I. J. Computer Network and Information Security, **2024, 3, 99-114**
Published Online on June 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2024.03.08

Encrypted Access Mapping in a Distinctly Routed Optimized Immune System to Prevent DoS Attack Variants in VANET Architecture

Rama Mercy. S.*
Avinashilingam Institute for Home Science and Higher Education for Women/ Department of Computer Science, Coimbatore, Pin/Zip code- 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/ Department of Computer Science, Coimbatore, Pin/Zip code- 641043, India
E-mail: padmavathi_cs@avinuty.ac.in
ORCID iD: https://orcid.org/0000-0002-5377-4451

Received: 16 February 2023; Revised: 27 April 2023; Accepted: 19 June 2023; Published: 08 June 2024

Abstract: The use of vehicle ad hoc networks (VANET) is increasing, VANET is a network in which two or more vehicles communicate with each other. The VANET architecture is vulnerable to various attacks, such as DoS and DDoS attacks hence various strategies were previously employed to combat these attacks, but the presence of end-to-end transparency and N-to-1 mapping of different IP addresses create failure in the blockage and not able to determine the twelve variants of DDoS attacks hence a novel technique, Encrypted Access Hex-tuple Mapping Attack detection was proposed, which uses triple random hyperbolic encryption, which performs triple random encoding to encrypt traffic signals and obtains the public key by plotting random values in hyperbola to strengthen the access control in the middlebox and Deep auto sparse impasse NN is used to detect twelve variant DDoS attacks in the VANET architecture. Moreover, to provide immunity against attack, the existing approach uses various artificial immune systems to prevent DDoS attacks but the selection of positive and negative clusters generates too many indicator packets. Hence a novel technique, Stable Automatic Optimized Cache Routing proposed, which uses a Deep trust factorization NN to detect irrational nodes without requiring prior negotiation about local outliner factor and direct evidence by automatically extracting trust factors of each node to manage the packet flows and detecting transmission of dangerous malware files in the network to prevent various types of hybrid DDoS attacks at VANET architecture. The proposed model is implemented in NS-3 to detect and prevent hybrid DDoS attacks.

Index Terms: VANET, DDoS, Hyperbolic Encryption, Middlebox, Packet Delivery Ratio, Routing, Nodes, Roadside Unit.

1. Introduction

A major problem in today's world is the traffic conjunction in major metropolitan cities which leads to traffic accidents due to human error or roadways so to overcome these problems vehicular ad hoc network (VANET) a self-organized network is used because in this architecture all the vehicles are interconnected to each other to produce a safe drive. The VANET reduces the number of collisions on the road and provides more comfortable, clean, and safer travel. However, the VANET architecture uses the internet to intercommunicate so it is vulnerable to based network attacks [1-2]. The VANET infrastructure creates communication between dynamic nodes that frequently change directions. Vehicle-to-vehicle communication inside the network is used to communicate information about alert messages and congestion in data transmission using the Roadside Unit (RSU), VANET node receives data from many RSUs, and there is the possibility of numerous hops to transport the information between the nodes. As a result, the network becomes more exposed to many types of attacks, particularly Denial of Service and Distributed Denial of Service

attacks [3-4]. DoS attacks in VANET disrupt legitimate node function by flooding packets to a specific node or network with redundant information and messages. Automated attackers to carry out large-scale DDoS attacks, blocking genuine users from accessing the network. Because of the peculiarities of the VANET design, such as shifting network node topology and decentralization, recognizing malicious assaults, disruptive nodes, and faulty vehicles is challenging [5-7].

Middleboxes are used in VANET to appropriately manage and secure its network resources. However, when end-to-end transparency is employed, any external host, including IPv4 and IPv6 hosts, could scan the entire IPv6 cellular network unless cellular carriers provide extra access control via the middlebox. As a result, an external host attacks the network by flooding packets to generate undesired traffic, acting as the attacker node in data transfer [8-10]. Furthermore, these attacker nodes act as rational nodes to produce hybrid DoS attacks, such as black hole attacks, by supplying incorrect routing information and reducing attack detection performance [11-12]. Black-hole attacks happen when all information from the router is erased. On rare occasions, a router is set up incorrectly to offer a cost-free path to every Internet destination. Previously, several Machine Learning (ML) approaches and Artificial Immune Systems (AIS) were employed to detect DDoS attacks and other hybrid threats [13-15]. However, previous systems were not focused on providing a solution for detecting various types of DDoS attacks. Furthermore, these solutions necessitate prior knowledge of critical network parameters, which adds additional load in a dynamic environment, lowering the attack detection rate and necessitating the use of an excessive number of detectors to enable secure communication. As a result, a unique framework must be developed to improve VANET security through efficient attack detection and trustworthy data transmission. The main contribution of this paper is as follows,

- To prevent hackers to penetrate the VANET architecture the presence of existing 1 to N mapping and not determining the variants of DDoS attacks is overcome by Deep auto sparse impasse NN, which is used to extract features from sensing and mapping reports in order to detect the 12 variants of DoS with blocking external host
- To prevent hybrid DDoS attacks without the selection of positive or negative clustering a novel technique Stable Automatic Optimized Cache Routing is used, in which a routing cache optimization algorithm is used to adopt time and frequency synchronized channel hopping, thereby effectively managing dynamic fluctuating constraints and transmission of dangerous malware files.

The content of the paper is structured as follows: section 2 denotes the literature survey, section 3 provides the technique and the novel solution, results obtained are provided in Section 4; finally, section 5 concludes the paper.

2. Literature Survey

Ahmed et al. [16] have presented a method that is more resistant to different attacks and attempts made by malicious code to access the entire network. It is built on a trust-management method. The scheme's goal is to find harmful data and phony nodes. The simulation results of VANSec are compared with those of trust and LT, two already existing techniques, in terms of trust computation error, end-to-end delay (EED), average link duration (ALD), and normalized routing overhead (NRO). The dependability of the proposed method, however, to jeopardise a node in the VANSec model disseminates fraudulent or faulty information.

Li et al. [17] have proposed an attack-resistant trust management system (ART) for VANETs to evaluate the trustworthiness of both data and mobile nodes in VANETs as well as to identify and react to malicious attacks. Functional trust and recommendation trust, which indicate a node's likelihood of carrying out its functionality and the veracity of its suggestions for other nodes, respectively, are the two dimensions in which node trust is assessed. Based specifically on the data sensed and gathered from multiple cars, a data trust assessment is made. But occasionally, the TrEPS may rely on murky, contradicting traffic information.

Othaman et al [18] developed Physically Safe Privacy-Preserving Message Authentication Using a Physical Unclonable Function (PUF). Even in the event of memory leakage, that protocol maintains security and privacy against passive and active attacks. The entities (i.e., vehicles, RSU) use their PUF to reassemble a secret polynomial-share in order to create pairwise temporal secret keys (PTKs) with other entities. In contrast to previous protocols, this protocol encrypts BSMs (using PTKs) to boost security and avoid vehicle tracing attacks, although it has difficulty mapping produced polynomials.

Bensaber et al. [19] developed an applied Adaptive Neuro-Fuzzy Inference System to develop a prediction model for the security index in VANET (ANFIS). The first step in the research process to build a database of attack occurrences is network simulations. After that, this latter is created and statistically evaluated. In order to achieve a high level of communication security, it is necessary to use robust routing algorithms that make it easier to detect and thwart unauthorized network intrusions in addition to secure communication frameworks.

Velayudhan et al. [20] developed the Emperor Penguin Optimization-based Routing protocol (EPORP), which aims to both detect Sybil attacks and enhance system efficiency. Improved VANET security and detection of the Sybil attack are the main objectives of the research. The original goal is achieved with the help of the Rumor riding strategy, which detects the Sybil assault in the urban VANET. The Split XOR (SXOR) process is employed like that to strengthen system security. The SXOR process employs Emperor Penguin Optimization (EPO) to aid in the creation of

the optimum key. DoS attack variations weren't found in this protocol model, though.

Aldhaheri et al. [21] develop a ground-breaking hybrid Deep Learning and Dendritic Cell Algorithm within the context of an Intrusion Detection System (DeepDCA). The framework uses the Self Normalizing Neural Network and the Dendritic Cell Algorithm (DCA) (SNNN). This study aims to categorize IoT infiltration and lessen the generation of erroneous alerts. By streamlining and automating the signal extraction process, classification performance be improved. The suggested IDS begins by choosing the most practical set of characteristics from the IoT-Bot dataset, followed by SNN signal categorization and DCA classification. This method needs too many detectors, and the system uses a negative selection technique in the sensing layer.

