International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 09 | Sep 2024 www.irjet.net p-ISSN: 2395-0072

Mitigating Gray Hole Attacks in the Internet of Vehicles Using PGHA and Network Trust Score

Niharika N[1], Akhila S[2]

[1]*Post Graduate Student, Department of ECE, BMS College of Engineering, Bengaluru, India*
[2]*Professor, Department of ECE, BMS College of Engineering, Bengaluru, India*

Abstract - *Vehicular Ad-Hoc Networks (VANETs) drive the development of the Internet of Vehicles (IoV), Intelligent Transportation Systems (ITS), and Vehicles to Everything (V2X) connectivity by providing a multitude of commercial and safety applications. Though VANETs have potential advantages, they are open, distributed, and dynamic making them vulnerable to a range of security threats, including inherent protocol design vulnerabilities. The infamous Gray- Hole Attack (GHA), which comes in two versions: Smart GHA and Sequence Number-based GHA, is one such attack. The malicious node in Sequence Number-based GHA begins acting strangely throughout the route discovery process, whereas in Smart GHA, the malicious node acts normally during this phase. In both the cases, the packets are dropped immediately after the route is successfully established. In this paper, a novel security approach called ''Prevention of GHA'' (PGHA) is proposed to detect and prevent both variants of GHA in Ad Hoc On-Demand Distance Vector (AODV) based VANETs. The approach is based on the generation of dynamic threshold values that identify abnormal differences in received, forwarded, and generated control or data packets among nodes and their sequence numbers. The proposed PGHA is implemented and tested in MATLAB and its performance is compared with the most relevant benchmark approaches. The results showed that the proposed PGHA performed better than the benchmark approaches in terms of increased detection accuracy of 97% on an average.*

Key Words: **—** GHA, PGHA, RREP, RREQ, RSU, MRT, DSN, NTS.

1.INTRODUCTION

Vehicular Ad Hoc Network (VANET) is a specific type of ad hoc network in which a group of moving vehicles and fixed Road Side Units (RSUs) are connected together through a wireless medium to provide a safe and secure traffic environment [1], [2], [3]. Owing to its practicality, ease of use, and adaptability, new cars with integrated onboard sensors allow them to interact with one another and make best use of the advantages offered by VANET's. These kinds of technologies work best in a variety of domains, such as fleet and traffic management, entertainment, and safety [4]. Three components make up a VANET from an architectural perspective: Trusted Authority (TA), RSUs, and OBUs (On-Board Units). Three communication modes produced by these components are infrastructure-to-infrastructure (I2I) communications, vehicle-to-vehicle (V2V), and vehicle-to-infrastructure (V2I) communications [14]. The ITS's backbone, VANET, is essential for giving real time information to drivers, passengers, and traffic administration authorities [7], [8].

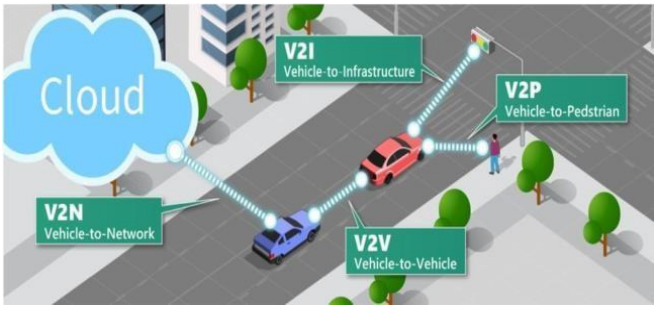

Fig 1. Vehicle to Everything

Security Problems with VANETs: Because of their unique features, VANETs face a number of security problems and challenges in spite of their remarkable applications, importance, and adaptability. VANET communications are particularly vulnerable to various security threats owing to their large-scale, rapid pace, open access medium, a highly dynamic network architecture, frequent disconnection, and protocol design flaws [2], [4], [9], [10]. Though there are several routing protocols available for establishing paths between nodes, AODV is one of the most popular choices for VANETs [12], [13].

The AODV routing protocol is a well-suited protocol for the extremely dynamic nature of VANET since it offers a quicker, more dynamic network connection with less computing and storage needs. However, it has a number of serious security flaws that increases the vulnerability to various assaults, such as Wormhole Attack, GHA, and Black-Hole Attack(BHA) [15],[16] VANET applications and services are constantly vulnerable to security risks and assaults because of their special qualities and characteristics. A GHA is one such difficult attack that jeopardizes the security messages transmitted across VANETs. Sometimes GHA behaves normally, but later starts dropping packets entirely, selectively, or partially. Second, while forwarding packets to all other nodes, it sometimes rejects packets coming from a particular node. These packets could include important alerts and information about safety. Moreover, deleting these packets can impair the security and functionality of the network as a whole, causing accidents, traffic fatalities, and congestion.

Because of this, mitigation of GHA in AODV-based VANET gains importance. Unlike other attacks, identifying a GHA is very challenging due to its contradictory behaviour. Though several authors have made efforts to solve GHA, it has resulted in a lower throughput and packet delivery ratios (PDR)

Contributions: This work aims at providing a solution for the detection and prevention of GHA with the following notable contributions:

- **Effective Detection and Prevention**: An effective method for detecting and preventing GHAs has been proposed to enhance the security and general functionality of AODV-based VANET.
- **Dynamic Thresholds:** The suggested method is based on creating dynamic thresholds of anomalous differences of received, forwarded, and created control/data packets and their sequence numbers, in contrast to the previous approaches that were based on static thresholds.
- **Dual-Purpose Approach**: The proposed method is versatile, as it is capable of recognizing and preventing both Sequence Number-based GHA and Smart GHA.

