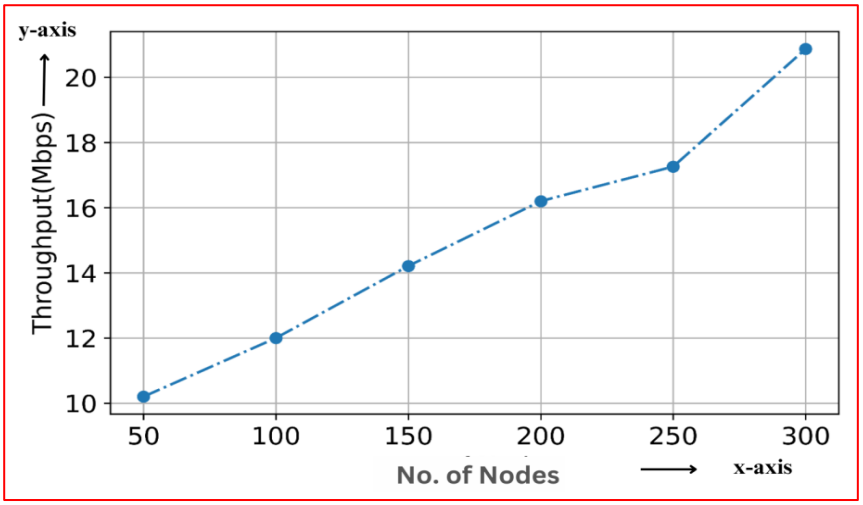

Figure 4.15: Throughput

Stable Automatic Optimization using Deep Trust Factorization Neural Network with Moth Flame Optimization algorithm is proposed to further enhance the detection rate in terms of accuracy.

The graph in Figure 4.16 demonstrates the proposed model's accuracy as it detects smurf attack with 99% of accuracy, ping flood attack with 97.4%, NTP amplification with 97.4%, SNMP reflection with 97.3%, DNS flood with 97.1%, HTTP flood with 94.4%, SYN flood with 94.4% and UDP flood with 94.2%. The proposed model has high accuracy because of Encrypted Access Hex-tuple Mapping Attack detection, which uses Deep auto sparse impasse NN for attack detection, which extracts features from sensing and mapping report to detect hybrid DDoS attacks.

