I. J. Computer Network and Information Security, **2023, 3, 90-105**
Published Online on June 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2023.03.07

Self-healing AIS with Entropy Based SVM and Bayesian Aggregate Model for the Prediction and Isolation of Malicious Nodes Triggering DoS Attacks in VANET

Rama Mercy. S.*
Avinashilingam Institute for Home Science and Higher Education for Women, Bharathi Park Rd, near Forest College Campus, Saibaba Colony, Coimbatore, Tamil Nadu 641043, India
E-mail: ramamercy_cs@avinuty.ac.in
ORCID iD: https://orcid.org/0000-0001-7557-973X
*Corresponding Author

G. Padmavathi
Avinashilingam Institute for Home Science and Higher Education for Women, Bharathi Park Rd, near Forest College Campus, Saibaba Colony, Coimbatore, Tamil Nadu 641043, India
E-mail: padmavathi_cs@avinuty.ac.in
ORCID iD: https://orcid.org/0000-0002-5377-4451

Received: 23 December 2022; Revised: 27 February 2023; Accepted: 03 April 2023; Published: 08 June 2023

Abstract: Vehicle ad hoc networks, or VANETs, are highly mobile wireless networks created to help with traffic monitoring and vehicular safety. Security risks are the main problems in VANET. To handle the security threats and to increase the performance of VANETs, this paper proposes an enhanced trust based aggregate model. In the proposed system, a novel adaptive nodal attack detection approach - entropy-based SVM with linear regression addresses the trust factor with kernel density estimation generating the trustiness value thereby classifying the malicious nodes against the trusted nodes in VANETs. Defending the VANETs is through a novel reliance node estimation approach - Bayesian self-healing AIS with Pearson correlation coefficient aggregate model isolating the malicious node thereby the RSU cluster communication getting secure. Furthermore, even a reliable node may be exploited to deliver harmful messages and requires the authority of both the data and the source node to be carried out by the onboard units of the vehicles getting the reports of incident. DoS attacks (Denial of Service) disrupting the usual functioning of the network leads to inaccessible network to its intended users thereby endangering human lives. The proposed system is explicitly defending the VANET against DoS attacks as it predicts the attack without compromising the performance of the VANET handling nodes with various features and functions based on evaluating the maliciousness of attacking nodes accurately and isolating the intrusion. Furthermore, the performance evaluations prove the effectiveness of the proposed work with increased detection rate by 97%, reduced energy consumption by 39% and reduced latency by 25% compared to the existing studies.

Index Terms: DoS Attacks, RSU, Cluster Network, Kernel Density Estimation, Pearson Aggregate Model, On-board Unit.

1. Introduction

Cyber threats are increasing to critical levels due to inclusiveness of Internet of Things (IoT) impacting every area of life with exchange of information. IoT threats between 2019 and 2020 arose to 100% and increased cyber-attacks in cyber-physical systems endanger human life and cause material damage. VANETs have gained popularity over the past ten years, and a number of applications, including early warning systems that can alert drivers to road construction, weather-related hazards, speed limits for curves, collisions, and pedestrian crossing warnings, merging lanes, are now prepared for widespread deployment [1]. The protection of the driver and passengers is now more important and difficult than ever before due to the ever-growing number of cars on the road. V2V communication is defined as communication between two or more vehicles when they are travelling on a road [2]. Vehicles that are connected to one another transmit information about position, directions, quick turns, speed, brakes, and emergency situations in order to prevent any potential collisions. Thus, nodes with an ad hoc network were constructed. VANET, which is also a division of Mobile Ad-Hoc Network (MANET), is a technology whose purpose is to improve driving safety, traffic flow, and comfort. This entails the registration and management of roadside units and onboard transportation units (OBUs) (RSUs) [3]. Fig.1. shows the VANET communication.

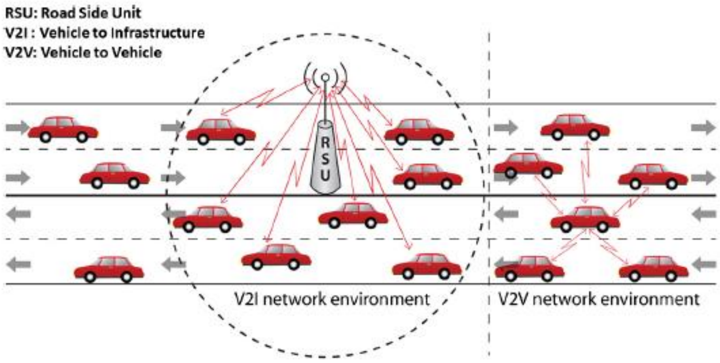


Fig.1. VANET communication

Information must be accurate, efficient, and dependable because information transmitted insecurely over VANET communication could have disastrous consequences [4]. By regularly exchanging information across network nodes, every project in the VANET field aims to effectively provide road safety [5]. Security is required in the VANET network to prevent attacker penetration from causing losses and privacy threats because any successful attack could result in serious accidents, the loss of life, or economic loss [6].

The biggest obstacle to putting VANETs into practice is the security issue because real-time VANETs include vital message exchange [7]. The timely transmission of messages has the power to either save or derail user lives. Denial of Service (DoS) attacks on the network are what lead to the lack of availability property of security [8]. As a result, denial-of-service (DoS) assaults become a significant issue when multiple vehicles conduct different forms of DoS operations to interfere with the network's normal operation and put human lives in danger [9]. Any form of DoS attack's primary objective is to prevent the targeted users from accessing the network service. Attacks of this nature are committed for a variety of motives, including monetary gain, rivalry, retaliation, self-gratification, diverting attention from more serious issues, etc. Due to their shorter length, DDoS assaults on VANET are become harder to detect [10]. A DDoS attack has the potential to cause mayhem and harm lives in this short amount of time. In order to prevent the Holocaust, an efficient detection mechanism should be created to identify DDoS attacks in their early phases [11].

This paper presents a novel hybrid model with self-healing AIS as a means to mitigate and immunize the VANETs without disrupting the normal functioning of the network. The security solutions provided in this paper are towards RSU cluster communication with response time and data transmission; isolating the attacked node on detection of maliciousness of the node thereby the proposed system performance is increased.

This work focuses on immunizing the network by isolating the node and deleting them in accordance with how of nodes behave within in the system. The work develops a learning strategy to identify and avoid DoS attackers without impacting the overall performance of the VANETs by utilizing the capabilities of anomaly detection and mitigation mixed with artificial immune system.

In this work, CICDDoS2019 dataset has been used to detect and isolate the affected node. The performance of the VANET that ensures seamless vehicular operation has been shown through the simulations and the assessment displays the system’s capability to detect abnormal behavior and act upon it to support the VANET operations. The paper is structured as follows. The state of the art in cyber-security for VANETs against DoS attacks is presented in section 2. The next, section 3, is dedicated to the hybrid model for the VANETs in securing the network performance and vehicular communications. Section 4 describes the simulation results and performance comparison. The section 5 presented the conclusion of the work.

2. State of the Art

Intelligent Transportation Systems are concentrating on focusing on cars that have significant computer, communication, and sensing capabilities (sometimes known as "smart" vehicles) (ITS). It might be challenging to safeguard wireless connections in automobile ad hoc networks. For the safety of individuals, security and its ensured level of implementation are crucial. This section provides a comprehensive analysis of the state-of-the-art literature on cyber security measures for VANETs, including associated work on glitch detection and mitigation techniques.

2.1. VANETs and Cyber Security Solutions

Vehicle communication for intelligent transportation systems (ITS) is quickly expanding, using wireless communication in vehicular ad hoc networks using specialized short-range communications. However, due to the different mobility of nodes in vehicles, the time it takes to connect a server to send or receive data with the cluster head from an external server is problematic, making it subject to security threats and causing packet losses in RSU cluster communication. Several surveys work exist in the literature which cover different security problems in vehicular networks and discuss challenges with solutions.