The paper is structured as follows: Section II briefly describes the background of GHA; related works are discussed; Section III, Section IV describes the proposed PGHA; a discussion on the results obtained is presented in Section V followed by the conclusion in Section VI.

1.1 GRAY- HOLE ATTACK(GHA) IN VANETs

Compared to conventional networks using wireless communication, the general security and performance of VANETs are significantly influenced by the nodes behaviour. This can be attributed to the fact that the node finds it challenging to establish whether the data it receives comes from a malicious or trustworthy source.

For instance, in the AODV protocol, a node broadcasts the Route Request (RREQ) to all of its nearby nodes in order to start the route discovery process when it wishes to speak with another node. A bidirectional path is formed and packets are transferred by the source node to the destination after it receives the first Route Reply (RREP). In an AODV-based VANET, the source is never aware of the destination, so, it is more vulnerable to various security threats, such as GHA. A malicious node can drop packets entirely in a GHA, which is a variant of BHA. GHA may function maliciously by dropping packets entirely, selectively, or partially, or it may act normally at times. GHA can be broadly divided into two types: Smart GHA and Sequence Number-based GHA. Fig. 2.

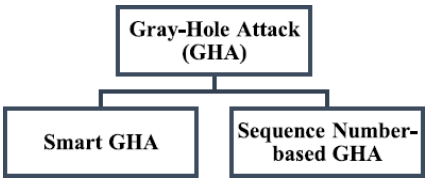

Fig 2. Types of GHA

The malicious node in the Smart GHA acts normally while it searches for a route. But as soon as the route is successfully created and the data packets start moving, it either starts honestly forwarding the packets or drops them entirely. In contrast, the malicious node uses Sequence Number-based GHA to draw packet flow toward itself by responding to RREQ with a false RREP that has a higher sequence number. In this scenario, the packets are entirely dropped by the route once it is built. A gray-hole node (either a Smart or a Sequence Number-based GHA) takes on the qualities listed below when interacting with other nodes in the AODV-based VANET.

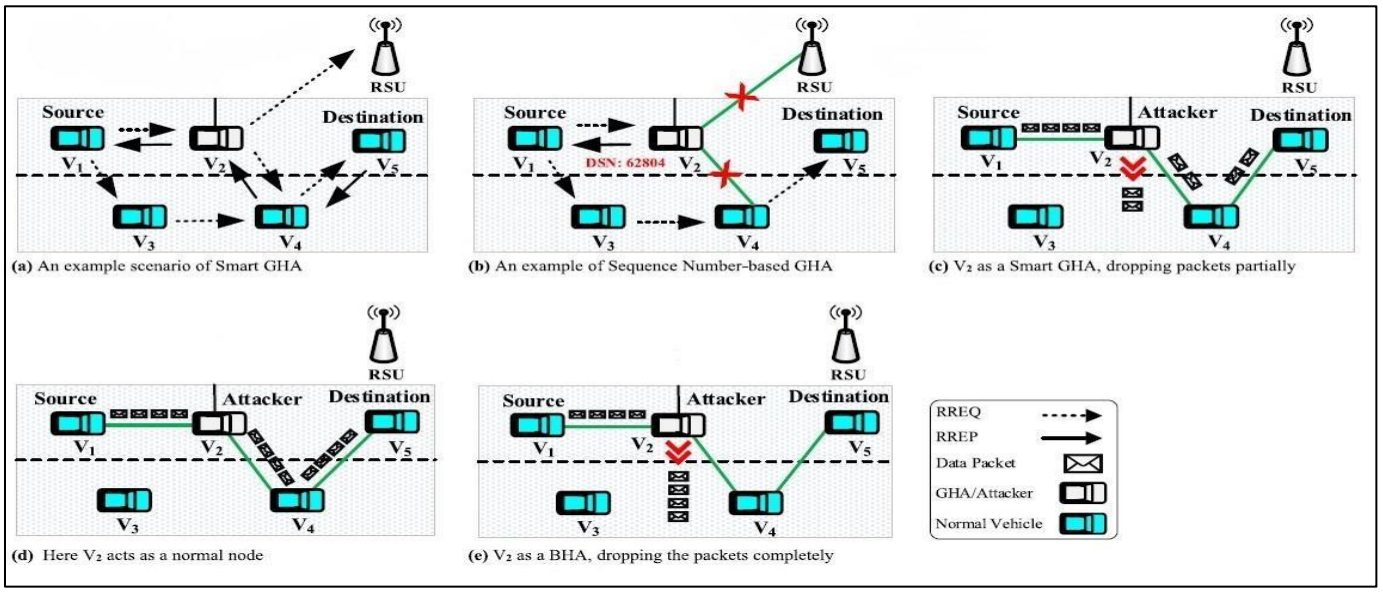

Fig 3. Different Scenarios of GHA [13]

The number of RREPs (in response to RREQs) generated by a gray-hole node is very high.