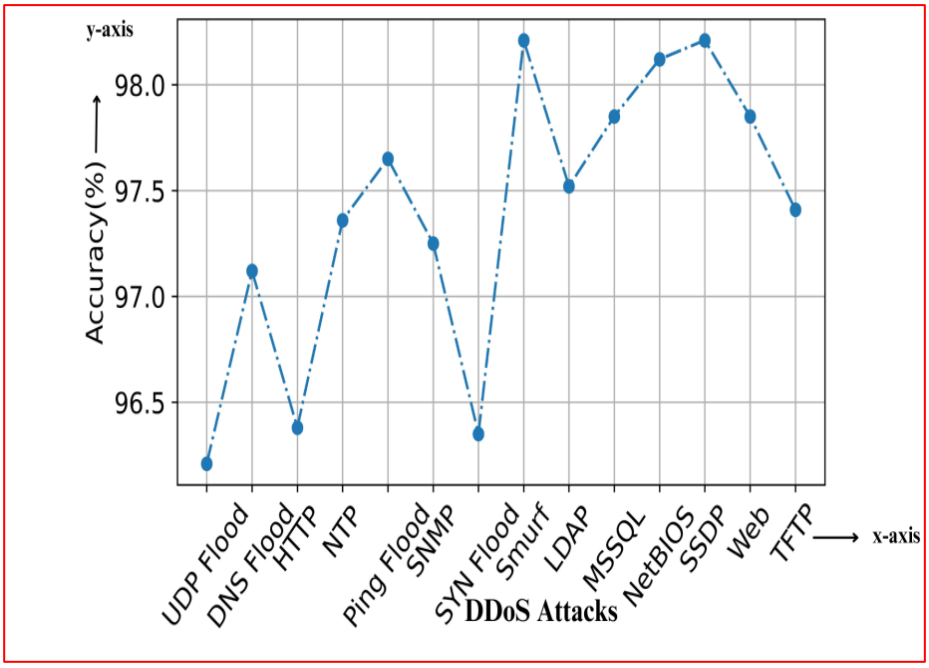

Figure 4.16: Accuracy

Cache parallelized circular link state routing in which a time and frequency-based channel hopping takes place to minimize the packet delay. Delay in a network is known as lag or latency amount of time taken for the packet to travel through multiple nodes. Low delay of 0.14 seconds observed for 50 nodes. As the node increases to 300 nodes, the delay decreases to 0.12 seconds as in Figure 4.17.

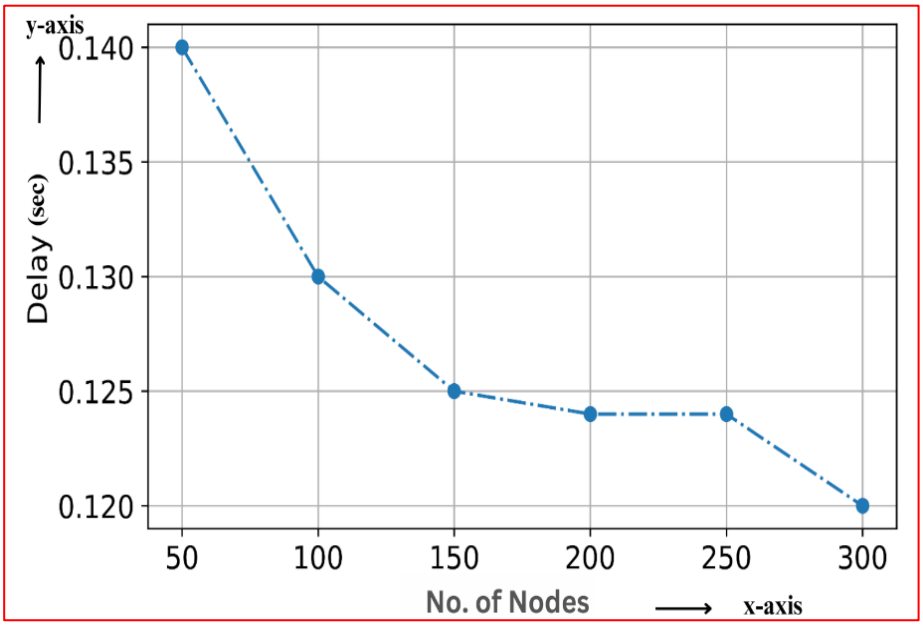

Figure 4.17: Delay

Hex tuple matched mapping provided high recall by same IP address mapped using a hex-tuple value. Figure 4.18 depicts the high recall of the proposed steps 2 and 3.