Raenu Kolandaisamy et al. [22] developed a DDoS attack detection based on the communication level of the entire VANET system. In this method, the source node will send data or information to the destination using immediate nodes and to minimize DDoS attacks, a proposed method of a packet marking based on adapted stream region (PMBASR) is used to trace back the source node and then the node of origin is used in the RSU server for the data request and at the same time, data will receive a response in the network. The (PMBASR) uses an analytical approach to detect DDoS attacks. This method only minimizes the DDoS attack, not prevent them.

Kaushik Adhikary et al. [23] This paper presents a hybrid detection-based algorithm based on the SVM kernel methods of AnovaDot and RBFDot for detecting DDoS attacks in VANETs. In this hybrid algorithm, features like collision, packet drop, and jitter have been used to simulate a real-time network communication scenario when the network is operating under normal conditions and a DDoS attack. This algorithm is superior in detecting DDoS attacks compared to the models based on single SVM kernel algorithms AnovaDot and RBFDot. This model only detects DDoS attacks, not prevents them.

Sousa et al [24] proposed an Intrusion Detection System (IDS) for detecting Flooding attacks in vehicular scenarios. The Network Simulator 3 (NS-3) can also be used to simulate 5G-enabled vehicle scenarios. Then create four datasets with various node, attacker, and mobility patterns taken from the Simulation of Urban MObility (SUMO) model. Each dataset included a unique scenario with a unique assortment of sender and receiver vehicles. A flooding attack was simulated in each dataset with a variable number of attackers. The resulting datasets were thoroughly merged and validated to provide accurate, precise, identifiable classification results for the flooding behaviour in the simulated scenarios (F-1 score). However, this method does not combine data from many attacks and scenarios to provide more complex information.

Gaurav et al. [25] created a DDoS detection technique that allows vehicles in the VANET to share critical information because the attacks are identified quickly. The model's fog-based DDoS detection technique. The model employs fuzzy logic to distinguish between attack and regular traffic. Only 5g networks can utilize this strategy.

Overall previous models [16] suffer from minimum reliability with inaccurate data [17] have poor connectivity due to high contradiction in traffic data [18] with low scalability issue the mapping of secret polynomial between users was difficult [19] as the routing algorithms were not robust enough the desired level security has not been possible [20] unable to find different types of attack and [21] require too many detectors to provide immunity in VANET architecture [22] minimize the DDoS attack not completely prevent them [23] only detect attack not prevent them [24] do not generate more complex data from different attacks and scenarios and [25] only used in 5g enable smart cities. Hence, there is a need for a novel DDoS attack detection system to eliminate all these limitations in the existing systems.

3. Encrypted Access Mapping in a Distinctly Routed Optimized Immune System

VANETs are vulnerable to numerous types of DDoS assaults. Various AIS strategies were previously employed in prior models to combat these attacks various Machine Learning (ML) techniques and Artificial Immune Systems (AIS) have been used previously but they have not focused on providing a solution for the detection of various forms of DDoS attacks and create an additional burden in the network environment. Hence a novel technique is proposed for Encrypted Access Hex-tuple Mapping Attack detection. Where the triple random hyperbolic encryption, performs random encoding three times to encrypt traffic signals and determine the public key by plotting random values as coefficients in hyperbola to strengthen the access control in the middlebox. Once the scanning is initiated hex-tuple matched mapping is used to map all the same IP addresses in a symmetrically matching hex-tuple value. Then Deep auto sparse impasse NN is used to extract features from the mapping report to detect twelve variants of DDoS attacks. Furthermore, to prevent these dangerous attacks various AIS techniques were used previously but they require positive or negative selection of clusters to provide immunity against DDoS attacks by arbitrarily generating too many indicator packet frames in dissimilar ways thereby not suitable for varying numbers of dangerous malware files in real-time. Hence a proposed technique Stable Automatic Optimized Cache Routing is used, in which Deep trust factorization NN detect irrational node without requiring prior negotiation and automatically extracts the trust factors of nodes. Then, the Moth Flame Optimization algorithm a population optimization algorithm used to create a balance between cluster groups with relation nodes to obtain a high packet delivery ratio without the need for positive or negative selection and Cache parallelized circulation link routing is applied to provide multiple parallelized path links in regular circular updation with adopting time and frequency synchronized channel hoping thereby effectively manage dynamically fluctuating constraints and transmission of dangerous malware files. Hence by preventing hybrid DoS attacks, the proposed model is used to detect and prevent various types of DDoS attacks.

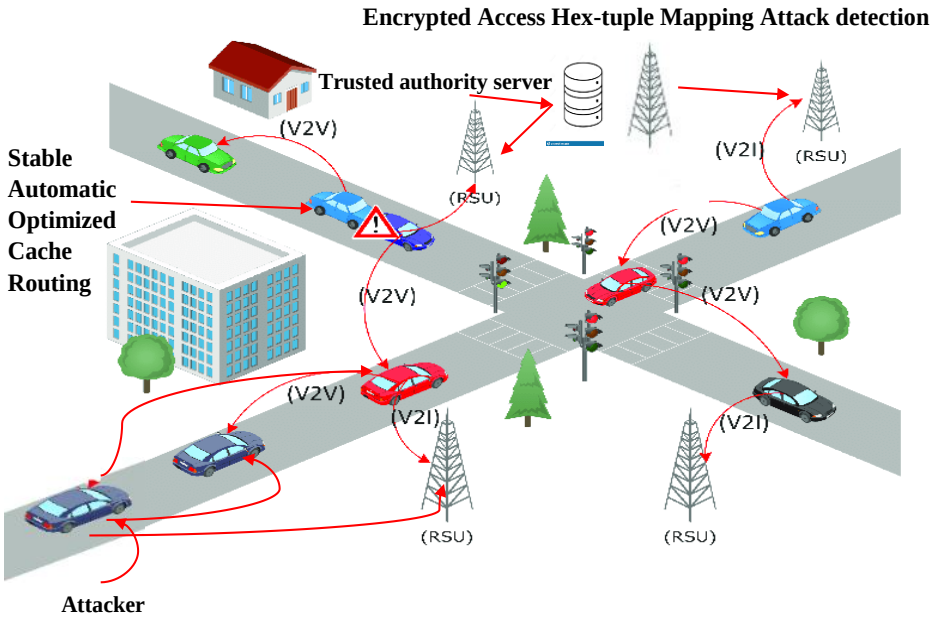

Fig.1. Block diagram for encrypted access mapping in a distinctly routed optimized immune system

Fig. 1 depicted the block diagram for the proposed model. The proposed model for Encrypted Access Mapping in a Distinctly Routed Optimized Immune system initially uses two methods for the detection and prevention of DDoS attacks. The Encrypted Access Hex-tuple Mapping Attack detection is used to perform a triple random hyperbolic encryption and map all the IP addresses in a systematic tuple value and uses Deep auto sparse impasse NN to extract information to detect twelve variants of DDoS attack. Stable Automatic optimized cache routing, which use deep trust factorization NN to detect irrational node without negating outline factor and direction. Then, the Moth Flame Optimization algorithm is used to collect and obtain a high packet delivery ratio, and Cache parallelized circulation link routing is used to manage dynamically fluctuating constraints and transmission of dangerous malware files hence preventing DDoS attacks.

3.1. Encrypted Access Hex-tuple Mapping Attack Detection

The traffic signals within the network are encrypted using triple random hyperbolic encryption, which performs an encoding three times to encrypt all the traffic in the VANET network and plot the values as a coefficient in a hyperbola to determine the public key. The architecture of Encrypted Access Hex-tuple Mapping Attack detection has been shown in fig. 2.