- The number of RREQs generated by a gray-hole node is very low and often equal to zero.
- The number of data packets received by a gray-hole node is very high.
- The number of data packets forwarded by a gray-hole node is lower than its received packets.
- The RREP of a gray-hole node (sequence number based) contains a larger sequence number.
- Due to presence of GHA in a VANET, the PDR of such a network is significantly decreased while the Packet Loss Ratio (PLR) increases.

Figure 3 (a-e) shows several GHA scenarios. Vehicles V1 and V5 are assumed to be the source and destination nodes, respectively, and V2 to be a gray-hole node, with the remaining vehicles being normal intermediary nodes. To construct a route toward the destination vehicle V5, source V1 broadcasts an RREQ packet to all of its nearby nodes as in Figure 3(a). This starts the routing discovery process. In this scenario, V2 takes on the role of a Smart GHA, participating as usual and exchanging control packets with nearby nodes. Subsequently, V2 functions as a Sequence Number-based GHA in Figure 3(b) by responding to V1's RREQ with a false RREP that has a higher Destination Sequence Number (DSN).

But as Figure 3(c) illustrates, after the route is set and the data packets start to move in the direction of destination V5, V2 (a Smart GHA) partially drops the packets. Comparably, V2 in Figure 3(d) exhibits typical node behavior by forwarding all packets received from source V1. Lastly, V2 (perhaps a Smart or Sequence Number-based GHA) entirely discards each and every packet received from source V1 as depicted in Figure 3(e). A visual representation of the effect of GHA in a VANET is shown in Figure 4. The gray-hole vehicle, V4, receives an accident alert message from V3, but it chooses not to relay it to the oncoming vehicles, V5 and V6. V4 purposefully skips this crucial message rather than sending it on to other vehicles, which leads to increased causes of accidents and traffic congestion.

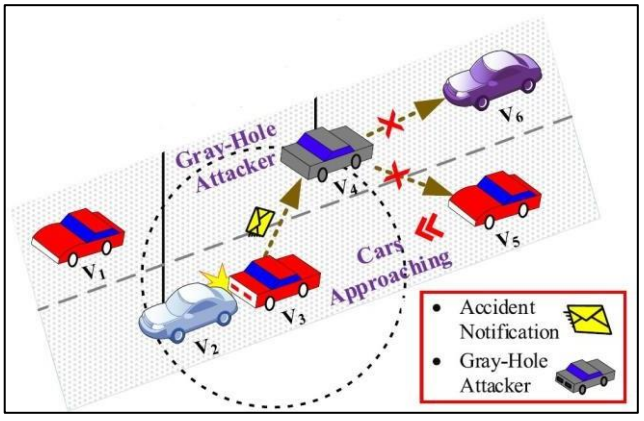

Fig 4. A Visual Representation of Impact of GHA on a VANET [13]

2. LITERATURE SURVEY

The concept of V2X communicationbegan to takeshape with the aimof enhancing road safety, traffic efficiency, and overall transportation systems. The early ideaof vehicle communication dates back to the late 20th century when researchersandtechnologistsenvisioned the possibility of vehicles communicating with each other and with roadside infrastructure. Early discussions focused on the potential benefits of such communication for improving road safety and traffic flow.

The concept gained momentum with the emergence of Vehicular Ad-Hoc Networks(VANETs)in the late 1990s and early 2000s. VANETs were conceptualized as self-organizing networks where vehicles could communicate with each other in an ad-hoc manner, forming a dynamicnetwork without the need for a fixed infrastructure. The development of the IEEE 802.11p standard, a modification of the Wi-Fi standard specifically designed for vehicular communication in the 5.9 GHz band, played a pivotal role in the formalization of V2X communication protocols. This standard addressed the unique requirements of communicationbetween fast-moving vehicles.

In [1], the authors introduced a three-phase algorithm for the detection of Black Hole Attack. Under the first phase, RSU plays the role of a certificate authority (CA) which maintains and generates a public and private key as well as certificates for the vehicles. Before the start of any communication, vehicles have to be verified from the RSU. In the second phase, the source broadcasts RREQ along with the correct certificate, nonce encryption, and destination's public key. The destination sends RREP back with the source's public key. In the third phase, Black Hole vehicles are detected based on the threshold of the destination sequence numbers, extracted from the RREPs, which are stored in the data structure used in the algorithm called Heaps.

In [2], AODV routing algorithm is considered by the authors. The Process starts with collecting the Destination Sequence Number and Hop Count Values for the incoming RREPs of the nodes in the network and then pre-calculating the thresholds from the data set collected for the two parameters.

If the Sequence Number and the Hop count is greater than the threshold then it is categorised as suspicious node and based on pre calculated the thresholds for Packet Delivery Rate, if the Sequence Number and the Hop count greater than the threshold, then categorised as BlackHole and the entire network is flooded encapsulating the Node ID of BlackHole into RREQ.

In [3], the authors consider route discovery process by AODV routing algorithm. The authors here take into consideration of both Black hole and gray hole attacks. Abnormal communicating nodes are separated into two subcategories named as a Blackhole and Gray Hole Attacker nodes using ABC (artificial bee colony) as an optimization technique with a novel fitness function. Those nodes that satisfy the ABC fitness function are considered as normal node otherwise considered as a malicious node. If [Source Node, Hop Count, Destination Node] == Neighbour Nodes [Source Node, Hop Count, Destination Node] then, Route = Neighbour Node is an Destination Node.Trained by Artificial Neural Network, the input layer comprises 50 numbers of nodes as input data, the information of which such as delay, energy consumption is being carried by 10 number of neurons as depicted under the hidden layer. At the output layer, there are 47 numbers of nodes has been attained, which demonstrates the class of communicating nodes. The network has been trained on energy consumption and the delay produced by the nodes. Later on, these parameters are used to decide that to which node the data is forwarded.