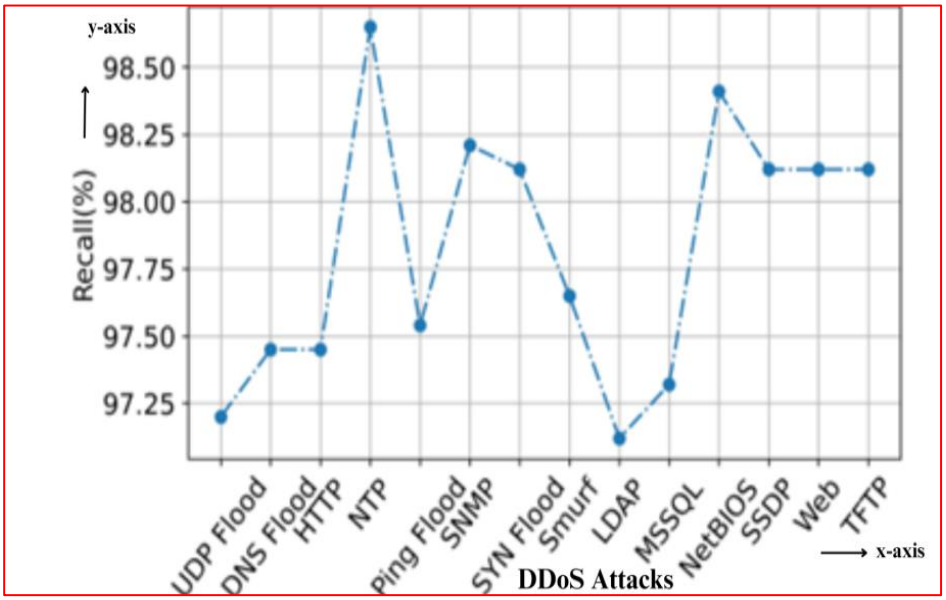

Figure 4.18: Recall

Hex tuple matched mapping by same IP address mapped using a hex-tuple value and Deep Auto Sparse Impasse NN provided high F1- Score in detecting hybrid DDoS attacks. Figure 4.19 shows the mean of precision and recall for the proposed steps 2 and 3.

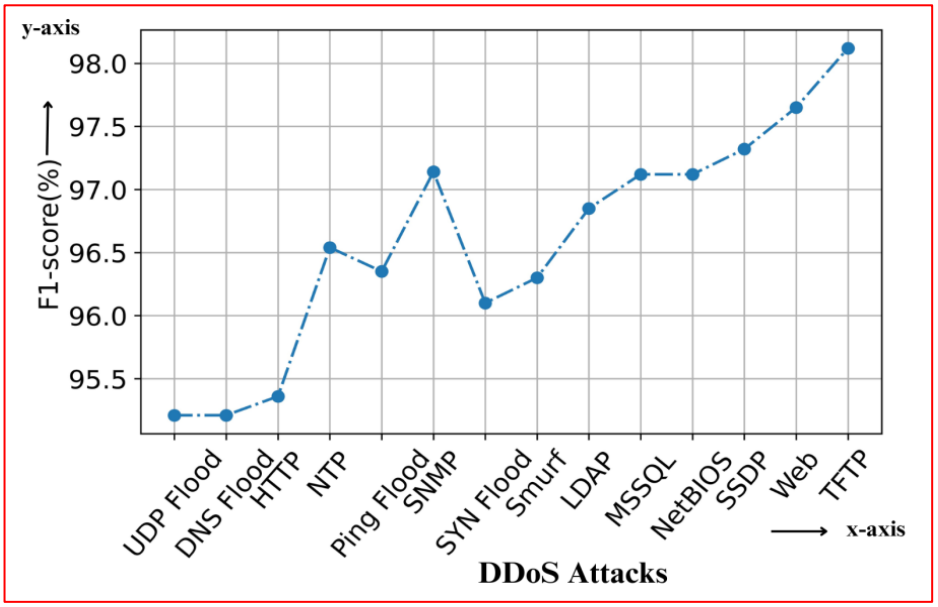

Figure 4.19: F1-Score

Performance Comparison of Contributions 5 and 6:

The comparisons are made from the previous techniques with various packet delivery ratios (PDR), attack detection, detection time, routing overhead, and false classification ratio. Comparisons are made with the existing techniques such as Trilateral trust, Host-based intrusion detection system (H-IDS), Multi filter, and Stream Position Performance Analysis (SPPA) (Poongodi et al., 2019).

Figure 4.20 shows the Packet Delivery Ratios (%) of five methods with varying node counts. The Proposed Method consistently outperforms others, maintaining near-perfect efficiency across all node counts. Trilateral Trust improves as node count increases, from 10% at 20 nodes to 90% at 100 nodes. H-IDS remain stable between 60% and 80%. Multi Filter shows an irregular pattern, peaking at 70% for 40 nodes and reaching 80% at 100 nodes. SPPA starts at 50% and improves to near full efficiency at 100 nodes. Cache parallelized circular link state routing adopts time and frequency synchronization channel hopping to get a high delivery ratio.