Fatemidokht et al [17] investigated how UAVs functioned in an ad hoc manner and how they interacted with other vehicles in VANETs to assist in the routing and identification of dangerous vehicles. Two distinct data routing techniques are included in the proposed VRU routing protocol: (1) using UAVs to convey data packets between automobiles using the VRU vu protocol, and (2) routing data packets between UAVs using the VRU u protocol. To evaluate the effectiveness of VRU routing components in an urban environment, Linux Ubuntu 12.04 and the NS-2.35 simulator are used. Additionally, the VanetMobiSim mobility generator and MobiSim are used, respectively, to create the motions of vehicles and UAVs. However, rural highways based on the suggested urban strategies require the introduction of a novel security protocol by enhancing energy saving, which is essential to UAV lifetime and enables the detection of hostile UAVs.

Brown et al [18] created the Blacksite framework for a revolutionary adaptive real-time intrusion detection in Internet of Things networks that integrates human intelligence with a synthetic immune system and uses a deep neural network-based validation model. They suggested a method that can handle the particular difficulties faced by IoT networks, and they presented implementation strategies in addition to a pilot implementation of Blacksite's key component. The suggested system is made to react to attacks quickly and change with evolving network topologies. It is necessary to look at other strategies, such as long short-term memory (LSTM) neural network algorithms, to counter sequence-specific traffic typical of DDoS attacks.

Nishanth et al [19] have discussed the flooding-based DoS assault, which led to a denial of sleep attack and targeted the mobile node's limited resources, which led to an excessive consumption of power. In a SYN flooding-based DoS attack, the attacker sends several spoof SYN packets, overflowing the target buffer and clogging the network. The three sections of the article are as follows: 1) Using Bayesian inference to mathematically represent SYN traffic in the network; 2) demonstrating that Bayesian inference and exponential weighted moving average are equivalent; and 3) creating an effective algorithm for the recognition of SYN flooding attacks via Bayesian inference. Any form of flooding-based DoS attack in a wireless ad hoc network is successfully defended by the suggested work's implementation. Data fusion techniques and an additional source of evidence are required for this method.

Alharthi et al [20] presented a biometrics blockchain (BBC) framework to secure data transfer among automobiles in VANET and to maintain archive data in a traditional and reliable manner. The benefit of biometric data in the suggested framework preserved privacy by keeping a record of the message sender's actual identity. Because of this, the proposed BBC approach creates security and trust among cars in VANET coupled with the ability to track down identities as needed. Simulations employing the urban mobility model were run in OMNeT CC, veins, and SUMO to show the proposed framework's feasibility. In terms of packet loss rate, packet delivery rate, and computing cost, the framework's performance is assessed. Future work will involve expanding the model for calculating the reputation and ranking of cars and drivers using machine learning methods.

Poongodi et al. [21] have presented a reCAPTCHA controller mechanism to stop automated attacks like botnet zombies. The majority of automated DDoS assaults are checked for and stopped by the reCAPTCHA controller. In order to implement this technique, the information theory-based metric is used to analyses the variance in user requests in terms of entropy. The criteria used to assess the attack's susceptibility are frequency and entropy. Large botnet-based attackers are deterred using the stochastic model-based reCAPTCHA controller. In the future, utilizing a hybrid technique to avoid and isolate assaults is performance- and security-wise efficient.

Yang et al [22] have created a method for the degradation-of-QoS (DeQoS) attack against mobile ad hoc networks. By using DeQoS, an attacker can waste the restricted connection resources of roadside units (RSUs) by relaying the verification relations between RSUs and distant vehicles in order to establish connections but not the service itself. The number of bogus connections could build up to the point where RSUs' resources are exhausted and they are unable to continue serving authentic cars. Due of the close relationship between vehicle mobility and the attacker's success likelihood, we simulate the arrival and departure of cars into a M=M=N-queue system. This illustrates how the attacker can choose alternative attack techniques in accordance with changing traffic situations. However, in future work, the distance-bounding-based defense mechanism to explore its practicability has to be implemented.

From the survey, for [17] a novel security protocol needs to be introduced to improve energy saving, for [18] supplementary mechanisms, such as LSTM neural network algorithms, are to be exposed to address sequence-specific traffic symbolic of DDoS attacks, for [19] On the basis of an additional source of evidence and data fusion techniques, future work is anticipated, [21] must be extend the model for computing ranking and reputation of vehicles and drivers using machine learning techniques, in [21] for avoiding and separating the attacks by using the fusion mechanism is performance- and security-wise efficient and for [22] the distance-bounding based protection mechanism to discover its operability has to be implemented. Hence, to overcome the above-mentioned issues a novel technique has to be implemented.

2.2. *Contributions to Secure VANETs against DoS Attacks*

Many academics have presented numerous algorithms for the limited network to be impervious to different attacks, and among them, the artificial immune systems (AIS) are categorized on inspired algorithms from biology [12]. These algorithms, as their name suggests, are computer-based algorithms whose principles and features are the outcome of a careful analysis of both adaptive qualities and the resistance of biological samples [13]. Theoretical immunology and observable immune activities, principles, and models provide as inspiration for these adaptive systems, which are used to tackle complicated problem areas. Various research areas are attempting to bridge the gap between immunology and engineering by using the methods of mathematical and computational modelling of immunology [14]. Many computer scientists suggested artificial immune-based computer models to address a variety of issues, from virus identification and fault analyzing to clustering [15], by carefully evaluating the effective natural mechanism. However, these algorithms have to be further enhanced for effective prevention of attacks with dimensionality reduction and less computational time [16]. Thus, to improve the security of the VANET platform subjected to DoS attacks, a novel algorithm based on AIS has to be implemented. The following are this paper's main contributions:

- A response feedback algorithm is suggested to identify the attacks in which micro cluster outlier detection monitors the abnormality behavior of the RSU cluster network based on temporal information is detected and linear regression is used to evaluate the attacks.
- An adaptive nodal attack detection approach is proposed to classify the new typical attacks in which entropy-based support vector machine is utilized for kernel density estimation and classify the attacks based on the trustiness value.
- The reliance node estimation approach is proposed in which the self-healing effect of AIS with Pearson correlation coefficient is utilized to check the similarity between the predicted data to estimate the maliciousness and the Bayesian aggregate model is utilized to check the credibility of the OBU to isolate the malicious node from the RSU cluster communication networks.

3. Proposed System with Aggregate Model for Prediction and Isolation of Malicious Nodes Triggering DoS Attacks in VANETs

Vehicle communication for intelligent transportation systems (ITS) is quickly expanding, using wireless communication in vehicular ad hoc networks using specialized short-range communications. However, due to the different mobility of nodes in vehicles, the time it takes to connect a server to send or receive data with the cluster head from an external server is problematic, making it subject to security threats and causing packet losses in RSU cluster communication. To close this gap, the proposed system introduces a novel Response Feedback Algorithm in which the microcluster outlier detection with linear regression utilizes to identify the attacks during the data communication and it considers the temporal information with variable speed range based on data transmission and response time between the RSU, deviation from the packets sent and loss, the relative speed between vehicles and their position. Moreover, to create a system capable of managing new typical DoS threats, such that no additional involvement in updating the attack repository is necessary to forecast attacks before they occur. To overcome this issue, the proposed system introduces a novel, Adaptive Nodal Attack Detection Approach in which an entropy-based SVM classifier utilized for kernel density estimation to detect the maliciousness of attacks based on trustiness value. Furthermore, different manufacturers' vehicles have varied features and functionalities, and these unique characteristics pose a variety of security risks, as well as being vulnerable to assaults. To bridge this gap, the proposed system introduces a novel Reliance Node Estimation Approach in which self-healing AIS with Pearson coefficient correlation used to check the similarity of the predicted value and the Bayesian aggregate model used to check the credibility of the OBU therefore the malicious attack node accurately identified and isolate the malicious node thereby the RSU cluster communication getting secure. As a result, the proposed system successfully identifies the attacks and classifies the attacks as well as isolates the attacked node thereby the proposed system performance is increased. The proposed system with the aggregate model against DoS attacks is shown in Fig.2.