In this research, the route formation has been performed using AODV routing algorithm, which is an on-demand routing protocol along with Dynamic Source Routing. Using this protocol, the source node sends the RREQ packet to the nearby node, which contains the address of the destination node. If the adjacent node is not the destination node (not found its address) in the RREQ packet, then forward the packet to the next node, which comes in its communication range. After receiving the RREQ packet by the black hole node, the affected node instantly sends an RREP packet towards the source node with a higher hop count to attract the request known as fake routing response (FRREP). The route is established from the source to the destination node through the black hole node, and hence the entire data packets are dropped by the black hole as an intermediate node, which in return decrease the throughput of the network in [4].

A self-cooperative detection scheme to detect simple and collaborative black hole attackers is proposed in [5]. Self-detection process is used for identifying the simple black hole attackers, and the collaborative detection process is used for determining the collaborative black hole attackers in the network. Trust values of the vehicles are predicted using the previous destination vehicles through which attackers are detected. It has high overheads because of the exchange of trust information.

[6] proposed a hybrid solution based on the assumption that a malicious node always sends the first RREP. The first RREP is ignored by the source node, and the second RREP is chosen for data transmission toward the destination. In this way, the likelihood of a malicious node on the second RREP's path is decreased, resulting in a safer route for transmission. However, this technique fails in the case when a malicious node is in the vicinity of the source node and the destination is far away. Likewise, an end-to end delay will occur if the second path is selected, voiding the presence of any malicious node.

A DPMV (Detection and Prevention of Misbehaving Vehicles) approach based on caching mechanisms that

improves the Detection of Malicious Vehicles (DMV) scheme is presented in [7]. It first examines all the available routes for the presence of malicious nodes. If a route containing an attacker is discovered, the route is ignored, and a new route toward the destination is established. In comparison to DMV, this approach detects malicious nodes efficiently with high mobility. However, the approach requires more time for its processing, resulting in a high end-to-end delay [8].

In [9], the authors proposed a dynamic threshold value scheme against cooperative black hole attackers. The threshold value is determined by using linear regression. Each node's analysis of the lost packets is carried over by using the proposed technique. Using linear regression also reduces the false positive rate to a greater extent but still has high overheads.

The authors in [10], proposed a Smart Black hole and Gray hole mitigation scheme. It uses dynamic time wrapping to analyse the time difference between the dropped packets. Attackers are identified by using the analysed time difference. It can be used in AODV and OLSR protocols, but monitoring all vehicles by RSUs is mandatory to analyse the time series difference of the dropped packets

The authors in [11] proposed an updated AODV protocol for detecting Black Hole Attack. The proposed modifications are in RREP and RREQ messages. Cryptographic encoding and decoding enhance security, which authorizes the sender and receiver. It detects the black hole attackers efficiently but can't prevent them from intruding on the network. Further the authors proposed a novel approach combining Signature-based and Anomaly-based IDS. Though it achieves higher accuracy, it increases the overheads using two intrusion detection schemes.

In [12] a hybrid approach is considered using dynamic threshold value and node credibility for early detection of black hole attackers. RSUs periodically compute the dynamic threshold value and categorize the vehicles into categories 1, 2, and 3. RSUs are responsible for the monitoring module, which monitor the vehicles in their range using a watchdog approach. Through monitoring, RSUs classify the vehicles into three categories based on their forward rate, computed using a dynamic threshold value. It then sends the information to the vehicles in its range. In the detection phase, vehicles use the classification information and the node credibility value to identify the black hole attackers. The identified attackers are isolated from the network in the recovery phase.

The authors in [13] have divided the gray hole attack into Smart GHA and Sequence number-based GHA. In Smart GHA, the malicious node behaves normally during the route discovery process. However, once the route is successfully established and the data packets begin to transfer, it either starts dropping the packets partially, or fully, or forwards them honestly. In Sequence Number-based GHA, the malicious node sends a fake RREP with a higher sequence number in response to the RREQ in order to attract the flow of packets towards itself.

3. METHODOLOGY

A Vehicular Ad hoc Network is represented as a graph $G = (N, E)$, where N is a finite set of nodes (vehicles or RSUs) and E is a finite set of edges connecting these nodes. The edges provide the communication links among nodes in the VANET, shown in Figure 5. In such a dynamic network the cardinality of nodes $|N|$ remains constant over a specific time while the cardinality of links $|E|$ can be changed due to the high mobility of nodes.

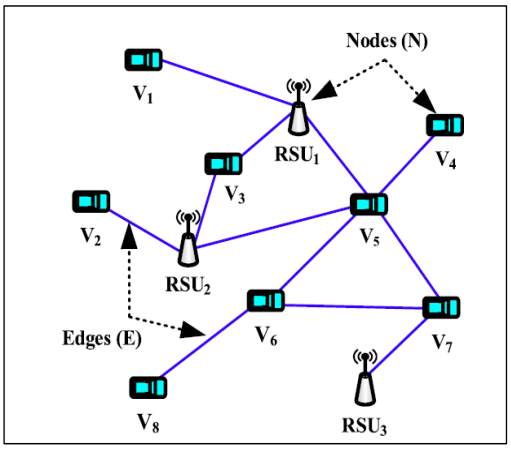

Fig 5. Graphical representation of a VANET [13]

The overall system design framework of the proposed prevention of Gray hole attack in IoV consists of 3 main phases.