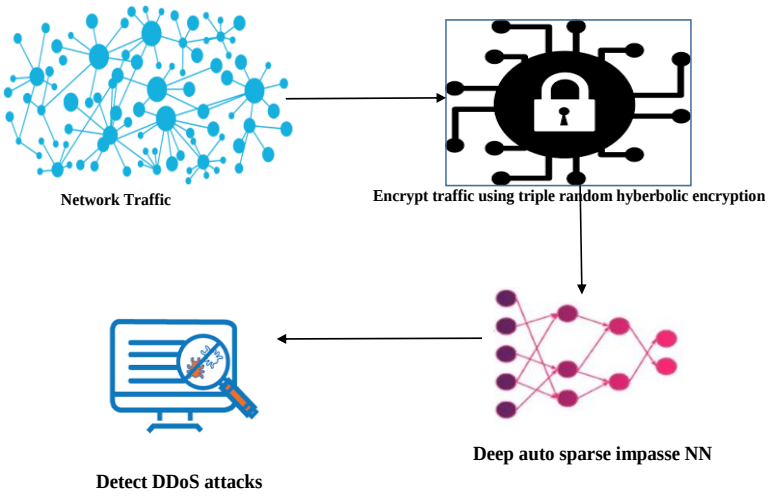

Fig.2. Block diagram for encrypted access hex-tuple mapping attack detection

In hyperbolic encryption to choose the coefficient the equation (1) follows:

$$x^2 - Dy^2 = 1 \tag{1}$$

The equation (1) is equation of hyperbola, and pick a base point $G = (x_0, y_0)$ with a large order r and this gives us $G^r = E$ and select an integer m and $m < r$ computes $B = G^m mod\ 2$, the private keys are formed by (G,B). In encryption process choose the secret integer k and Computes in following equation (2) & (3)

$$H = G^k mod\ n \tag{2}$$

$$T = B^k w mod\ n \tag{3}$$

The equation (2) and (3) produce the cipher text (H, T) and in decryption process the is compute as following equation:

$$R = H^m mod\ n \tag{4}$$

The data is recovered by the following equation:

$$w = T / R mod\ n \tag{5}$$

The proposed model uses a process called hex tuple matched mapping to map all the network resources such as source IP, destination IP, source port number, destination port number, public key, and IP address range in an N to N mapping. The mapping structure is shown in figure 3 and the mapping of the IP address in a tuple means the value is immutable.

Node:1 IP:192.168.0.1 Source IP: 192.168.0.3 Destination Source port: 4356 Destination port:8975 IP:192.168.0.10 MAC:44:02:EF:9C:09:4E Public key: C*F-JaNdRgUkXp2s5v8y/A?D(G+KbPeS	Node:2 IP:192.168.0.2 Source IP:192.168.0.7 Destination IP: 192.168.0.17 Source port: 4595 Destination port:7885 MAC:A9:4E:47:AC:DA:B9 Public key: C*F-JaNdRgUkXp2s5v8y/A?D(G+KbPeS	Node:3 IP:192.168.0.3 Source IP:192.168.0.1 Destination IP:192.168.0.8 Source port: 4686 Destination port: 8549 MAC:8C:9D:39:67:4C:59 Public key: C*F-JaNdRgUkXp2s5v8y/A?D(G+KbPeS	Node: N IP:N Source IP:N Destination IP:N MAC:N Source port: N Destination port: N Public key: C*F-JaNdRgUkXp2s5v8y/A?D(G+KbPeS

Fig.3. The value stored in hex tuple mapping

The discovery of misconfiguration in the middle box will lead to performance degradation making it vulnerable to attacks. In the proposed model, the middlebox is used to control the nodes and does N to 1 mapping IP address. To detect twelve variants of hybrid DDoS attacks by blocking external hosts and so provide end-to-end network transparency, the Encrypted Access Hex-tuple Mapping Attack Detection model uses Deep Auto Sparse Impasse NN, which gathers the data from sensing and mapping reports to detect the attacker node on the network. The diagram of Deep Auto Spare Impasse NN is given in fig. 4.

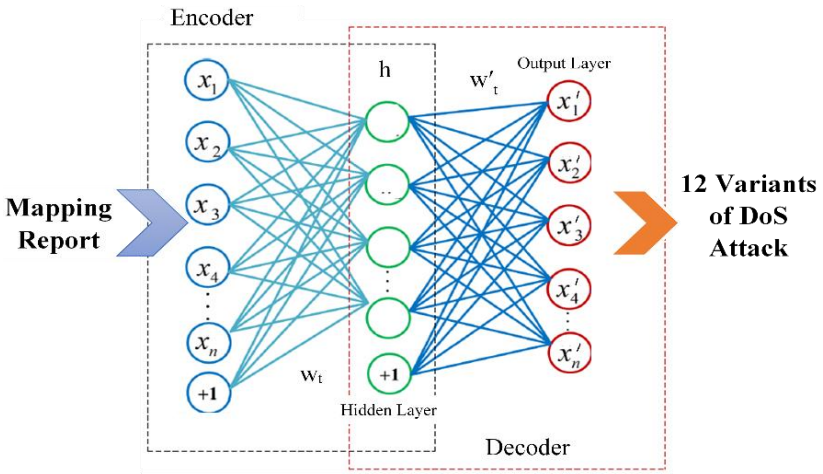

Fig.4. Deep auto sparse impasse NN

The Deep Auto Sparse Impasse Neural Network is a type of structure made up of numerous basic neurons acting as nodes or elements. These components are constantly working together in parallel. The connections between the neurons have a significant role in how the Deep Auto Sparse Impasse Neural Network functions. These neurons are linked together via links, and each link has weights that are adjustable values. The neural network consists of the input layer in which the mapping report is sent as an input and the connection between the neurons in the neural network is close to zero because if there is more connection between neurons it takes more memory and the connections do not affect the accuracy of the neural network. The prediction speed of the neural network is twenty-five times faster than a regular neural network.

When dealing with Deep Auto Sparse Impasse neural networks, the number of layers and nodes are chosen using similar concepts as in standard neural networks, but there are several concerns that are unique to these sparse networks. Neurons are grouped logically in three layers that make up the Deep Auto Sparse Impasse NN. The Deep Auto Sparse Impasse NN has three layers (the input layer, the hidden layer and the output layer), one neuron in the output layer, and a variable number of neurons in the hidden layer. The values of each output vector member fall between [-1,1]. Neurons on both layers have "tan-sigmoid" transfer functions. This function condenses the result into the range [-1,1] from an input that can be any value between plus and minus infinity. The Deep Auto Sparse Impasse NN contains fewer active connections or parameters, resulting in more efficient and interpretable models. Which connections are present and which are pruned or set to zero are determined by the sparsity pattern. The pruning approach used in this sparse neural network eliminates the superfluous connections and reduces the number of parameters.

The unformatted training set is used in the Auto Sparse Impasse NN to provide the mapping report as the auto-encoder input data and it is shown in equation (6) below

$$x = (x_1, x_2, x_3, ..., x_n) \tag{6}$$

The hidden and output layer neurons are activated by sigmoidal activation function which is shown in the below equation (7)

$$g(s_k) = \frac{1}{1+e^{-s_k}} \tag{7}$$

where, s_k represents the cumulative input signal of the k-th neuron in the hidden or output layer of the NN and it is given in equation (8) below,

$$s_k = \sum_{i=1}^{n} (w_{i,k}\ x_{i,k} + x_0\ f_k) \tag{8}$$

where, $w_{i,k}$ is the the link weight from the previous layer's i-th neuron to the hidden or output layer's k-th neuron, x_0 is the input link weight of neuron and the offset of k-th neuron is represented by f_k.

The below equation (9) shows the output data signal from the neural network having L number of neural layers,

$$h_{w,f}(x) = A^{(L)} \tag{9}$$

where, $A^{(L)}$ is the value array of output layer neuron.

The twelve variants of DDoS attack are identified and predicted by this Sparse Impasse output layer. Only a subset of connections or weights is active in the Deep Auto Sparse Impasse NN, with the remainder set to zero. Because zero-valued connections do not need to be processed, this sparsity minimizes computing costs during training and inference. Consequently, fewer procedures are needed, resulting in quicker training time and this NN has a high prediction accuracy for DDoS attacks. The mode used detects NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebDDoS, SYN, and TFTP DDoS attacks.

3.2. Stable Automatic Optimized Cache Routing

To detect the node that causes hybrid DDoS attack is detected and to provide immunity to DDoS attacks in the network, a novel method of Stable automatic optimization is used in which Deep trust factorization NN is used in which the nodes are connected using a trust score and provides access to nodes based on the trust score which is shown in fig. 5.