3.1. *Response Feedback Algorithm*

Response feedback algorithm proposed to identify the threat in the RSU cluster communication. Because the RSU interacts with cluster members via cluster heads which change often owing to vehicles moving along the route. As a result, an attacker can launch an attack by overloading the network, causing packet failures in RSU cluster communication. Hence, the proposed system introduced a novel response feedback algorithm in which the transmission response time between RSU and the network is calculated by using temporal-based data with variable speed change. Then the RSU unit is utilizing micro cluster outlier detection with linear regression for identifying the attack in the RSU cluster region. The micro cluster outlier detection with linear regression identifies the attacks based on temporal information such as the data transmission and response time in-between network nodes, deviation from the packets sent and loss, the relative speed between vehicles and their position, and vehicle density from which the deviation from the forecasted transmission response time during data communication is derived. The micro cluster outlier detection algorithm is given below.

Algorithm1: Micro Cluster Outlier Detection Algorithm

```
Input:   New message (R)
Output: Detect abnormal behavior
    Start
    Increase the counter by 1: a++ // based on parameters
    If a% t = 0 then // t = threshold
    E = current time – the previous time
    s = t / E
    else send the message to the RSU
    end if
    s input to MCOD
    if s is normal then notify the node
    otherwise, find out whether the abnormality is because of attacks (by using linear regression)
```

Micro-cluster outlier detection abnormality monitoring steps are given below.

- When a new message (R) received, the counter (a) for new messages is incremented by one.
- A specified maximum boundary for the number of fresh texts is derived using the modular division of counter (a) and threshold (t).
- The new message delivered to the RSU if the remaining is not zero. Else, the present time is recorded.
- The time lapsed (e) then determined by subtracting the current time from the prior time.
- The new message's rate (s) is determined by dividing the threshold by the amount of time elapsed.

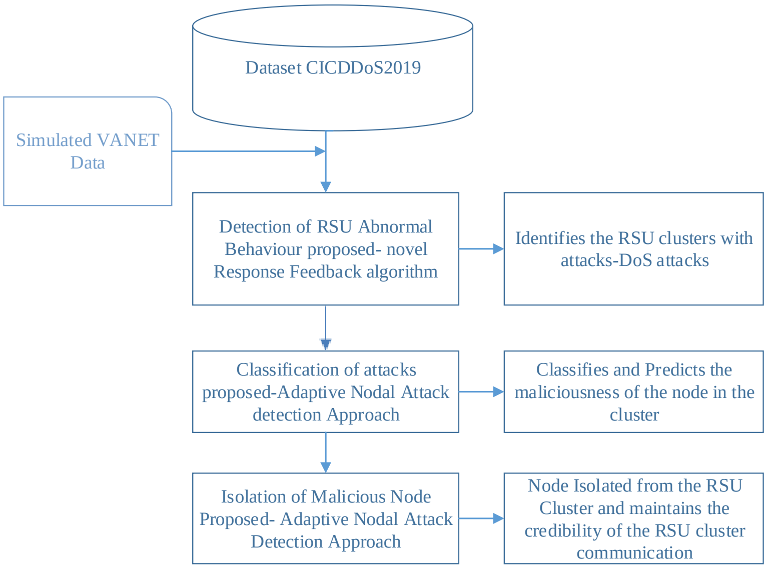

Dataset CICDDoS2019
Simulated VANET Data
Detection of RSU Abnormal Behaviour proposed- novel Response Feedback algorithm
Identifies the RSU clusters with attacks-DoS attacks
Classification of attacks proposed-Adaptive Nodal Attack detection Approach
Classifies and Predicts the maliciousness of the node in the cluster
Isolation of Malicious Node Proposed- Adaptive Nodal Attack Detection Approach
Node Isolated from the RSU Cluster and maintains the credibility of the RSU cluster communication

Fig.2. Proposed system with aggregate model

Then the proposed system added the linear regression with the micro cluster outlier detection for identifying the attacks in the RSU cluster network. The linear regression model identifies the attack by considering the number of new messages and the counter value. When the micro cluster outlier detection algorithm shows, that the numbers of a new message are raised then the counter is incremented by one, if the network is normal and then counter is increased based on the temporal information. Therefore, the linear regression takes into account of new message and counter values are used to identify the attacks. The mean absolute error of this line is derived using the formula

$$M = \frac{1}{n}\sum_{i=1}^{n}(|Xi - \acute{X\imath}|) \tag{1}$$

Where

- Xi – the number of counters
- $\acute{X\imath}$ – estimation of this value

In this way, the proposed system has identified the attacks in the RSU cluster communication network. If the attack is identified then the proposed system requires to find out the maliciousness of the attacks caused by the network, therefore, the suggested system introduces a novel adaptive nodal detection approach.

3.2. Adaptive Nodal Attack Detection Approach

To detect maliciousness of DDoS attacks from VANET, the proposed system used a trust-based assessment process. In the adaptive nodal attack detection approach, the maliciousness of attacks identified using the kernel density estimation for vehicle density, average latency, packet delivery ratio, detection rate, and energy consumption during communication of nodes between the RSU and cluster network depending on traffic data, which accurately identified using the using entropy-based support vector machine (SVM) classifier. The kernel density estimation, estimate the probability density function in the RSU cluster network and generates the trustiness values based on the parameters. If maliciousness of attack affects the node in the RSU or cluster network, the proposed system evaluates the trustiness value as 0 otherwise, if the cluster network or RSU is secure, the proposed system evaluates the trustiness value as 1. If the trustiness value is 0, then the entropy-based support vector machine classifies the maliciousness of attack to analyze the parameters such as vehicle density, energy consumption, average latency, packets delivery ratio, and detection rate.

The adaptive nodal attack detection approach algorithm is shows in algorithm 2 and the flowchart is shows in fig.3.

Algorithm 2: Adaptive Nodal Attack Detection Approach Algorithm

```
Input: parameters (x)
Output: maliciousness of attacks
    1. Start
    2. If ( the parameters (x) is equal to the threshold value in the cluster network)
           // create a token for incrementing the trust value by one
           Token j = j + 1
    3. Else ( the parameter (x) is not equal to the threshold value in the cluster network)
           // create a token for decrementing the trust value by one
           Token j = j – 1
    4. Find trust factor $\mathrm{TF} = \mathrm{VD} \times \mathrm{AL} \times \mathrm{PDR} \times \mathrm{DR} \times \mathrm{EC}$
    5. If (trust factor less than Kernel density estimation)
           // find out how much the node is affected by the attack
           SVM classify and predict the maliciousness of the attacks
    6. End
```

The adaptive nodal attack detection approach steps as follows

- The procedure starts by initializing the parameters VD, AL, PDR, DR, EC
- To classify the node Entropy-based SVM classifier takes the trustiness value of every parameter
- Then find out the trust factor using the formula

$$\mathrm{TF} = \mathrm{VD} \times \mathrm{AL} \times \mathrm{PDR} \times \mathrm{DR} \times \mathrm{EC} \tag{2}$$

- If the trust factor is not equal to the kernel density estimation (KDE) value, an entropy-based SVM classifier classifies and predicts the maliciousness of the node in the cluster network.

After predicting the maliciousness of attack from the node based on the trustiness kernel value by entropy-based support vector machine, then the malicious node must be isolated. Therefore, the proposed system uses a novel reliance node estimation approach to isolate the malicious node.