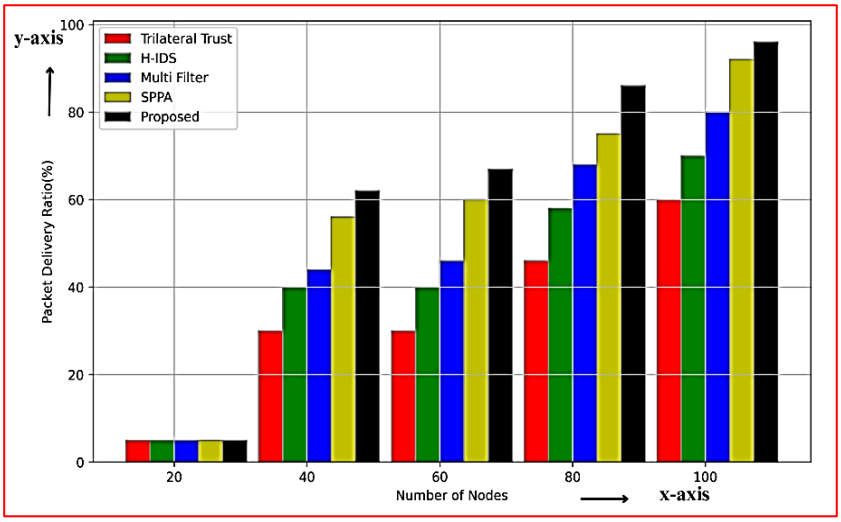

Figure 4.20: Packet Delivery Ratio

Figure 4.21 illustrates the performance of five methods in detecting attacks based on the number of nodes. Trilateral Trust shows moderate scalability, peaking at 60% effectiveness with 100 nodes. H-DS starts strong at 80% with 20 nodes but drops to 60% as node count increases. Multi-Filter peaks at 80% around 60 nodes, then declines slightly. SPPA shows excellent scalability, improving from less than 20% to near-perfect as node count increases. The Proposed Method also scales well, starting below 20% and reaching near full efficiency at maximum node count.

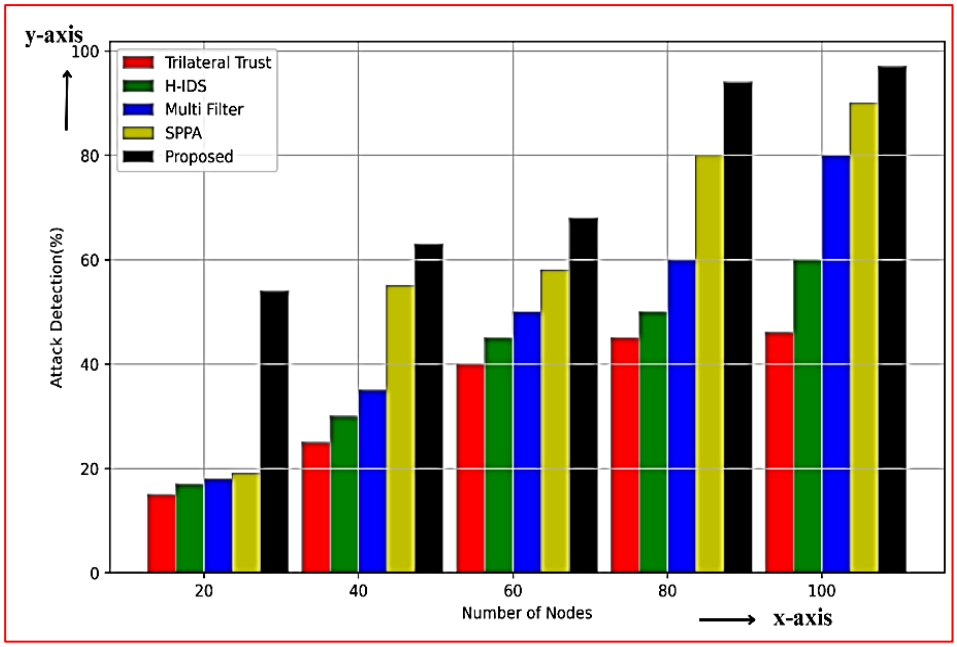

Figure 4.21: Detection Rate

Triple random hyperbolic encryption (TRHE) with hex tuple matched mapping and Deep Auto Sparse Impasse NN provided high accuracy by extracting features from sensing and mapping report to detect hybrid DDoS attacks.