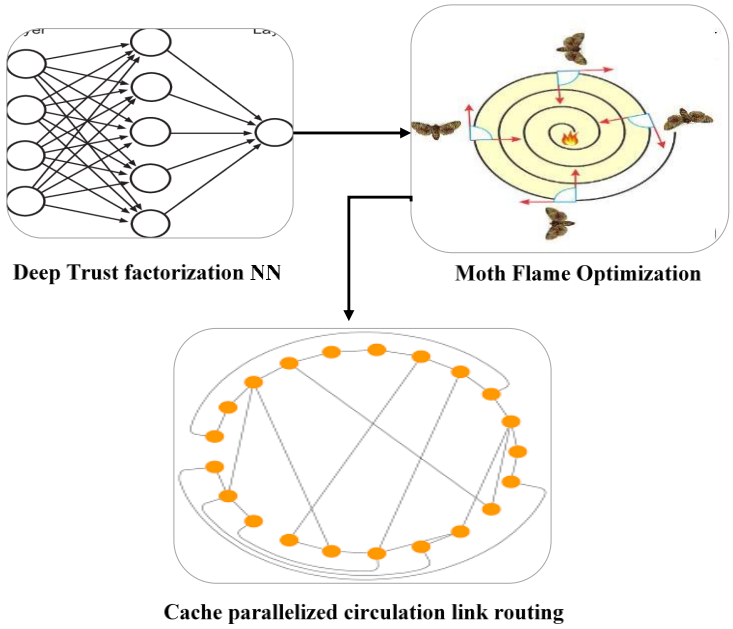

Fig.5. Block diagram for stable automatic optimized cache routing

The architectural diagram of Deep trust factorization NN has been shown in fig. 6 that is responsible for detecting the trust values thereby it predicts the rational nodes.

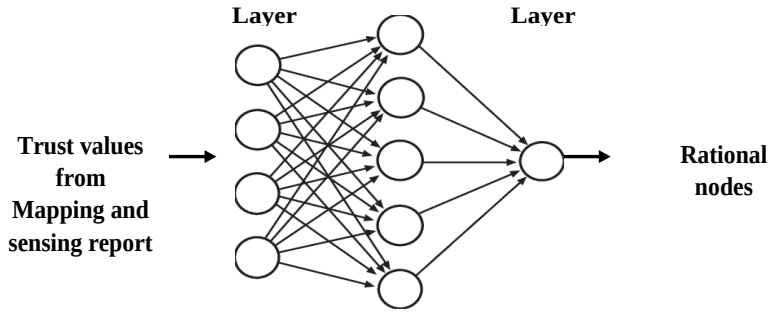

Fig.6. Deep trust factorization NN

In fig. 6 the structure of Deep trust factorization NN is given and the neural network consists of an input layer, a hidden layer, and one output layer. The data gathered from the detection of the DDoS attack is used to give the input in trust factorization. The output layer consists of one layer to ensure whether the node is trusted or not by the trust score added to each node by the hidden layer. Then, the Moth Flame Optimization algorithm is used to form a balanced cluster group and relation node to obtain the maximum packet delivery ratio (PDR). To ensure the connectivity of each node in the cluster group, the Moth Flame optimization algorithm is a population-based algorithm used to detect the best path in the network by updating each position in the node. Three different functions are used in the optimization of the proposed model as follows:

$$M = (I, P, T) \tag{10}$$

In equation (10) I refers to the random location of the vehicle node $(I : \phi \rightarrow \{M\})$, P refers to the motion of the vehicle node in the search space $(P : M \rightarrow M)$, T refers to finish the search process $(T : M \rightarrow \text{true, false})$ and the following represent the I function:

$$M(i, j) = (ub(i) - lb(j)) \times rand\ (j) + lb(i) \tag{11}$$

In equation (11) lb and ub indicate the lower and upper bounds of the variable. The search takes place in transverse orientation the spiral initial point should start from the vehicle node and the spiral final point should be positioned next vehicle node and fluctuation of range should not exceed search space. The spiral equation follows as.

$$S(M_i, F_j) = D_i . e^{bt} . cos(2\pi t) + F_j \tag{12}$$

In equation (12) the D_i refer to the space between the i^{th} node and j^{th} node, b indicates a fix to define the shape of the logarithmic spiral, and t indicates a random number between $[-1,1]$. The balancing between exploitation and exploration is guaranteed by the spiral motion of the node near the next node in the search space. The moth Flame optimization algorithm is given below.

Algorithm: Moth Flame Optimization Algorithm

Initialize the parameters for the vehicle
Initialize the vehicle at a position M_i randomly
for $i = 1$ to n **do**
  calculate the fitness function f_i
end for
while iteration ≤ Max_iteration **do**
  Update the position of M_i
  Calculate the number of vehicles
  Evaluate the fitness function f_i
if $iteration == 1$ **then**
  $F = sort(M_{t-1}, M_t)$ and $OF = sort(M_{t-1}, M_t)$
end if
for $i = 1$ to n **do**
 for $j = 1$ to **do**
  update the values of r and t
  calculate the value of D concerning its corresponding vehicle
  update $M(i.j)$ respect to its corresponding moth using
  end for
 end for
end while

The algorithm initials with a vehicle and M_i a random vehicle. The iteration took place to detect paths with a high packet delivery ratio (PDR). The Cache parallelized circulation link routing is applied to make time and frequency synchronization base channel hopping on a network to effectively manage the dynamic fluctuation of each node and remove the transmission of dangerous malware files on the network. The method eradication of the twelve variants of hybrid DDoS attacks without reducing the high packet delivery. The circular routing process packet and hoping process on circular link state is a process of the nodes instead of changing the channel randomly each node knows the sequence where they should be and is always able to communicate. The proposed optimization algorithm connects the node in the circular link to make the nodes in regular circular updation with effective hopping between one node and another node.

Overall, the Encrypted Access Mapping in a Distinctly routed Optimized Immune System has been proposed to provide immunity to the VANET network against the twelve types of hybrid DDoS attack by Encrypted Access Hex-tuple Mapping Attack detection, a process in which all the traffic in the network is encrypted using triple random hyperbolic encryption and the middlebox does the N to 1 mapping of IP address. The Stable Automatic Optimized Cache Routing used deep trust factorization NN to detect the irrational node by adding the trust score and Moth Flame Optimization algorithm to obtain the high packet delivery ratio. The Cache parallelized circulation link routing is applied to synchronize the time and frequency of each node, therefore, eliminating the malicious traffic in the network. So, the proposed model provides immunity to the DDoS attacks on the VANET architecture.

4. Result and Discussion

This section includes a thorough analysis of the performance of the proposed network model, the implementation results simulated in the NS-3 platform, and a comparison section to make sure the proposed model is immune to DoS attacks.

4.1. Experimental Setup

The proposed system is simulated in Python and this section provides a detailed description of the implementation results and the performance of the proposed system and a comparison section to ensure that the proposed system performs valuable.

Software: NS-3
OS: Windows 10 (64-bit)
Processor: Intel i3

RAM: 8GB RAM

4.2. Dataset Description

The dataset used in the proposed model is CICDDoS2019. The dataset contains the most common DDoS attacks, which resemble true real-world data. It also includes the result of the network traffic analysis using CICFlowMeter-V3 with labeled flows based on the time stamp, source, destination IP address, protocols, and attack (CSV files). This dataset has different modern reflective DDoS attacks such as NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebDDoS, SYN, and TFTP. The dataset itself is organized per day and the raw data is captured by the Pcaps. This data set is used in the proposed model to detect the DDoS attack on the VANET architecture.

4.3. Simulated Output of Proposed Model

The simulated output of the proposed model for attack detection and prevention has been explained in this section from initial setup itself.