1. Primary Phase
2. Detection Phase
3. Prevention Phase

3.1 PRIMARY PHASE

The first step begins with the initialization of the network with number of nodes considered as 50 and the communication range within which each node can communicate as 100 and specific time interval as 1 second for simulation updates and total duration of the simulation in time steps as 100. Lastly, initialization of the position of the nodes randomly within 500x500 grid.

For each time step, each node checks the communication between each pair of nodes within the communication range, if the communication is established, a message is sent between the nodes. The node checks for the presence of a GHA using a placeholder function is 'GrayHoleAttackDetected'. Increments the 'numAttacks' counter if an attack is detected. Updates the communication matrix to indicate successful communication between nodes.

The communication matrix over time using an image plot, shown in the below Figure 6. Once the communication is established between each pair of nodes, a message "This is a VANET message" is sent between the nodes. Further, randomly adjusts the positions of nodes to simulate mobility.

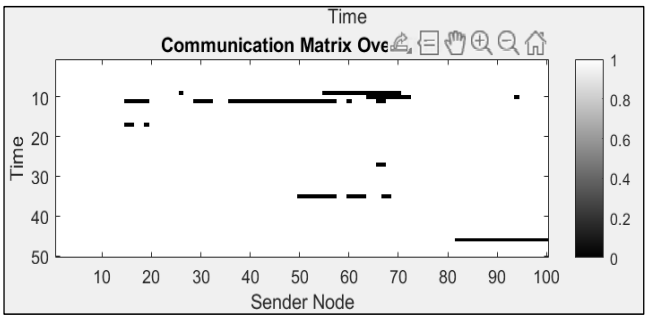

Fig 6. Communication Matrix

Next step is to check for the presence of a Gray-Hole attack using the function is 'GrayHoleAttackDetected'. If a GHA is detected, it displays a message indicating the attack, mentioning the time and the nodes involved. The simulation then continues to the next pair of nodes. A while loop is considered to simulate the transmission of packets until all packets are transmitted or discarded. Selects a packet to transmit "Msg" from the packet list and randomly selects source and destination nodes from the network. Finds all the paths from source and destination and evaluates the best path.

The visualization of the results is in terms of time and energy of the packets travelling in the network. If there is presence of attack in certain nodes, then complete packets are dropped indicating that there is no energy in packets between those nodes and no time taken for the packets to be transmitted in that region.

Twoemptyarrays, data and labels, areinitialized. These arrays will storethefeaturesextractedfromthenetwork paths (data) and the corresponding labels indicating whether the path is validor not (labels), along with the total number of RREQ, RREP, DSN is contained in the arrays. The next step is consideration of mobility of the network. 100 iterations is considered for the network to dynamically change along with the different position of the attack. In each iteration, a network is generated using the make net function with 50 nodes.

For each path found in the network, features are extracted using the path feature's function. These features characterize the properties of each path. The network nodes are simulated to move over this time interval. For each path, it is determined whether the

path is valid or not. Ifthe path contains the attack, it is marked as invalid. Otherwise, its validity is determined usingthe 'path_isvalid' function. The extracted features (Vectors) and corresponding labels indicating path validity (validation) are appended to the data and labels arrays, respectively.

A feedforward neural network (net) is initialized using the feedforward net function with 10 hidden neurons and the Levenberg-Marquardt backpropagation algorithm for training. The activation function of the neurons in the second layer of the neural network is set to 'tansig', which is the hyperbolic tangent sigmoid function. Thischoiceofactivation function is commonin neural networks for its properties like bounded output and efficient learning.

The neural network (net) is trained using the train function with the feature data (data) as input and corresponding labels (labels) as target outputs. The accuracy of the trained neural networkis calculated by comparing the rounded predictions of the network with the actual labels. The accuracy is calculated as the ratio of correct predictions to the total number of predictions, expressed as a percentage. For a particular iteration of a network, the output graph is obtained showing the best possible route from source to destination avoiding the attack regions.

3.2 DETECTION PHASE

RSU node is invoked in the promiscuous mode that periodically monitors all neighboring vehicles to determine whether numbers of packets received by a node are passed to their next-hop nodes or not. A total of 8 vehicles under the observation of a single RSU is considered. In promiscuous mode, a network device, such as an adapter on a host system, can intercept and read in its entirety each network packet that arrives. This mode applies to both a wired network interface card (NIC) and wireless NIC. In both cases, it causes the controller to pass *all* traffic it receives to the central processing unit instead of just the frames it is specifically programmed to receive.