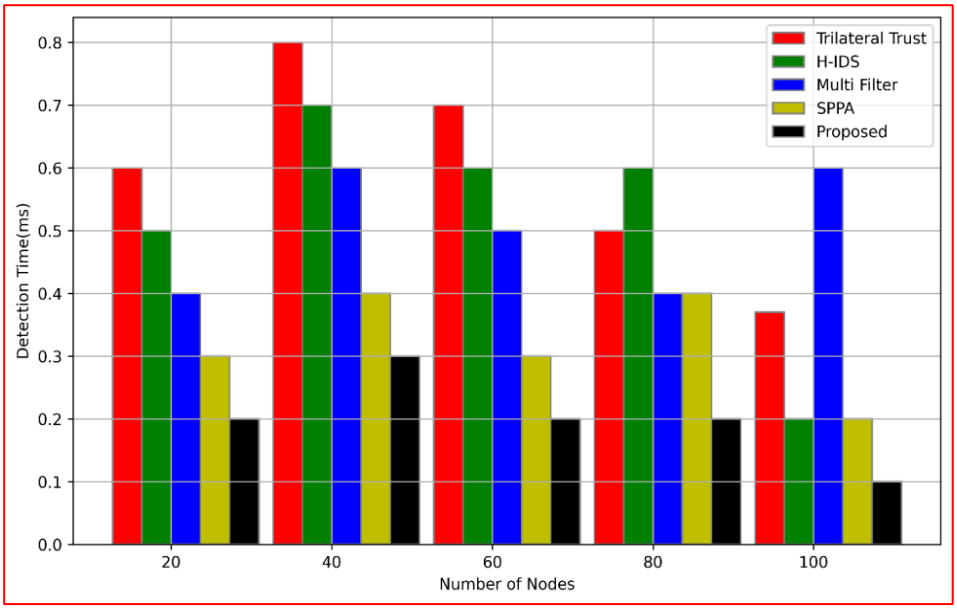

Figure 4.22 Detection Time

Figure 4.22 shows detection times of five methods across varying network nodes. Trilateral Trust has the highest detection time, starting at 0.7 ms for 20 nodes and

remaining high up to 100 nodes. H-DS starts at 0.6 ms and decreases to 0.4 ms at 100 nodes. Multi Filter starts at 0.5 ms, drops to 0.3 ms at 60 nodes, but rises to 0.4 ms at 100 nodes. SPPA starts at 0.6 ms and drops to just over 0.2 ms. The proposed contributions has the lowest times, starting at 0.45 ms and decreasing with more nodes.

The routing overhead is the amount of packet taken to check whether the neighbor node is active. Figure 4.23 shows that the proposed model has a very low routing overhead than the existing model. The increase in nodes to 100 provided the routing overhead of the proposed model remains remarkably low, maintaining an approximate value of 650 packets. The graph used to assume that the model. Trilateral trust has a very high routing overhead. The proposed contributions 5 and 6 has very low routing overhead due to Cache parallelized circular link state routing adopts time and frequency synchronization channel hopping with hex tuple matched mapping.