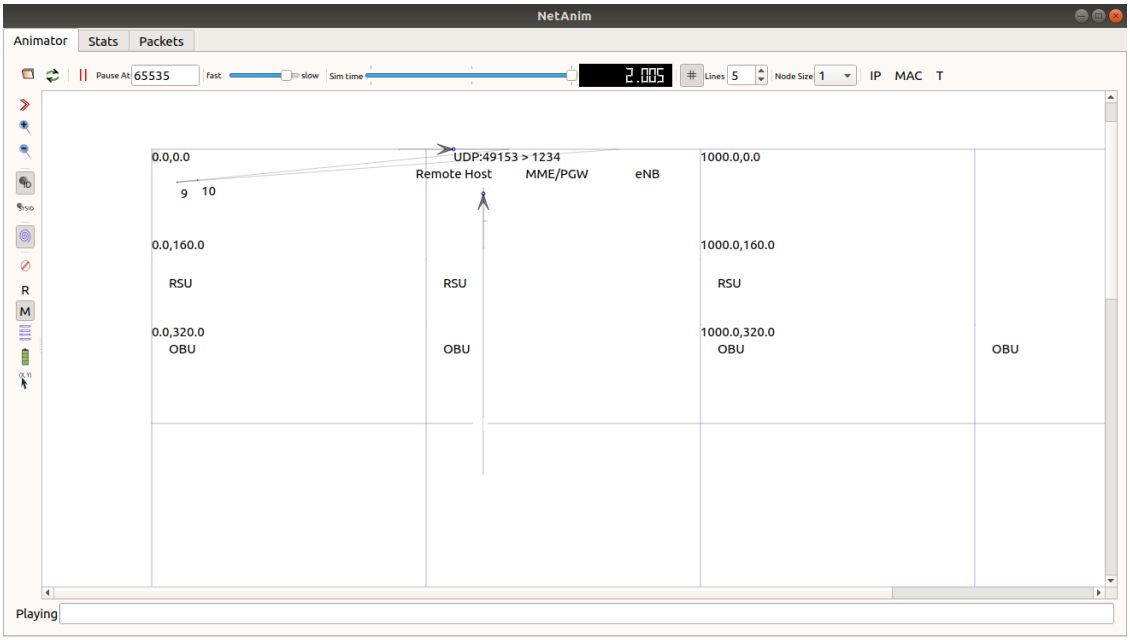

Fig.7. Simulation of the proposed model in NS-3

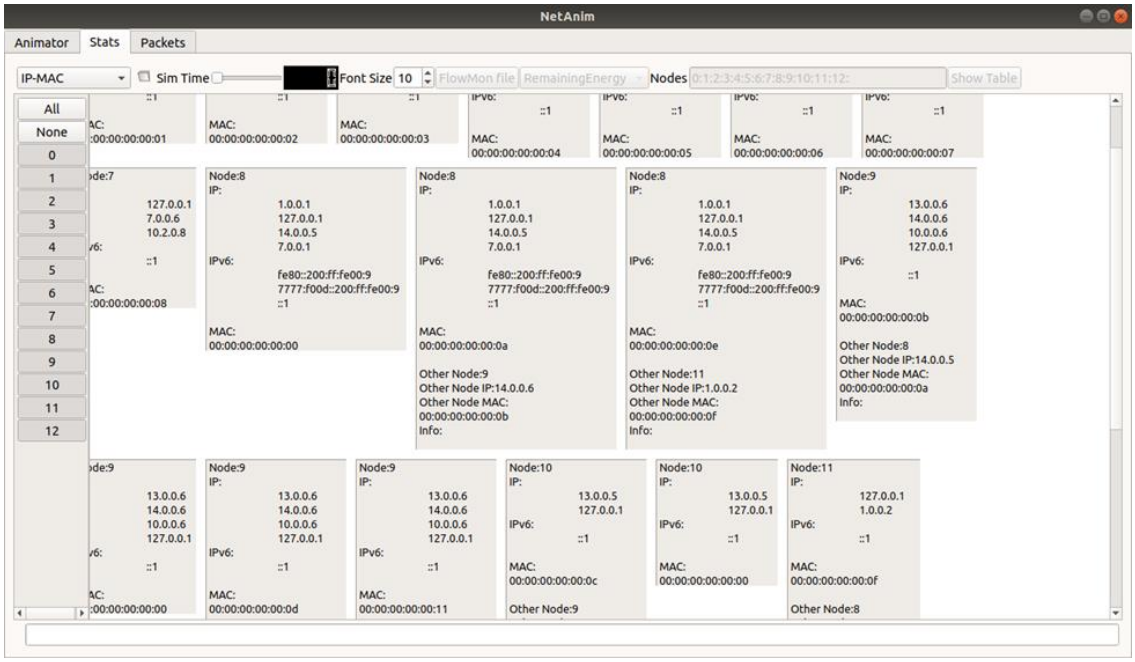

Fig.8. Statistics of the proposed model in NS-3

The animation of the proposed model is shown in fig. 7, an overall architecture of VANET. The main architecture of VANET consists of a Board Unit (OBU), which allows the vehicles to communicate with Road side unit (RSU) or other OBU, and the figure shows the number of nodes that are interconnected to each other. They represent the data flow from each node in fig. 4.

The network status of each node in the proposed system is given in fig. 8. The statistics of each node include the Media Access Control (MAC), IPv4 address, IPv6 address, and the details of the node connected. The proposed model uses triple random hyperbolic encryption to encrypt the traffic and deep auto sparse impasse NN to map the report to detect the DDoS attacks.

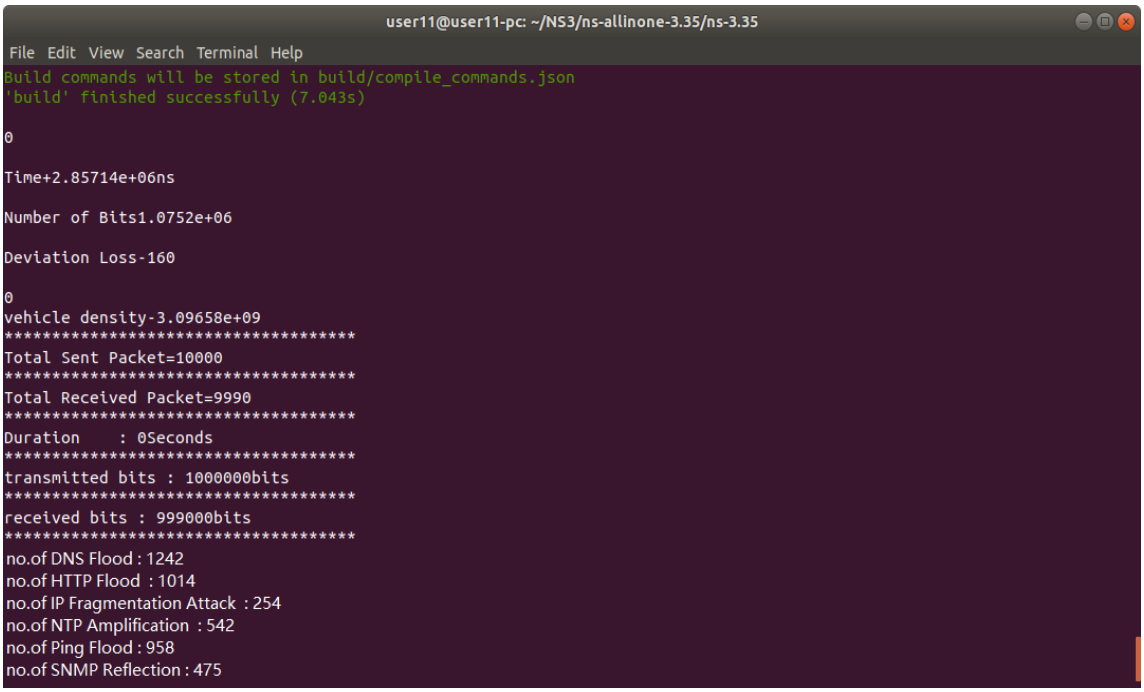

Fig.9. Output of the simulation

In fig. 9 the output simulation of the proposed system is given and it indicates the number of bits transferred in the time and the deviation loss or packet loss on the network. the vehicle density is how close the vehicle gets to and the total packets send & received in the network, the duration indicates the time taken to send & receive the packets. The output also indicates the number of requests sends to cause DDoS attacks such as DNS flood, HTTP flood, fragmentation attack, NTP amplification, Ping flood, and SNMP reflection, and the proposed model is able to detect twelve types of DDoS attacks and protect the network from packet loss and other hybrid attacks.

4.4. Performance Metrics of the Proposed System

The performance of the proposed approach and the achieved outcome was explained in detail. This section is to explain the proposed model detection of various types of DDoS attacks such as UDP Flood, DNS Flood, HTTP, NTP, Ping Flood, SNMP, SYN flood, Smurf, LDAP, MSSQL, NetBIOS, SSDP, WebDDoS and TFTP.