To detect Smart GHA, an RSU counts the number of packets received, forwarded, and generated by each neighbouring node and stores them in the Master Routing Table. The RSU first calculates the Packet Loss Rate (PLR) value of all the received and forwarded data packets of each node in the MRT according to the following equations -

$$DPD(Vni) = \sum DPR - \sum DPF \quad ---[1]$$

$$PLR(Vni) = DPD / \sum DPR * 100 \quad ---[2]$$

where DPD = Data packets dropped, DPR = data packets received, DPF = data packets forwarded.
If the PLR value of a vehicle is found to be greater than the threshold (δ) i.e. *PLR* (*Vk*)> δ, then the RSU marks it as a suspicious vehicle. In this model, the value of threshold (δ) is set at 3%, because the standard AODV protocol for a normal node has a PDR of 97–98% Next, the RSU checks the amount of abnormal differentiation of the RREQ and RREP control packets of each vehicle and then compares it with the threshold value (λ). If an intermediate vehicle is not the destination itself and never forwards an RREQ packet for a given route, but instead responds with an RREP packet, its suspicious value is recorded in the MRT. To determine the rate of abnormal differences in control packets the RSU node calculates the Ratio of RREQ received and RREP generated using the equation

$$RRR(Vni) = \sum RREPG / \sum RREQR * 100 \quad ---[3]$$

If a vehicle's RRR value is found greater than or equal to the threshold value (λ) i.e., $RRR \geq \lambda th$, then the RSU marks it as a suspicious vehicle. An RSU declares a vehicle as a Smart GHA if its $RRR \geq \lambda th$ and $PLR > \delta th$, and then moves it to the blacklist.
The maximum value for λ is assumed to be 70% in this model. This is obviously an abnormal indicator of generating a large number of RREPs in response to the RREQs differentiating the harmful property of a Smart GHA from the group of normal nodes.

Next, the RSU node checks the fake RREP with a high sequence number stored in the MRT. DSN is included in every RREP packet to identify the route's freshness. Despite having a fresh route to the destination, a Sequence Number-based GHA generates a fake RREP with a higher DSN to get involved in the route and attract the flow of traffic towards itself. To identify such a malicious node, an RSU computes the mean (μ) value of all the recorded RREPs' DSN exchanged by each node in its MRT table according to the below equation

$$\mu = \sum DSNni(Vi) / n \text{ -------[4]}$$

where μ (*DSNni)* is the mean value of the DSN of all the RREPs of an *ith* vehicle recorded in the MRT. After computing the μ(*DSNni*) value, the RSU calculates a threshold value (β) according to the below equation –

$$\beta = \text{mean}(\mu(DSNni(Vi)))\text{---------[5]}$$

where β is a dynamic threshold value that frequently changes each time a new process of GHA detection is initiated and *n* is the total number of vehicles recorded in the MRT.

Now the RSU node compares each vehicle's μ^{th} value with β^{th} value. If a vehicle's μ^{th} value is found greater than or equal to the β^{th} value, then the RSU marks it as a suspicious vehicle. An RSU declares a vehicle as a Sequence Number-based GHA if its $\mu(DSNni) \geq \beta^{th}$, and either its $PLR > \delta^{th}$ or its $RRR \geq \lambda^{th}$, and then moves it to the blacklist.

Support Vector Machine (SVM) is a supervised learning algorithm used for classification. It works by finding the hyperplane that best separates the classes in the feature space. SVM for classification rely on the same thresholds (λ, β, δ) from the main algorithm to determine the labels for training data. SVM learns the decision boundary between different classes based on the features provided (e.g., PLR, RRR, DPD, DSN, and NTS). It doesn't directly use the thresholds, instead, it learns the relationship between features and labels from the training data which is obtained from vehicles, here 8 vehicles are considered.

Network Trust Score (NTS) for each vehicle is a feature that represents the overall trustworthiness of a vehicle in the network. NTS is calculated based on various factors such as the number of request and response packets received, detection packets received and forwarded, and data sequence numbers. The purpose of NTS is to provide additional information about the behavior of each vehicle in the network. It can help in distinguishing between genuine nodes and potential attackers based on their overall activity and behavior. In the context of SVM classification, NTS serves as one of the input features along with other features like PLR, RRR, DPD, and DSN. SVM learns the relationship between these features and the corresponding labels (Smart GHA, sequence-based GHA, or genuine node) during the training phase.

3.3 PREVENTION PHASE

As in the detection phase, once an RSU detects a GHA (either Smart or Sequence Number-based GHA), it broadcasts the identity of that vehicleto all its neighboring nodes (RSUs or vehicles) via an alert Message. The alert message contains the issuing identity of an RSU, the identity of the GHA, the type of GHA.When a node (RSU or vehicle) receives an alarm message from an RSU, it first examines its blacklist table for a GHA entry.

The alert message is discarded if an entry for the gray-hole node already exists; otherwise, the node's ID is added to the blacklist. Subsequently, the participation of the gray-hole node in the route discovery process is prevented by checking the blacklist table. A node ignores the RREP from another node if its identity is found in the blacklist table. During route discovery time, a vehicle drops the RREQ or RREP packet if its ID is found in the blacklist table. The MRT table keeps the records of all packets received, forwarded, and generated and the RREPs' DSNs of each one-hop node. While the blacklist table is used to keep the record of gray-hole nodes

4. RESULTS

The Figure 7 shows the sample of network topology.