3.3. Reliance Node Estimation Approach

In the reliance node estimation approach, the proposed system checks the similarity between the predicted data within the VANET network by using the Pearson correlation coefficient method. In this work, the Pearson correlation coefficient shows the quality of the RSU cluster communication network. Pearson correlation coefficient captures the correlation between the predicted data that is measure the linear relationship between the low trustiness values for their diverse functions. Moreover, the correlation coefficient yields the value between -1 to 1, where,

- -1 indicates a strong negative relationship between nodes
- 1 indicates a strong positive relationship between nodes
- 0 (zero) indicates a no relationship between nodes

The Pearson coefficient correlation calculated by using

$$r = \frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{[n\sum x^2 - (\sum x)^2][n\sum y^2 - (\sum y)^2]}} \tag{3}$$

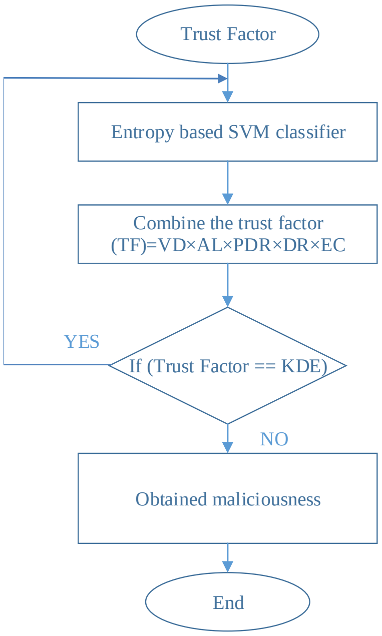

Trust Factor
Entropy based SVM classifier
Combine the trust factor (TF)=VD×AL×PDR×DR×EC
YES
If (Trust Factor == KDE)
NO
Obtained maliciousness
End

Fig.3. Flowchart of adaptive nodal attack detection approach

The variations are very high between the nodes; the correlation coefficient returns the value 1. If the variations are differing, then the correlation coefficient returns the value -1. If no relationship between the nodes, then the correlation coefficient returns zero. The scale of Pearson correlation coefficient factors measures [23] is tabulated in table 1.

Table 1. Pearson's coefficient's range

The scale of the correlation coefficient	Value
$0.8 \le r \le 1.0$	Very High Correlation
$0.6 \le r \le 0.79$	High Correlation
$0.4 \le r \le 0.59$	Moderate Correlation
$0.2 \le r \le 0.39$	Low Correlation
$0 < r \le 0.19$	Very Low Correlation

Furthermore, vehicles from diverse manufacturers have varied features and functionalities, and these unique characteristics provide a variety of security risks and are vulnerable to assaults. For that reason, the proposed system is also considering the onboard unit (OBU) and it checks the credibility by using a Bayesian aggregate model based on the Pearson coefficient. The RSU and OBU is given in fig.4.

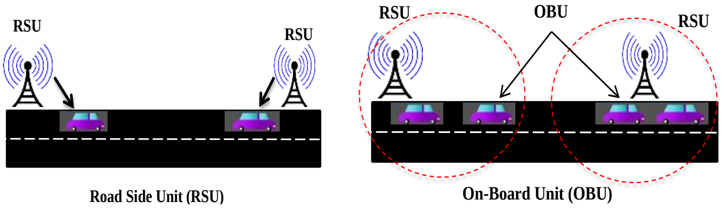


Fig.4. RSU and OBU

A hardware component placed on the vehicle, an on-board unit communicates with other OBCs and RSUs. The reliability of other cars it interacts with within the network is determined by the Bayesian aggregate model. Because even a truthful node could be used to send hateful messages. Consequently, the accuracy of the information and the reliability of the source node performed by the onboard components of the cars receiving the event reports This results in the on-board units in reception vehicles producing ratings for source vehicles, which are then utilized to update their individual faith values in the trust value. The proposed system is considering the trust level of the source node, and security status to check the credibility of the vehicle. Here the ratings (credibility score) of the vehicle are correct then the trust value is considered one otherwise the trust value is considered zero.

The Bayesian aggregate model continuous to check the credibility of the RSU cluster communication network therefore if any vulnerability action identified in the communication, the Bayesian aggregate model generates a credibility score of zero; therefore, the particular node is isolated with the self-healing effect of the artificial immune system (AIS).

The algorithm steps of the artificial immune system are as follows

Step 1: The algorithm starts with the initializing the predicted values in the cluster communication network.

Step 2: By transmitting Basic Safety Messages (BSM), it is sensing activities conducted by vehicles. The On-Board Unit (OBU) broadcasts BSMs based on the credibility value that contain information on the vehicle's density, energy consumption, average latency, detection rate, and packet delivery ratio.

Step 3: Evaluate the performance of each parameter.

Step 4: Decision is making based on the step 3, if the performance is less than threshold value the node is isolate from the cluster network.

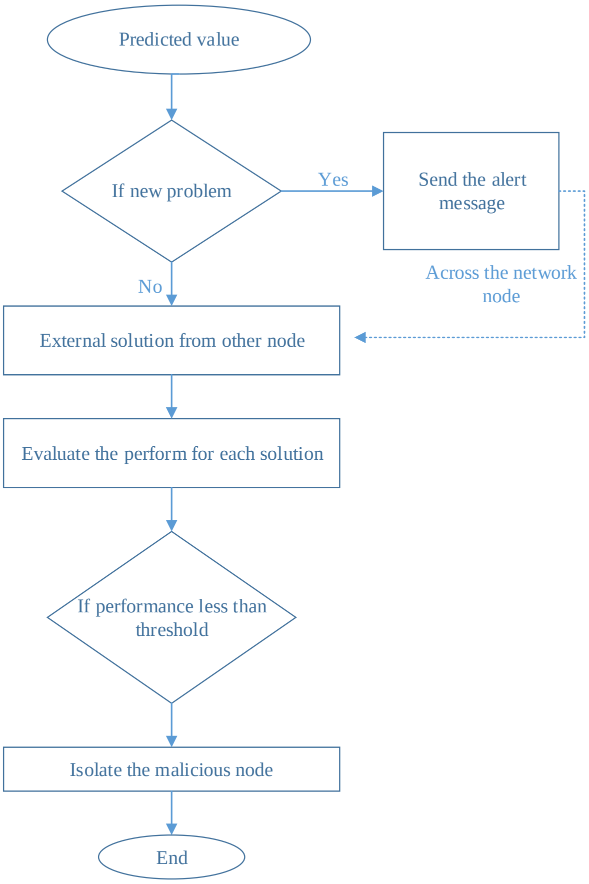

Predicted value
If new problem
Yes
Send the alert message
Across the network node
No
External solution from other node
Evaluate the perform for each solution
If performance less than threshold
Isolate the malicious node
End