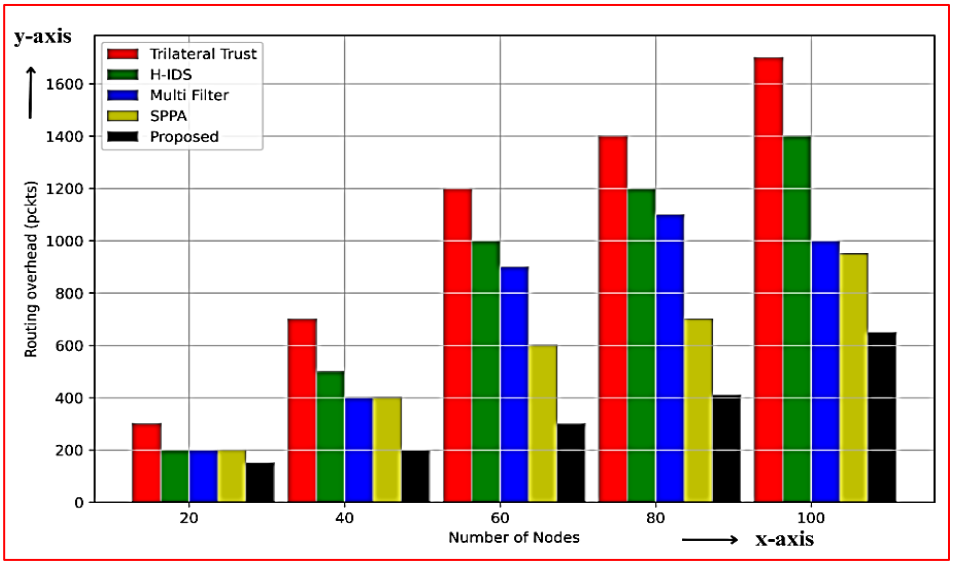

Figure 4.23: Routing Overhead

4.4 Performance Comparison of the Proposed Hybrid Approach

The performance of the proposed hybrid approach was evaluated by comparing it to the existing "Multivariant Stream Analysis Approach to Detect and Mitigate DDoS Attacks in Vehicular Ad Hoc Networks (MVSA)" (Kolandaisamy, R. et al., 2021). The MVSA model classifies traffic based on application type using predefined rules. These rules are then applied to incoming traffic to compute a multivariant stream weight. The

MVSA method, which classifies traffic streams as malicious or benign based on the computed weight, demonstrates effectiveness in detecting and mitigating DDoS attacks in VANET. However, the proposed hybrid approach surpasses the performance of the MVSA method. This is achieved through a combination of innovative techniques, including enhanced feature selection, self-healing mechanisms, and advanced machine learning algorithms, resulting in improved overall system resilience and security.

A comparative analysis was conducted between the proposed hybrid approach and the Multivariant Stream Analysis Approach (MVSA) for the detection and mitigation of DDoS attacks within Vehicular Ad Hoc Networks. The results of this comparative analysis are presented in tabular format. The proposed hybrid approach based on phase 2 and 3 provided the overall performance in mitigation of DoS attacks and its types thus obtaining the major objective. The performance metrics for the proposed hybrid approach on comparison is shown in the Table 4.11.

The table shows that the technique that is used here, Encrypted Access Mapping in a Distinctly routed Optimized Immune System, has a comparatively high packet delivery ratio (PDR) of 98%, an attack detection accuracy of 99%, an attack detection time of 0.1 ms, less routing overhead of 600 pkt and false classification ratio of 5%. The overall performance is above all existing methods.

Table 4.11: Performance Comparison of the Proposed Hybrid Approach

Techniques	Packet Delivery Ratio (%)	Attack Detection Accuracy (%)	Routing Overhead (pkt)	False Classification Ratio (%)	Detection Time (ms)
Trilateral Trust	60	42	1700	50	0.3
Host-based Intrusion Detection System (H-IDS)	70	60	1400	20	0.2
Multi Filter	80	80	1000	15	0.6
Stream Position Performance Analysis (SPPA)	90	90	990	10	0.2
Proposed Step – 2 and 3	98	99	600	5	0.1

The performance of the proposed hybrid approach has been analyzed in terms of packet loss, throughput and detection rate. The packet loss of the proposed Self-healing AIS with Entropy-based SVM is reduced by managing the mobility nodes using Response Feedback Algorithm and stable automatic optimized cache routing by using triple random hyperbolic encryption that performs random encoding three times and maps all the same IP addresses in a symmetrically matching hex-tuple value. The higher values of 0.9499 and 0.9854 are attained by the hybrid approach.

The proposed hybrid approach significantly enhances accuracy by incorporating a novel Response Feedback Method. By effectively combining linear regression and micro-cluster outlier detection, this method enables the identification and tracking of anomalous network behavior based on temporal data, facilitating rapid attack detection and mitigation.