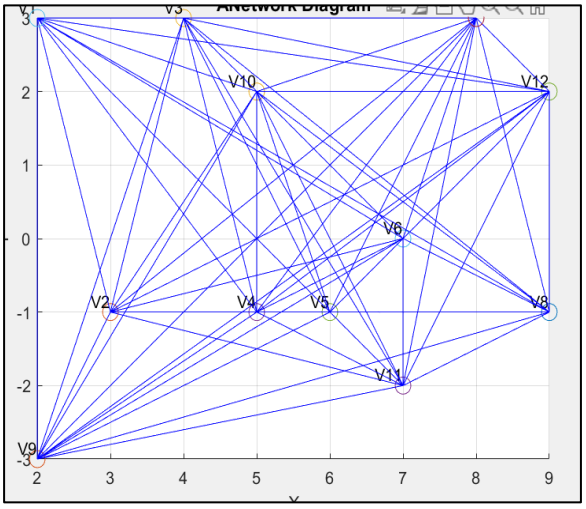

Fig 7. Network Topology

As the RSU can operate in promiscuous mode, where it listens to all the packets within its range. By analyzing the packet headers, it can identify RREQ and RREP packets, and count the number of these packets sent and received by each vehicle. Each packet has headers that include the source and destination addresses. The RSU can maintain a log of these packets to track the activity of each vehicle.

The below table, Table 1. shows the total RREQ – Route Request, RREP – Route Reply, DPR – Data Packets Received, DPF – Data Packets Forwarded and DSN – Destination Sequence of each of the Vehicles maintained in the master routing table in RSU.

Table 1. DSN, RREQ, DPR, DPF of Vehicles

Vehicle	DSN	RERQ	RREP	DPR	DPF
V1	21	40	15	550	545
V2	25	60	25	920	910
V3	23	50	46	850	810
V4	18	45	12	640	630
V5	200	80	75	1400	1370
V6	32	65	40	960	895
V7	60	41	25	1620	1590
V8	17	39	19	210	205

For classification of Smart GHA, Sequence Number Based GHA, and Normal Vehicles Support Vector Machine Model is used to train and test the model for efficient classification.

Here the labeled data for RREQ, RREP, DSN and DPR and DPD is randomly generated for the purpose of classification in the training phase and then compared with the new data from Table 1 to test for efficient classification and Figure 8, shows the efficient classification under "Label" for the new data from Table 1.

RREQ	RREP	Data_received	Data_forwarded	DSN	Label
40	15	550	545	21	normal
60	25	920	910	25	normal
50	46	850	810	23	smart_gha
45	12	640	630	18	normal
80	75	1400	1370	200	sequence_based_gha
65	40	960	895	32	normal
41	25	1620	1590	60	normal
39	19	210	205	17	normal

Fig 8. Label of Dataset using SVM

Table 2 shows the complete table of RREQ, RREP, DSN and DPR and DPD of all the 8 vehicles along with the calculation of the PLR and RRR and the conditions for categorizing the Vehicles as Smart GHA, Sequence Number Based GHA, Normal Vehicles. Here the threshold considered is δ – 5%, **λ** – 70%, NTS **–** 0.5

Table 2. Entry in MRT

Vehicle	DSN > β	PLR > δ	RRR > λ	NTS
V1	×	×	×	0.2025
V2	×	×	×	0.2444
V3	×	×	Yes	0.7650
V4	×	×	×	0.2315
V5	Yes	×	Yes	0.5505
V6	×	×	×	0.4969
V7	×	×	×	0.4242
V8	×	×	×	0.3471

Here it can be noticed that for Vehicle number 3, whose the Packet Loss Rate (PLR) < δ and RRR > λ and the NTS > NTS threshold (0.5), this vehicle will not be broadcasted as Smart GHA since the threshold **δ** is set to 5% which allows more number of packets to be lost and still is not considered as malicious node. While Vehicle number 5 has, DSN > β and RRR > **λ** the NTS > NTS threshold (0.5)**,** hence this vehicle will be broadcasted as Sequence Number based GHA.

Fig 9, shows the screenshot of the output broadcasting the vehicles number under Sequence number-based GHA for the threshold considered is **δ** – 5%, **λ** – 70%, **NTS –** 0.5

```
Broadcasting alert for Sequence Number based Gray Hole Attack vehicles:
    5
```

Fig 9. Broadcasting the vehicles number under Sequence number-based GHA

Table 3 shows the complete table of RREQ, RREP, DSN and DPR and DPD of all the 8 vehicles along with the calculation of the PLR and RRR and the conditions for categorizing the Vehicles as Smart GHA, Sequence Number Based GHA, Normal Vehicles.

Here the threshold considered is **δ** – 3%, **λ** – 70%, **NTS** – 0.5

Table 3. Entry in MRT

Vehicle	DSN > β	PLR > δ	RRR > λ	NTS
V1	×	×	×	0.2025
V2	×	×	×	0.2444
V3	×	Yes	Yes	0.7650
V4	×	×	×	0.2315
V5	Yes	×	Yes	0.5505
V6	×	×	×	0.4969
V7	×	×	×	0.4242
V8	×	×	×	0.3471

From Table 3, it can be noticed that for Vehicle number 3, whose the Packet Loss Rate (PLR) > **δ** and RRR > **λ** and the NTS > NTS threshold (0.5) hence this vehicle will be broadcasted as Smart GHA while Vehicle number 5 has, DSN > β and RRR > **λ** the NTS > NTS threshold (0.5)**,** hence this vehicle will be broadcasted as Sequence Number based GHA.