Fig.5. Flowchart of AIS

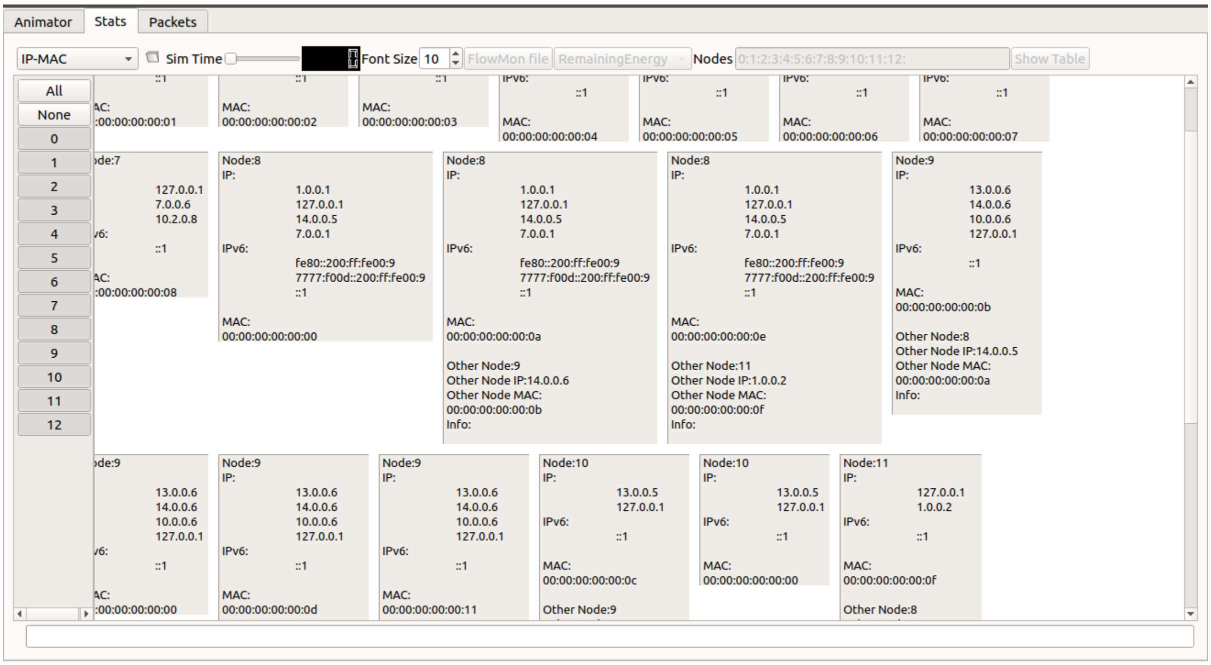
Fig.5. shows the flowchart of artificial immune system. As a result, the reliance node estimation approach evaluates the maliciousness of attacking nodes accurately and isolates the intrusion, and predicts the attack without compromising the performance of the VANET handling nodes with various features and functions.

4. Result and Discussion

This section includes a detailed explanation of the implementation outcomes, the performance of the suggested system, and a comparison section to guarantee the suggested system functions effectively. This work has been implemented in the working tool of NS-3 and CICDDoS2019 dataset used to detect and isolate the affected node. The benign and current common DDoS attacks in CICDoS2019 are a close reflection of actual data (PCAPs). Furthermore, it provides flows that have been labelled according to the time stamp, destination address IP addresses, input and output ports, protocols, and attack vectors, as well as the results of a network traffic analysis performed with CICFlowMeter-V3. Include many types of recent reflected DDoS attacks in this dataset, such as PortMap, UDP, LDAP, SYN, MSSQL, UDP-Lag, NTP, DNS, NetBIOS, and SNMP.

4.1. Simulation Results and Discussions

The simulation results of the proposed system are illustrated and discussed in this section. The proposed system uses a novel Response Feedback Algorithm in which micro cluster outlier detection with linear regression is used to identify attacks during data communication, and it takes into account temporal information with a variable speed range based on data transmission and response time between the RSU, deviation from the packets sent and loss, the relative speed between vehicles and their position. Therefore, the proposed systems have successfully identified the attacks in the RSU cluster communication network with the deviation loss, vehicle density, send and received packets, time duration, throughput, and average end-to-end delay. Moreover, the proposed system used a novel adaptive nodal attack detection approach for identifying the maliciousness of attacks. Based on the parameters, the kernel density estimate gives the trustworthiness values. If a node in the RSU or cluster network is subjected to an attack, the proposed system assigns a trustiness value of 0; otherwise, if the cluster network or RSU is safe, the proposed system assigns a trustiness value of 1. If the trustiness value is 0, an entropy-based support vector machine is used to distinguish maliciousness of attacks and examine characteristics such as vehicle density, energy consumption, average delay, packet delivery ratio, and detection rate. Therefore, the proposed system is successfully predicted the maliciousness of the attack.



IP-MAC □ Sim Time Font Size 10 RemainingEnergy Nodes 0:1:2:3:4:5:6:7:8:9:10:11:12:

```
AC:
:00:00:00:00:01

MAC:
00:00:00:00:00:02

MAC:
00:00:00:00:00:03

IPv6:
    ::1
MAC:
00:00:00:00:00:04

IPv6:
    ::1
MAC:
00:00:00:00:00:05

IPv6:
    ::1
MAC:
00:00:00:00:00:06

IPv6:
    ::1
MAC:
00:00:00:00:00:07

ode:7
    127.0.0.1
    7.0.0.6
    10.2.0.8
v6:
    ::1
AC:
:00:00:00:00:08

Node:8
IP:
    1.0.0.1
    127.0.0.1
    14.0.0.5
    7.0.0.1
IPv6:
    fe80::200:ff:fe00:9
    7777:f00d::200:ff:fe00:9
    ::1
MAC:
00:00:00:00:00:00

Node:8
IP:
    1.0.0.1
    127.0.0.1
    14.0.0.5
    7.0.0.1
IPv6:
    fe80::200:ff:fe00:9
    7777:f00d::200:ff:fe00:9
    ::1
MAC:
00:00:00:00:00:0a
Other Node:9
Other Node IP:14.0.0.6
Other Node MAC:
00:00:00:00:00:0b
Info:

Node:8
IP:
    1.0.0.1
    127.0.0.1
    14.0.0.5
    7.0.0.1
IPv6:
    fe80::200:ff:fe00:9
    7777:f00d::200:ff:fe00:9
    ::1
MAC:
00:00:00:00:00:0e
Other Node:11
Other Node IP:1.0.0.2
Other Node MAC:
00:00:00:00:00:0f
Info:

Node:9
IP:
    13.0.0.6
    14.0.0.6
    10.0.0.6
    127.0.0.1
IPv6:
    ::1
MAC:
00:00:00:00:00:0b
Other Node:8
Other Node IP:14.0.0.5
Other Node MAC:
00:00:00:00:00:0a
Info:

ode:9
    13.0.0.6
    14.0.0.6
    10.0.0.6
    127.0.0.1
v6:
    ::1
AC:
:00:00:00:00:00

Node:9
IP:
    13.0.0.6
    14.0.0.6
    10.0.0.6
    127.0.0.1
IPv6:
    ::1
MAC:
00:00:00:00:00:0d

Node:9
IP:
    13.0.0.6
    14.0.0.6
    10.0.0.6
    127.0.0.1
IPv6:
    ::1
MAC:
00:00:00:00:00:11

Node:10
IP:
    13.0.0.5
    127.0.0.1
IPv6:
    ::1
MAC:
00:00:00:00:00:0c
Other Node:9

Node:10
IP:
    13.0.0.5
    127.0.0.1
IPv6:
    ::1
MAC:
00:00:00:00:00:00

Node:11
IP:
    127.0.0.1
    1.0.0.2
IPv6:
    ::1
MAC:
00:00:00:00:00:0f
Other Node:8
```

Fig.6. Simulation results of the proposed systems

Furthermore, the proposed system used a novel reliance node estimation approach to isolate the malicious node. The RSU cluster communication network's quality is represented by the Pearson correlation coefficient. The Pearson correlation coefficient measures the linear link between the low trustworthiness values for their various functions and represents the correlation between the anticipated data. The figure 6 shows the node's IP value and MAC values of the node in the RSU cluster communication network. The Bayesian aggregate model determines the reliability of other cars with whom it interacts in the network. The Bayesian aggregate model continuously checks the credibility of the RSU cluster communication network; as a result, if any vulnerability action is discovered in the communication, the Bayesian aggregate model generates a credibility score of zero, and the particular node is isolated using the automatic identification system's self-healing effect (AIS). As a result, it isolated the malicious node in the RSU cluster communication network.

4.2. Performance Metrics of the Proposed System

The transactions of packets in the proposed method explained in Fig.7. The network size grows from 60 to 200 nodes in the presented graph, while the suggested number of packet transactions scheme increases. The self-healing effect of AIS with Pearson correlation coefficient was used to check the similarity of the predicted data with the VANET in the reliance node estimation approach, and the Bayesian aggregate model used to check the credibility of the OBU. As a result, it accurately evaluates malicious nodes and isolates malicious nodes; lowering packet loss in the proposed system thereby the transactions of the packet ratio are also secure and increased.