Furthermore, the system leverages kernel density estimation to continuously monitor crucial parameters within the RSU cluster communication, such as vehicle density, energy consumption, average delay, packet delivery ratio, and detection rate. By analyzing these parameters, the system accurately assesses the trustworthiness of each node.

To further enhance performance, the system integrates an entropy-based Support Vector Machine classifier. This classifier effectively categorizes nodes as malicious or benign with trust values, significantly improving the system's detection rate.

Finally, the introduction of a Stable Automatic Optimized Cache Routing technique significantly improves the system's precision. Notably, the proposed system demonstrates significantly lower latency compared to existing approaches. While AODV exhibits a latency of 33 seconds, the trust-based framework experiences a latency of 57 seconds, and Firecol records a latency of 90 seconds. This demonstrates a significant performance improvement in terms of latency reduction.

From the experimental results and based on the comparison made with the existing approaches, the Proposed - A Hybrid Approach for Securing the Vehicular Ad-

hoc Networks by Mitigating Denial of Service Attack and types with Self-Healing and Immunization provided

a. Transactions of the packet ratio secured and increased.
b. Energy consumption reduced by isolating the malicious nodes.
c. Detection rate increased based on the trustworthiness values of the vehicle nodes.
d. Throughput considered higher reflecting the high transmission rate.
e. The delay decreasing to 0.12 seconds and packet loss for each node decreasing to 0.5 bits.
f. The system accurately detected twelve variants of DDoS attacks with 99% accuracy and exhibited a remarkably fast detection time of less than 0.1 milliseconds.
g. Accuracy, Recall and F1 Score of the proposed model in detecting DoS and DDoS attacks found higher with

    i. smurf attack with 99% accuracy, 97.65% Recall and 96.3% F1 Score
    ii. ping flood attack with 97.6%, 97.50%, and 96.4%
    iii. NTP amplification with 97.4%, 98.6% and 96.5%
    iv. SNMP reflection with 97.3%, 98.25% and 97.1%
    v. SNMP with 97.35%, 98.2% and 97.2%
    vi. DNS flood with 97.1%, 97.48%, and 95.1%
    vii. HTTP flood with 96.4%, 97.48%, and 95.1%
    viii. SYN flood with 96.4%, 98.15% and 96.1%
    ix. UDP flood with 96.2%, 97.24% and 95.1%
    x. LDAP with 97.5%, 97.15% and 96.85%
    xi. MSSQL with 97.5%, 97.3% and 97.1%
    xii. NetBIOS with 98.2%, 98.45% and 97.1%
    xiii. SSDP with 98.4%, 98.15% and 97.4%
    xiv. WebDDoS with 97.7%, 98.15% and 97.6%
    xv. TFTP with 97.45%, 98.15% and 98.15%

The proposed hybrid approach detects the twelve variant DDoS attacks with accuracy of 99% and less detection time of 0.1ms, thereby outperforming all existing techniques.

The hybrid approach proposed can have the consideration of the multi attribute optimization for the resilience of VANET. This can enhance the stable nature of VANET to be enhanced further and this is the limitation existing based on the proposed hybrid approach.

4.5 Chapter Summary

This chapter presents the findings of the research on securing VANET through a hybrid approach, combining DoS attack mitigation, self-healing, and immunization strategies. The results section presents a comprehensive evaluation of the proposed approach, including quantitative data on key metrics such as packet delivery ratio, delay, energy consumption, and detection rate. Comparative analysis with existing methods demonstrates the effectiveness of the proposed approach.

The discussion section delves deeper into the implications of the results, interpreting the findings in the context of VANET security. It analyzes the factors contributing to the performance improvements achieved through the hybrid approach, emphasizing the synergy between DoS attack mitigation, self-healing, and immunization mechanisms. The chapter concludes by discussing the limitations of the study and outlining promising avenues for future research that could further enhance the proposed system.

Overall, this chapter provides a comprehensive understanding of the proposed system's performance and its potential to significantly improve VANET security and reliability.