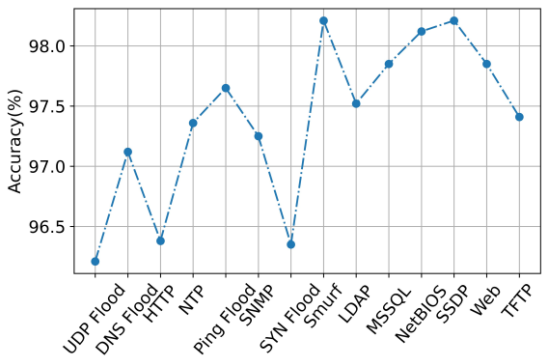

Fig.10. Accuracy of the proposed model in the prediction of different types of DDoS attacks

The graph in fig. 10 shows the accuracy of the proposed model as it detects UDP Flood with 96.2% accuracy, DNS Flood with 97.2% accuracy, HTTP with 96.4% accuracy, NTP with 97.45% accuracy, Ping Flood with 97.7% accuracy,

SNMP with 97.35% accuracy, SYN flood with 96.4% accuracy, Smurf with 98.4% accuracy, LDAP with 97.5% accuracy, MSSQL with 97.5% accuracy, NetBIOS with 98.2% accuracy, SSDP with 98.4% accuracy, WebDDoS with 97.7% accuracy and TFTP with 97.45% accuracy. The proposed model has high accuracy because 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.

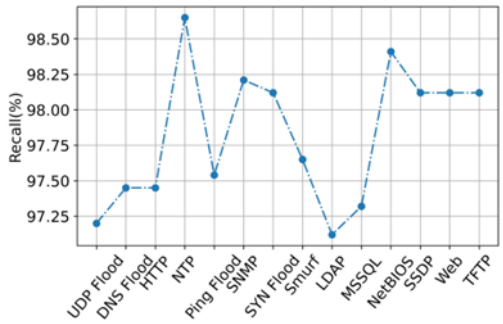

Fig.11. The recall of the proposed model in detecting different types of DDoS attacks

The graph in fig. 11 shows the recall of the proposed model as the graph explains the model detects UDP Flood with 97.2% recall, DNS Flood with 97.45% recall, HTTP with 97.45% recall, NTP with 98.65% recall, Ping Flood with 97.53% recall, SNMP with 98.2% recall, SYN flood with 98.15% recall, Smurf with 97.67% recall, LDAP with 97.15% recall, MSSQL with 97.3% recall, NetBIOS with 98.45% recall, SSDP with 98.15% recall, WebDDoS with 98.15% recall and TFTP with 98.15% recall. The proposed model Encrypted Access Hex-tuple Mapping Attack detection has high recall because it uses hex-tuple mapping in which the same IP address is mapped using a hex tuple value.

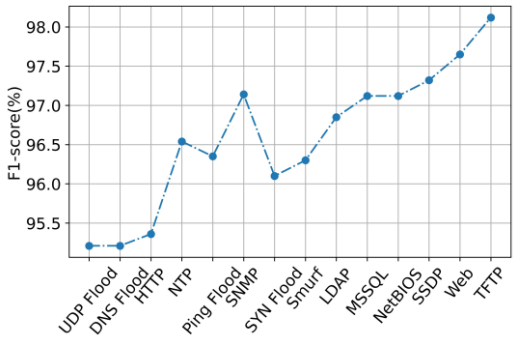

Fig.12. F1-Score of the proposed model

The F1-Score of the proposed model is shown in fig. 12, F1-Score is used to calculate the mean of precision and recall. The proposed model detects UDP Flood with 95.2% F1-Score, DNS Flood with 95.2% F1-Score, HTTP with 95.45% F1-Score, NTP with 96.5% F1-Score, Ping Flood with 96.4% F1-Score, SNMP with 97.2% F1-Score, SYN flood with 96.15% F1-Score, Smurf with 96.4% F1-Score, LDAP with 96.85% F1-Score, MSSQL with 97.1% F1-Score, NetBIOS with 97.1% F1-Score, SSDP with 97.4% F1-Score, WebDDoS with 97.6% F1-Score and TFTP with 98.15% F1-Score. The proposed model has high F1-Score because it uses the Encrypted Access Hex-tuple Mapping Attack detection which uses a Deep auto sparse neural network to detect various hybrid DDoS attacks.

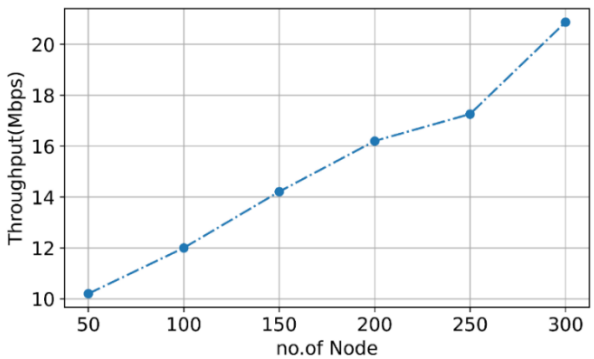

Fig.13. The throughput of the proposed system

The throughput is the amount of information that the system process in a given time the throughput of the proposed model is given in fig. 13. The number of nodes in the proposed model increases the throughput of the amount of data the network takes to transfer also increases. The time taken for the packet to transfer is 0 seconds because the proposed model uses 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.

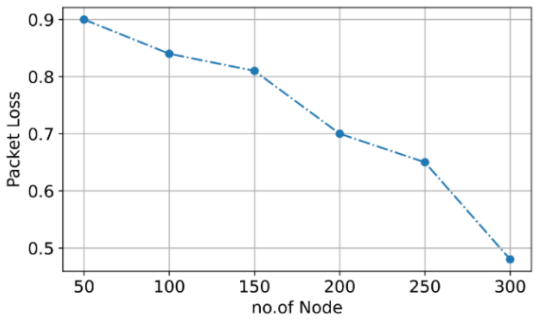

Fig.14. The packet loss of the proposed model

In fig. 14, the graph for packet loss of the proposed model is given. The proposed model has very low packet loss. The graph indicates the packet loss at the 50 nodes present in the VANET. The packet loss for each node is 0.9 bits, and as the number of nodes increases, the packet loss for each node increase to 300 the packet loss for each node decrease to 0.5 bits. The proposed model has low packet loss because the novel solution Stable Automatic Optimized Cache Routing uses Cache parallelized circulation link routing to effectively route the packages to minimize the packet loss.

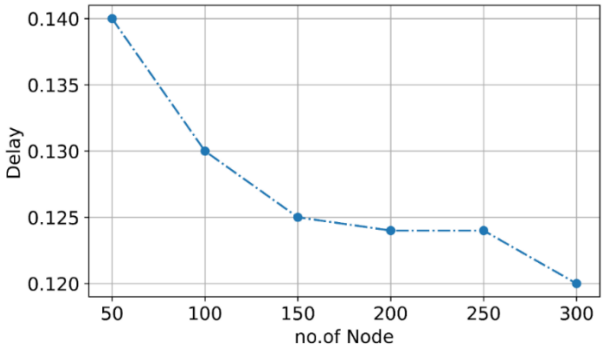

Fig.15. The delay of a packet in the proposed model

The delay in a network is known as lag or latency amount of time taken for the packet to travel through multiple nodes. The delay of the proposed model is given in fig. 15. The graph indicates the proposed model has a low delay of 0.14 seconds for 50 nodes; when the node value increases to 300 nodes, the delay decreases to 0.12 seconds. The proposed model has low delay because of a novel approach Stable Automatic Optimized Cache Routing which uses circular link state routing in which a time and frequency-based channel hopping takes place to minimize the packet delay.

4.5. Comparison Results of the Proposed Network Model

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) [11].

The comparison of the packet delivery ratio of various models is shown in fig. 16. The packet delivery ratio of the proposed model is compared with the existing models such as Trilateral trust, H-IDS, Multi filter and SPPA. From the graphical representation, when the number of nodes increased, the packet delivery ratio of the proposed system also increased. When the proposed model's number of node is 20, the packet delivery ratio of the proposed model attains at 5%. The proposed model has high packet deliver ratio of 98% than existing models even though the number of nodes increased. The graph is used to assume that the model Trilateral trust has the least packet delivery ratio. The proposed model has a high packet delivery ratio because of the novel technique of Stable Automatic Optimized Cache Routing.