The transactions of packets in the proposed method explained in Fig.7. The network size grows from 60 to 200 nodes in the presented graph, while the suggested number of packet transactions scheme increases. The self-healing effect of AIS with Pearson correlation coefficient was used to check the similarity of the predicted data with the VANET in the reliance node estimation approach. Which assesses the linear relationship between the low trustworthiness levels and depicts the association between the expected data. and the Bayesian aggregate model used to check the credibility of the OBU. As a result, it accurately evaluates malicious nodes and isolates malicious nodes linearly; lowering packet loss in the proposed system thereby the transactions of the packet ratio are also secure and increased 11000 p/sec.

The above-mentioned graph clearly explains the trust value of the suggested system. From the Fig.8, the network size increased from 25 nodes to 200 nodes as well as the proposed system of trust value also increased. Because the proposed system uses a novel adaptive nodal attack detection approach in which the kernel density estimation is estimated probability density function for vehicle density, energy consumption, average latency, packet delivery ratio, and detection rate in the RSU cluster communication and it generates the trustiness value thereby the trust value of the proposed system is increased.

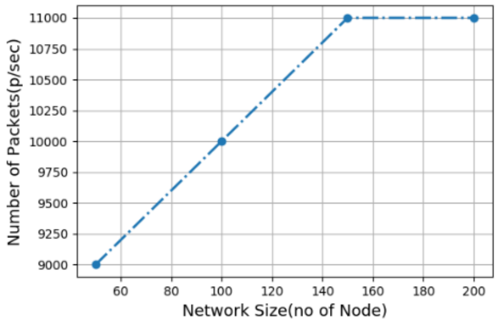


Fig.7. Transactions of packets

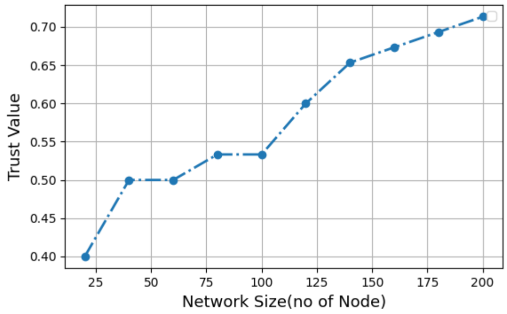


Fig.8. Trust value of the proposed system

The energy consumption of the proposed system is shows in fig.9. According to the graph, the network size has increased from 60 to 200 nodes, but the proposed energy consumption mechanism maintains the levels between from 10 to 40 as number of node increases. The Bayesian aggregate model used to check the credibility of the OBU, so it accurately evaluates malicious nodes and isolates the malicious node, thereby decrease the energy consumption in the proposed system.

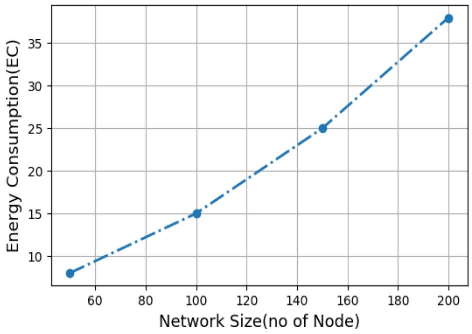


Fig.9. Energy consumption of the proposed system

The energy consumption of the proposed system is shows in fig.9. According to the graph, the network size has increased from 60 to 200 nodes, but the proposed energy consumption mechanism maintains the levels between from 10 to 40 as number of node increases. The entropy-based support vector machine categorizes the attack's maliciousness to examine energy usage and it generates the trustiness value in nonlinear regression. The Bayesian aggregate model used to check the credibility of the OBU, so it accurately evaluates malicious nodes and isolates the malicious node, thereby decrease the energy consumption of 39% in the proposed system.

Fig.10. clearly shows the latency of the proposed system. The latency of the suggested system improves by using a novel response feedback algorithm, in which micro-cluster outlier detection techniques with linear regression are used to monitor the abnormality behavior of the RSU cluster network and gives the feedback of the current cluster network thereby the attack RSU cluster is identified easily. As a result, the proposed system detects the attacks in a short amount of time, resulting in higher latency due to a response feedback algorithm that uses linear regression and micro-cluster outlier detection algorithms to track unusual network topology behavior, offer feedback based on temporal data, and detect attacks. From the graph, the network size increased from 60 to 200 nodes; the latency of the suggested system is also increased.

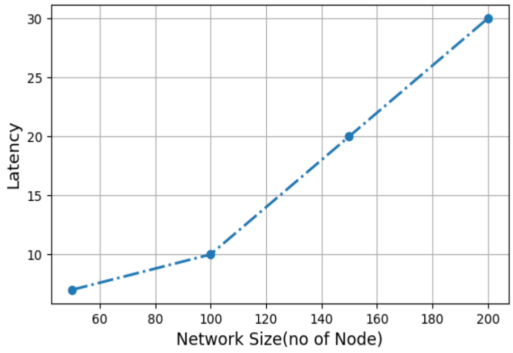


Fig.10. Latency of the proposed system

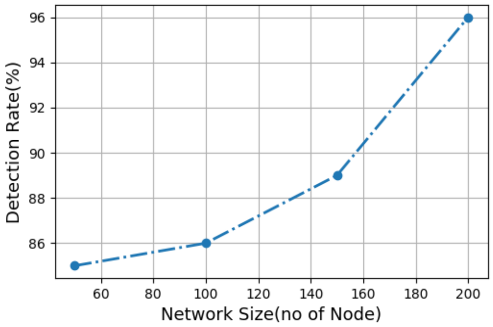


Fig.11. Detection rate of the proposed system

The detection rate of the suggested approach clearly illustrated, in fig.11. The network size has expanded from 60 to 200 nodes, and the suggested system of detection rate has increased, as seen in the graph. Because the proposed system employs a novel adaptive nodal attack detection approach, the entropy-based support vector machine classifier categorizes maliciousness based on their trustworthiness value, increasing the proposed system's detection rate.

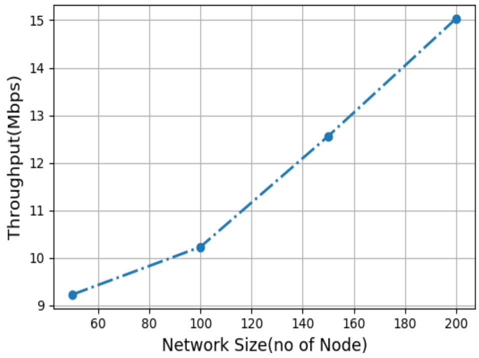


Fig.12. Throughput of the proposed system

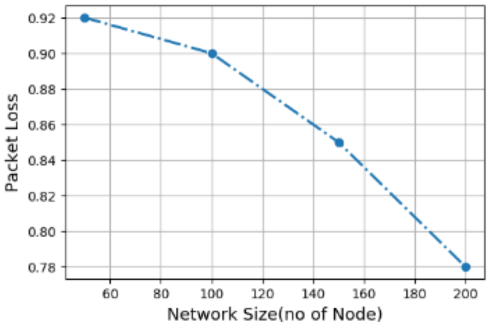


Fig.13. Packet loss of the proposed system

The throughput of the suggested technology is clearly, shown in fig.12. The throughput of the proposed system improved by using a novel response feedback algorithm in which micro-cluster outlier detection techniques used to monitor the abnormality behavior of the RSU cluster network Which are added the linear function and provide feedback on the current cluster network considering the temporal relationship between them thereby the suggested system identifies assaults quickly, resulting in greater throughput.

Fig.13, clearly explains the packet loss of the proposed system. From the graph, the network size increased from 60 nodes to 200 nodes as well as the proposed system of packet loss also decreased. In reliance node estimation approach, the self-healing effect of AIS with Pearson correlation coefficient used to check the similarity of the predicted data with the VANET, and the Bayesian aggregate model also utilized to check the credibility of the OBU therefore it evaluates malicious node accurately and isolates the malicious node thereby the packet loss of the proposed system reduced. Table 2 lists the overall performance values of the proposed system.