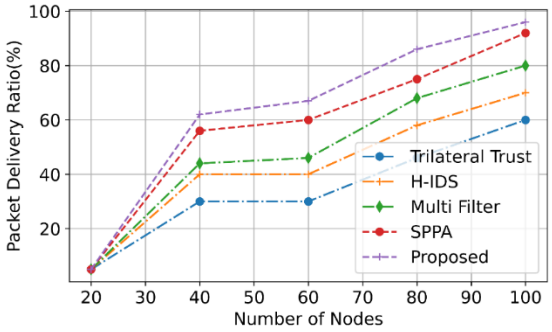

Fig.16. The packet delivery ratio comparison

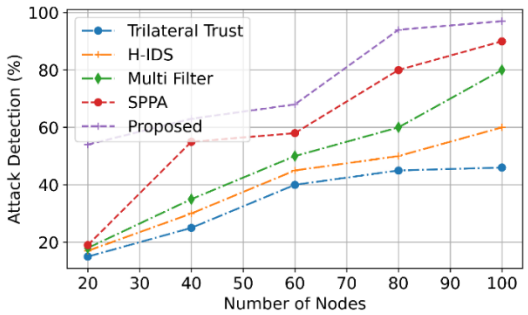

Fig.17. The attack detection comparison proposed model

The comparison of attack detection of various models is shown in fig. 17. The attack detection of the proposed model is compared with the existing models such as Trilateral trust, H-IDS, Multi filter and SPPA. From the graphical representation, when the number of nodes increased, the attack detection of the proposed system also increased. When the proposed model's number of node is 20, the attack detection of the proposed model attains at 55%. The proposed model has high attack detection accuracy of 99% than existing models when the number of nodes is 100. The graph also indicates the attack detection of an increase in the number of nodes has no deviation in detection accuracy. The graph used to assume that the model Trilateral trust has the least accuracy in attack detection. The proposed model has high attack detection accuracy because of the novel technique of Encrypted Access Hex-tuple Mapping Attack detection.

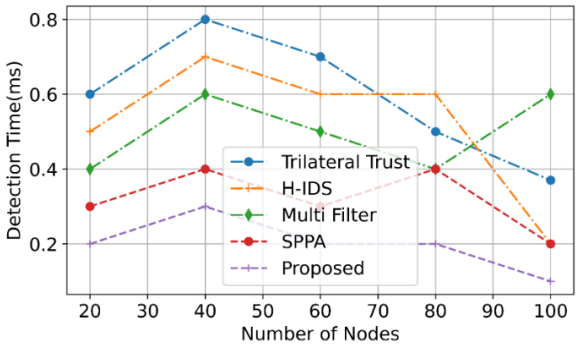

Fig.18. The comparison of time taken to detect the DDoS attacks in the proposed model

The comparison of time taken to detect various DDoS attacks in the previous model is shown in fig. 18. The detection time of the proposed model is compared with the existing models such as Trilateral trust, H-IDS, Multi filter and SPPA. When the proposed models number of node is 20, the detection time of the proposed model attains at 0.6ms. when the number of nodes increases, the proposed model takes less time to detect DDoS attacks of 0.2 *ms* that's extremely fast than existing models. The graph used to assume that the model Multi filter has taken more time to detect DDoS attacks than other models. The proposed model takes less time to detect DDoS attacks because of the proposed novel technique Encrypted Access Hex-tuple Mapping Attack detection.

The routing overhead is the amount of packet taken to check whether the neighbor node is active. Fig. 19 shows that the proposed model has a very low routing overhead than the existing model. The routing overhead of the proposed model is compared with the existing models such as Trilateral trust, H-IDS, Multi filter and SPPA. From the graphical representation, when the number of nodes increased, the routing overhead of the proposed system also increased. When the proposed models number of node is 20, the routing overhead of the proposed model attains at 225 packets. The

routing overhead of the proposed model, even after the number of node increase to 100, is still around 650 packets. The graph used to assume that the model. Trilateral trust has a very high routing overhead. The proposed model has very low routing overhead because of the novel solution Stable Automatic Optimized Cache Routing.

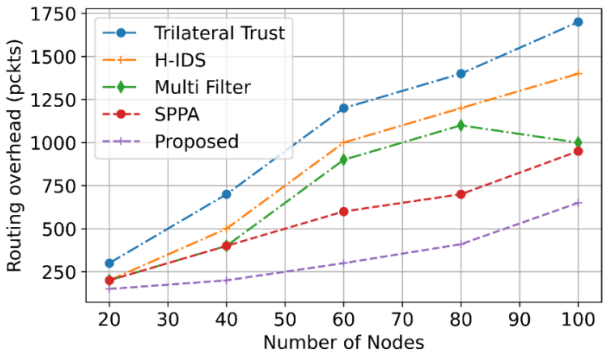

Fig.19. The routing overhead comparison

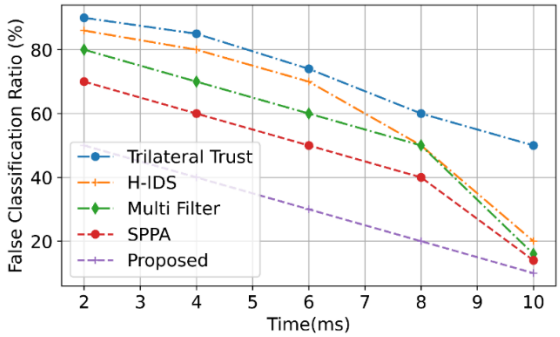

Fig.20. Comparison of false classification ratio

The false classification ratio is the number of negative cases mistakenly reported as positive. Fig. 20 shows that the proposed model has a low false classification ratio of 5%. The false classification ratio of the proposed model is compared with the existing models such as Trilateral trust, H-IDS, Multi filter and SPPA. From the graphical representation, when the time (ms) is increased, the false classification ratio of the proposed system is decreased. When the proposed models time is at 2ms, the false classification ratio of the proposed model attains at 225 packets. If the number of ms increase, the proposed model still has a very low false classification ratio. The Trilateral trust has a very high false classification ratio. The proposed model has a very low false classification ratio because of the novel solution novel technique, Encrypted Access Hex-tuple Mapping Attack detection.

Table 1. Overall table for the comparison of the previous model and the proposed model

Methods	Packet delivery ratio	Attack detection accuracy	Detection time	Routing overhead	False Classification ratio
Trilateral trust	60%	42%	0.3 ***ms***	1700 ***pkt***	50%
A host-based intrusion detection system (H-IDS)	70%	60%	0.2 ***ms***	1400 ***pkt***	20%
Multi filter	80%	80%	0.6 ***ms***	1000 ***pkt***	15%
Stream position performance analysis (SPPA)	90%	90%	0.2 ***ms***	990 ***pkt***	10%
Proposed	98%	99%	0.1 ***ms***	600 ***pkt***	5%

Table 1 gives the overall data of the comparison between the previous and proposed models. The proposed model is more effective and relevant when compared to the existing technologies, in which the other models have not acquired a high attack prediction ratio and the proposed model also has an efficient routing protocol to reduce routing overhead and ensure a high packet delivery ratio.

In the result area from the proposed methodology, a comparison is made with the previous study, and the techniques were explained using graphs. 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.