Table 2. The performance value of the proposed system

Network Size	Number of Packets(p/sec)	Energy Consumption(EC)	Latency	Detection Rate (%)	Throughput	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	96	15.03	0.78

4.3. *Performance Comparison of the Proposed System*

This section discusses how the proposed technique performs in many ways when compared to the outcomes of earlier methodologies and presents those outcomes using a variety of measures.

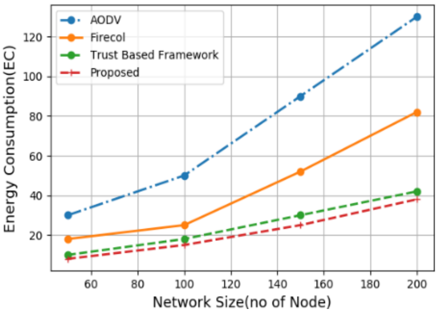


Fig.14. Comparison of energy consumption of the proposed system

The self-healing effect of AIS with Pearson correlation coefficient used to check the similarity of the predicted data with the VANET in the reliance node estimation approach in which the cluster network problems are resolved with the help of AIS. Moreover, the Bayesian aggregate model is also used to check the credibility of the OBU, so it accurately evaluates malicious nodes and isolates the malicious node, decreasing energy consumption in the proposed system. Fig14. and Table 3 shows the results of the energy consumption comparison of proposed method is given in table 3.

Table 3. Comparison of the proposed system's energy consumption

Number of Packets(p/sec)	AODV	Firecol	Trust Based Framework	Proposed system
50	30	18	10	8
100	50	25	18	15
150	90	52	30	25
200	130	82	42	38

The proposed system's energy consumption decreased by 39 than the existing output, when compared to the energy consumption of AODV (ad-hoc on-demand distance vector), which is 137, trust based framework, which is 40 and firecol, which is 82. In conclusion, AODV has the energy consumption, whereas our proposed system has the lowest energy consumption [24].

The proposed system's latency decreased by 25% than the existing output when compared to the latency of AODV, which is 95 percent, trust based framework, which is 27% and firecol, which is 58 percent. In conclusion, AODV has the latency, whereas our proposed system has the lowest latency. Fig.15. and Table 4 show the results of the latency comparison. The suggested system's latency decreases due to a response feedback algorithm that combines micro-cluster outlier detection techniques with linear regression to monitor anomalous network topology behavior and provide feedback based on the temporal information as well as identify the attacks. Consequently, the suggested system identifies the assaults quickly, resulting in reduced latency of the proposed system.

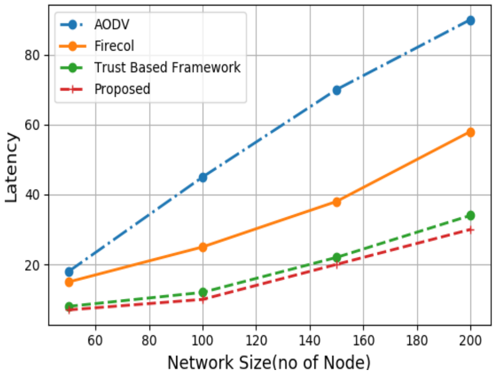


Fig.15. Comparison of latency of the proposed system

Table 4. Comparison of latency of the proposed system

Number of Packets(p/sec)	AODV	Firecol	Trust Based Framework	Proposed
50	18	15	8	7
100	45	25	12	10
150	70	38	22	20
200	90	58	34	30

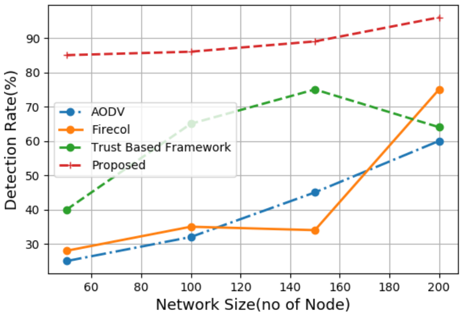


Fig.16. Comparison of detection rate of the proposed system

The suggested system uses a unique adaptive nodal attack detection technique that uses kernel density estimation to continually measure vehicle density, energy consumption, average latency, packet delivery ratio, and detection rate in RSU cluster communication and provide the trustworthiness value. Furthermore, the suggested system's detection rate improved by the entropy-based support vector machine classifier, which categorizes attacks depending on their trustworthiness value.

Table 5. Comparison of detection rate of the proposed system

Number of Packets(p/sec)	AODV	Firecol	Trust Based Framework	Proposed
50	25	28	40	85
100	32	35	65	86
150	45	34	75	89
200	60	75	64	97

Therefore, the proposed system's detection rate increased by 97% over the existing output, when compared to the detection rate of AODV, which is 60%, trust based framework, which is 65% and firecol, which is 77%. In conclusion, AODV has the lowest detection rate when the nodes are increases, whereas our proposed system has the highest detection rate. Fig.16. and Table 5 shows the results of the detection rate comparison.

When the attacker tries to put DDoS attack in the communication of VANET, the proposed system efficiently detects the affected node even if the number of attackers increase therefore the detection accuracy of the proposed system is high. Attackers Vs detection accuracy of the proposed system is show in fig.17 and the comparison values are tabulated in Table 6.

When compared to other techniques such as SVM that is 93%, Naïve Bayes that is 90%, K-nearest that is 92.3%, and multilayer perceptron (MLP) that is 83% but the proposed detection accuracy is high that is 97%. In which response feedback algorithm, adaptive nodal attack detection approach, and reliance node estimation approach are utilized to identify and isolate the attack nodes [25].

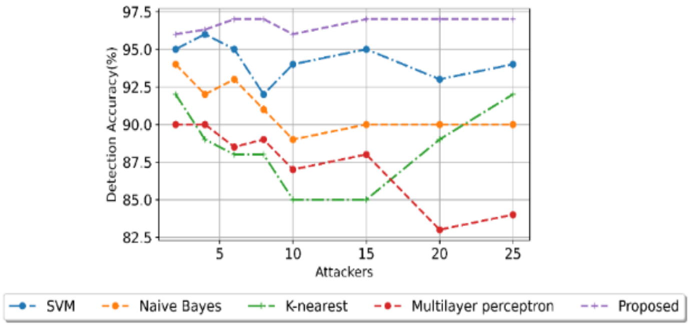


Fig.17. Attackers versus detection accuracy

Table 6. Attackers versus detection accuracy

Number of attackers	Detection Accuracy (%)				
	SVM	Naïve Bayes	K-nearest	MLP	Proposed
5	95.4	92.5	89.5	89.32	96.8
10	93.3	89.32	87.3	86.9	96
15	95	90	87.52	87.51	97
20	92.5	90	82.54	82.29	97
25	94.5	90	84.5	84	97

5. Conclusions

In this work, the attacks are identified by used a novel adaptive feedback response in which the micro cluster outlier detection with linear regression is utilized to recognize the attacks in the RSU cluster network. Moreover, the maliciousness of attacks classified used a novel adaptive nodal attack detection approach in which entropy-based SVM with kernel density estimation utilized to classify the attacks thereby the suggested system classifies the maliciousness of the node with trustiness value. Therefore, in a network of 50, 100, 150, and 200 nodes, the attempts to minimize packet loss in RSU cluster communication resulted in a drop in packet loss of 0.92, 0.9, 0.85, and 0.28, respectively. The proposed system of packet loss was also improved. The proposed system's output is 39% less energy-intensive. As compared to the latency of the current system, such as AODV, Firecol, and Trust based framework, which has latency of 95%, 27%, and 58% respectively, the recommended system's latency drops by 25% as a result of a response feedback algorithm than the existing output. The suggested system's detection rate performed 97% better than what was produced by the old method. The detection rates of AODV, Firecol, and Trust-based framework are 60%, 77%, and 65%, respectively, when compared to those of existing approaches. The proposed models detection accuracy is excellent, at 97%, compared to other approaches like SVM (93%), Naive Bayes (90%), K-nearest (92.3%), and multilayer perceptron (MLP) (83%). The proposed system effectively locates the afflicted node when an attacker attempts to disrupt VANET connection with a DDoS assault, even as the number of attackers grows. As a result, the proposed system's detection accuracy is high.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] Hamdi, Mustafa Maad, et al., "A review of applications, characteristics, and challenges in vehicular ad hoc networks (VANETs)," *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. IEEE, 2020.

[2] Hassija, Vikas, et al., "Dagiov: A framework for vehicle-to-vehicle communication using directed acyclic graph and game theory," *IEEE Transactions on Vehicular Technology,* vol. 69, no. 4, pp. 4182-4191, 2020.

[3] Hossain, Mohammad Asif, et al., "Comprehensive survey of machine learning approaches in cognitive radio-based vehicular ad hoc networks," *IEEE Access,* vol. 8, pp. 78054-78108, 2020.

[4] Wang, Yu, et al., "Efficient Privacy-Preserving Authentication Scheme with Fine-Grained Error Location for Cloud-Based VANET," *IEEE Transactions on Vehicular Technology,* vol. 70, no. 10, pp. 10436-10449, 2021.

[5] Khatri, Sahil, et al., "Machine learning models and techniques for VANET based traffic management: Implementation issues and challenges," *Peer-to-Peer Networking and Applications,* vol. 14, no. 3, pp. 1778-1805, 2021.

[6] Jan, Sagheer Ahmed, et al., "A Survey on Privacy-Preserving Authentication Schemes in VANETs: Attacks, Challenges and Open Issues," *IEEE Access,* vol. 9, pp. 153701-153726, 2021.

[7] Malhi, Avleen Kaur, ShaliniBatra, and Husanbir Singh Pannu, "Security of vehicular ad-hoc networks: A comprehensive survey," *Computers & Security*, vol. 89, pp. 101664, 2020.

[8] Adhikary, Kaushik, et al., "Hybrid algorithm to detect DDoS attacks in VANETs," *Wireless Personal Communications,* vol. 114,

no. 4, pp. 3613-3634, 2020.

[9] Xiao, Shunyuan, et al., "Secure Distributed Adaptive Platooning Control of Automated Vehicles Over Vehicular Ad-Hoc Networks Under Denial-of-Service Attacks," *IEEE Transactions on Cybernetics*, 2021.

[10] Kolandaisamy, Raenu, et al., "A stream position performance analysis model based on DDoS attack detection for cluster-based routing in VANET," *Journal of Ambient Intelligence and Humanized Computing,* vol. 12, no. 6, pp. 6599-6612, 2021.

[11] Fatemidokht, Hamideh, et al., "Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular Ad Hoc networks in intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems,* 2021.

[12] Mahmudova, Shafagat, "Developing an algorithm for the application of Bayesian method to software using artificial immune systems," *Soft Computing,* pp. 1-7, 2021.

[13] Lang, Wangjie, et al., "Artificial Intelligence-based Technique for Fault Detection and Diagnosis of EV Motors: A Review," *IEEE Transactions on Transportation Electrification*, 2021.

[14] Dagdia, ZainebChelly, Pavel Avdeyev, and MdShamsuzzohaBayzid, "Biological computation and computational biology: survey, challenges, and discussion," *Artificial Intelligence Review,* pp. 1-67, 2021.

[15] Kanwal, Summrina, Amir Hussain, and Kaizhu Huang, "Novel Artificial Immune Networks-based optimization of shallow machine learning (ML) classifiers." *Expert Systems with Applications,* vol. 165, pp. 113834, 2021.

[16] Zhang, Jun, et al., "Deep learning based attack detection for cyber-physical system cybersecurity: A survey, *IEEE/CAA Journal of AutomaticaSinica,* vol. 9, no. 3, pp. 377-391, 2021.

[17] Fatemidokht, Hamideh, et al., "Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular Ad Hoc networks in intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems,* 2021.

[18] Brown, James, and Mohd Anwar, "Blacksite: human-in-the-loop artificial immune system for intrusion detection in internet of things," *Human-Intelligent Systems Integration,* vol. 3, no. 1, pp. 55-67, 2021.

[19] N. Nishanth, and A. Mujeeb, "Modeling and detection of flooding-based denial-of-service attack in wireless ad hoc network using Bayesian inference," *IEEE Systems Journal,* vol. 15, no. 1, pp. 17-26, 2020.

[20] Alharthi, Abdullah, Qiang Ni, and Richard Jiang, "A Privacy-Preservation Framework based on Biometrics Blockchain (BBC) to Prevent Attacks in VANET," *IEEE Access,* 2021.

[21] M. Poongodi, et al., "Intrusion prevention system for DDoS attack on VANET with reCAPTCHA controller using information based metrics," *IEEE Access,* vol. 7, pp. 158481-158491, 2019.

[22] Yang, Anjia, et al., "DeQoS attack: Degrading quality of service in VANETs and its mitigation," *IEEE Transactions on Vehicular Technology,* vol. 68, no. 5, pp. 4834-4845, 2019.

[23] Zamani, Nurfatihah, et al., "A study on customer satisfaction towards ambiance, service and food quality in Kentucky Fried Chicken (KFC), Petaling Jaya," *Malaysian Journal of Social Sciences and Humanities (MJSSH),* vol. 5, no. 4, pp. 84-96, 2020.

[24] M. Poongodi, et al., "Intrusion prevention system for DDoS attack on VANET with reCAPTCHA controller using information based metrics," *IEEE Access,* vol. 7, pp. 158481-158491, 2019.

[25] L. Huang, “Design of an IoT DDoS attack prediction system based on data mining technology,” *J Supercomput.,* vol. 78**,** pp. 4601–4623, 2022. https://doi.org/10.1007/s11227-021-04055-1

Authors’ Profiles

Rama Mercy. S. is a temporary teaching assistant in the Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore. She involved in teaching post graduates based on cyber security in the recent years. Having 15 years of teaching experience, her areas of interest rooted in data mining, network security, cyber security and artificial intelligence. She is pursuing Ph.D as part time in cyber security.

Dr. Ganapathi Padmavathi is the Dean-School of Physical Sciences and Computational Sciences and Professor in the Department of Computer Science, Avinashilingam Institute for Home Science and Higher Education for Women (Deemed to be University), Coimbatore. She has more than 34 years of teaching experience and 26 years of research experience. Her areas of interest include Cyber Security, Wireless Communication and Real Time Systems. She has executed funded projects worth 267.368 lakhs Sponsored by AICTE, UGC, DRDO and DST. Supervised 22 scholars at Ph.D level, she has more than 200 publications in Prestigious conferences and peer-reviewed journals. She is the life members of various professional bodies like CSI, ISTE, ISCA, WSEAS, AACE and AICW. Reviewer for many IEEE Conferences and Journals. She has visited many countries for technical deliberations. She is the Course Co-ordinator for SWAYAM-MOOC on Cyber Security. So far, more than 1,13, 000 learners have enrolled for various sessions and benefitted. She has authored 10 books in Cyber Security and Data Science Domain.

Vidwan Profile Page: https://vidwan.inflibnet.ac.in/profile/132327

How to cite this paper: Rama Mercy. S., G. Padmavathi, "Self-healing AIS with Entropy Based SVM and Bayesian Aggregate Model for the Prediction and Isolation of Malicious Nodes Triggering DoS Attacks in VANET", International Journal of Computer Network and Information Security(IJCNIS), Vol.15, No.3, pp.90-105, 2023. DOI:10.5815/ijcnis.2023.03.07