5. Conclusions

The various types of DDoS attacks are carried out in vehicle ad hoc networks (VANET) thus it is essential to detect and prevent the attacks. To detect DDoS attacks, a novel attack detection framework is proposed in which Encrypted Access Hex-tuple Mapping Attack detection and Stable Automatic Optimized Cache Routing are used to provide immunity against DDoS attacks in the network. The Encrypted Access Hex-tuple Mapping Attack detection uses Triple random hyperbolic encryption to encode the traffic three times in a random manner and plot the values in co-efficient in hyperbolic encryption to determine the public key. The Hex-tuple Matched Mapping approach uses a Deep auto sparse impasse NN to map the IP addresses in hex tuple values and extract the features from the mapping report and classifies the twelve variants of DDoS attacks and arrest external hosts so as to prevent unauthorized access, interception, and interference with sensitive information and communication nodes. With this proposed attack detection approach, the detection time has been reduced and found to be 0.2 ms for 20 nodes when compared to other existing attack detection approaches. The accuracy of the proposed model is 96.2% for UDP flood detection, 97.2% for DNS flood detection, 96.4% for HTTP flood detection, 97.45% for NTP flood detection, 97.7% for Ping flood detection, 97.35% for SNMP flood detection, 96.4% for SYN flood detection, 98.4% for Smurf flood detection, 97.5% for LDAP flood detection, 97.5% for MSSQL flood detection. The recall of the proposed model identifies UDP Flood with 97.2% recall, DNS Flood with 97.45% recall, HTTP with 97.45% recall, NTP with 98.65% recall, Ping Flood with 97.53% recall, SNMP with 98.2% recall, SYN flood with 98.15% recall, Smurf with 97.67% recall, LDAP with 97.15% recall, MSSQL with 97.3% recall, NetBIOS with 98.45% recall, SSDP with 98.15% recall, WebDDoS with 98.15% recall and TFTP with 98.15% recall. The mean of recall and precision is computed using the F1-Score. The proposed model detects UDP Flood with 95.2% F1-Score, DNS Flood with 95.2% F1-Score, HTTP with 95.45% F1-Score, NTP with 96.5% F1-Score, Ping Flood with 96.4% F1-Score, SNMP with 97.2% F1-Score, SYN flood with 96.15% F1-Score, Smurf with 96.4% F1-Score, LDAP with 96.85% F1-Score, MSSQL with 97.1% F1-Score, NetBIOS with 97.1% F1-Score, SSDP with 97.4% F1-Score, WebDDoS with 97.6% F1-Score and TFTP with 98.15% F1-Score. Then the Stable automatic optimized cache routing is introduced in which Deep trust factorization NN adds trust value for each node and the moth flame optimization is used to form a balance between the cluster to produce the high packet deliver ratio of 98% thereby detecting the malicious nodes and ensuring the linkage of each node in the cluster. Cache parallelized circulation link routing is used to provide multiple parallelized paths to each node and time and frequency synchronization to packets thereby removing unwanted traffic from the network so the response time of each node is reduced to 0.1 ms. The proposed model detects the twelve variant DDoS attacks with an accuracy of 99% and less detection time of 0.1ms and thereby outperforming all other existing techniques. This framework creates a baseline of typical VANET operation and detects any substantial abnormalities, such as a rapid increase in traffic or unexpected communication patterns. This can prevent these anomalies and signal the presence of a DDoS assault by monitoring network flow and detecting rapid spikes in packet rates, strange packet sizes, or aberrant traffic patterns thereby prompting the implementation of suitable corrective measures. As a result, the proposed model achieves 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%. This approach can be used in the practical applications such as Road Transport Emergency Services that employ VANET communications by broadcasting the road safety warning and status information to cut down on delays and hasten emergency rescue operations in order to save the lives of individuals who have been injured.

References

[1] R. Shrestha, R. Bajracharya, A. P. Shrestha and S. Y. Nam, "A new type of blockchain for secure message exchange in VANET," *Digital communications and networks,* vol. 6, no. 2, pp. 177-186, 2020.

[2] A. K. Kazi, S. M. Khan and N. G. Haider, "Reliable group of vehicles (RGoV) in VANET," *IEEE Access,* vol. 9, pp. 111407-111416, 2021.

[3] A. Ilavendhan and K. Saruladha, "Comparative analysis of various approaches for DoS attack detection in VANETs," *In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC) IEEE,* pp. 821-825, July 2020.

[4] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," *Cybersecurity,* vol. 4, no. 1, pp. 1-27, 2021.

[5] I. O. Olayode, L. K. Tartibu and M. O. Okwu, "Application of Fuzzy Mamdani Model for effective prediction of traffic flow of vehicles at signalized road intersections," *In 2021 IEEE 12th International Conference on Mechanical and Intelligent Manufacturing Technologies (ICMIMT) IEEE,* pp. 219-224, May 2021.

[6] M. A. Al-Absi, A. A. Al-Absi and H. J. Lee, "Comparison between DSRC and other Short Range Wireless Communication Technologies," *In 2020 22nd International Conference on Advanced Communication Technology (ICACT) IEEE,* pp. 1-5, February 2020.

[7] N. Ganeshkumar and S. Kumar, "Obu (on-board unit) wireless devices in vanet (s) for effective communication—A review," *Computational Methods and Data Engineering,* pp. 191-202, 2021.

[8] M. Poongodi, V. Vijayakumar, F. Al-Turjman, M. Hamdi and M. Ma, "Intrusion prevention system for DDoS attack on VANET with reCAPTCHA controller using information based metrics," *IEEE Access,* vol. 7, pp. 158481-158491, 2019.

[9] M. Poongodi, M. Hamdi, A. Sharma, M. Ma and P. K. Singh, "DDoS detection mechanism using trust-based evaluation system in VANET," *IEEE Access,* vol. 7, pp. 183532-183544, 2019.

[10] N. A. Alsulaim, R. A. Alolaqi and R. Y. Alhumaidan, "proposed solutions to detect and prevent DoS attacks on VANETs system," *In 2020 3rd international conference on computer applications & information security (ICCAIS) IEEE*, pp. 1-6, March 2020.
[11] R. Kolandaisamy, R. M. Noor, I. Kolandaisamy, I. Ahmedy, M. L. M. Kiah, M. E. M. Tamil and T. Nandy, "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.
[12] S. Kumar and K. S. Mann, "Prevention of dos attacks by detection of multiple malicious nodes in VANETs," In 2019 International Conference on Automation, *Computational and Technology Management (ICACTM) IEEE*, pp. 89-94, April 2019.
[13] H. Bangui, M. Ge and B. Buhnova, "A hybrid machine learning model for intrusion detection in VANET," *Computing*, vol. 104, no. 3, pp. 503-531, 2022.
[14] K. Adhikary, S. Bhushan, S. Kumar and K. Dutta, "Hybrid algorithm to detect DDoS attacks in VANETs," *Wireless Personal Communications*, vol. 114, no. 4, pp. 3613-3634, 2020.
[15] S. Ercan, M. Ayaida and N. Messai, "Misbehavior detection for position falsification attacks in VANETs using machine learning," *IEEE Access*, vol. 10, pp. 1893-1904, 2021.
[16] S. Ahmed, M. U. Rehman, A. Ishtiaq, S. Khan and A. Ali, S. Begum, "VANSec: Attack-resistant VANET security algorithm in terms of trust computation error and normalized routing overhead," *Journal of Sensors*, 2018.
[17] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE transactions on intelligent transportation systems*, vol. 17, no. 4, pp. 960-969, 2015.
[18] W. Othman, M. Fuyou, K. Xue and A. Hawbani, "Physically secure lightweight and privacy-preserving message authentication protocol for VANET in smart city," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 12, pp. 12902-12917, 2021.
[19] B. A. Bensaber, C. G. P. Diaz and Y. Lahrouni, "Design and modeling an Adaptive Neuro-Fuzzy Inference System (ANFIS) for the prediction of a security index in VANET," *Journal of Computational Science*, vol. 47, pp. 101234, 2020.
[20] N. C. Velayudhan, A. Anitha and M. Madanan, "Sybil attack with RSU detection and location privacy in urban VANETs: An efficient EPORP technique," *Wireless Personal Communications*, vol. 122, no. 4, pp. 3573-3601, 2022.
[21] S. Aldhaheri, D. Alghazzawi, L. Cheng, B. Alzahrani and A. Al-Barakati, "Deepdca: novel network-based detection of iot attacks using artificial immune system," *Applied Sciences*, vol. 10, no. 6, pp. 1909, 2020.
[22] R. Kolandaisamy, R. M. Noor, M. R. Z'aba, I. Ahmedy and I. Kolandaisamy, "Adapted stream region for packet marking based on DDoS attack detection in vehicular ad hoc networks," *The Journal of Supercomputing*, vol. 76, no. 8, pp. 5948-5970, 2020)
[23] K. Adhikary, S. Bhushan, S. Kumar and K. Dutta, "Hybrid algorithm to detect DDoS attacks in VANETs," *Wireless Personal Communications*, vol. 114, no. 4, pp. 3613-3634, 2020.
[24] B. Sousa, N. Magaia, and S. Silva, "An Intelligent Intrusion Detection System for 5G-Enabled Internet of Vehicles," *Electronics*, vol. 12, no. 8, pp. 1757, 2023.
[25] A. Gaurav, B. B. Gupta, F. J. G. Peñalvo, N. Nedjah and K. Psannis, "Ddos attack detection in vehicular ad-hoc network (vanet) for 5g networks," *In Security and Privacy Preserving for IoT and 5G Networks Springer, Cham.*, pp. 263-278, 2022.

Authors' Profiles

S. Rama Mercy 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. Padmavathi Ganapathi 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, "Encrypted Access Mapping in a Distinctly Routed Optimized Immune System to Prevent DoS Attack Variants in VANET Architecture", International Journal of Computer Network and Information Security(IJCNIS), Vol.16, No.3, pp.99-114, 2024. DOI:10.5815/ijcnis.2024.03.08