Figure 10, shows the screenshot of the output broadcasting the vehicles numbers under Smart GHA and Sequence number-based GHA.

```
PLR for vehicle 8: 2.381
RRR for vehicle 8: 48.7179
Beta for vehicle 8: 49.5
Broadcasting alert for SMART Gray Hole Attack vehicles:
     3

Broadcasting alert for Sequence Number based Gray Hole Attack vehicles:
     5
```

Fig 10. Broadcasting the vehicles numbers under Smart GHAand Sequence number-based GHA.

The below Figure 11, gives the comparative study of the Detection Accuracy vs Number of nodes for different algorithms. Here detection accuracy is the correct identification of the actual attacker/gray-hole nodes. It is calculated as the ratio of True positive to true positive plus false negative. The False Negative measures the number of attacker nodes that are identified as normal nodes.

The conventional AODV severely suffers from packet drop attacks because it has been designed without taking into account the security aspects, thus its detection accuracy is recorded as 00.0%. The Dual-Attack Detection of Black-hole and Gray-hole Security Attacks (DDBG) approach has a lower chance of detecting a malicious node, with a recorded detection accuracy of 92%. Finally, in the case of the Smart Black-hole and Gray-hole Mitigation (SBGM) approach, the average detection rate is recorded as 95%, which is approximately 3% higher than the DDBG approach. The proposed PGHA with solution has the best performance with the highest detection rate, that is, an average of 97%.

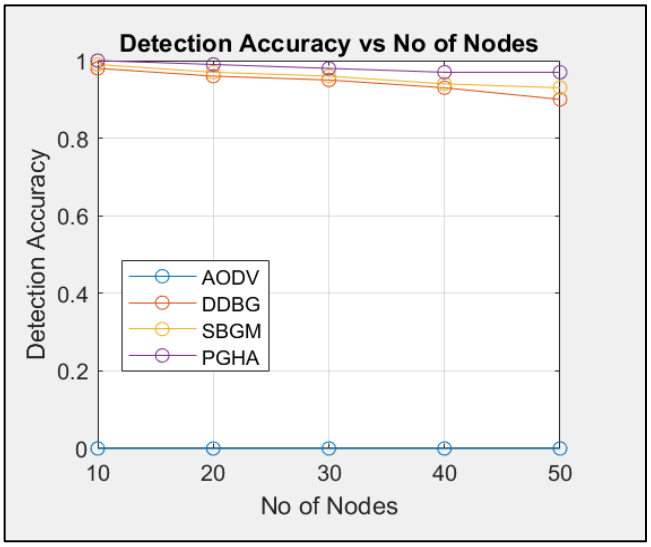

Fig 11. comparative study of the Detection Accuracy vs Number of nodes

5. CONCLUSION

A GHA in VANET is a type of security attack in which a malicious node exhibits unpredictable behavior. Initially it acts as an honest node, but later it starts misbehaving by partially, selectively, or completely dropping packets. This work presented a new and efficient approach for the detection and prevention of gray-hole attacks called PGHA to improve the overall security and performance of AODV based VANETs.

The approach relies on multiple thresholds of abnormal differences among received, forwarded, and generated control/data packets and the sequence number of RREPs. PGHA detects both types of GHA, namely Smart GHA and Sequence Number-based GHA. A comparison in terms of performance evaluation metrics of the proposed PGHA with the most relevant benchmark approach is carried out by implementing it in MATLAB tool.

The findings showed that the proposed PGHA with NTS performs better than the benchmark approaches in terms of achieving a maximum detection accuracy of 97%.

REFERENCES

[1] R. Abubakar, A. Aldegheishem, M. Faran Majeed, A. Mehmood,H. Maryam, N. A. Alrajeh, C. Maple, and M. Jawad, ``An effective mechanism to mitigate real-time DDoS attack,'' *IEEE Access*, vol. 8, pp. 126215_126227, 2020.

[2] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan and A. Aldegheishem, "Intelligent Detection of Black Hole Attacks for Secure Communication in Autonomous and Connected Vehicles," in *IEEE Access*, vol. 8, pp. 199618-199628, 2020

[3] P. Rani, Kavita, S. Verma and G. N. Nguyen, "Mitigation of Black Hole and Gray Hole Attack Using Swarm Inspired Algorithm With Artificial Neural Network," in *IEEE Access*, vol. 8, pp. 121755-121764, 2020

[4] A. Kumari, M. Singhal, and N. Yadav, ``Blackhole attack implementation and its performance evaluation using AODV routing in MANET,'' in Inventive Communication and Computational Technologies. Singapore: Springer, 2020, pp. 431 438.

[5] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan, and A. Aldegheishem, ''Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles,'' *IEEE Access*, vol. 8, pp. 199618–199628, 2020.

[6] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan, and A. Aldegheishem, ''Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles,'' *IEEE Access*, vol. 8, pp. 199618–199628, 2020.

[7] P. Rani, Kavita, S. Verma, and G. N. Nguyen, ''Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network,'' *IEEE Access*, vol. 8, pp. 121755–121764, 2020.

[8] H. Gao, C. Liu, Y. Li, and X. Yang, ''V2VR: Reliable hybrid-networkoriented V2V data transmission and routing considering RSUs and connectivity probability,'' *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3533–3546, Jun. 2021.

[9] R. Krishnan and P. A. R. Kumar, ''A dynamic threshold-based technique for cooperative blackhole attack detection in VANET,'' *Intelligent Data Communication Technologies and Internet of Things* (Lecture Notes on Data Engineering and Communications Technologies), vol. 101, D. J. Hemanth, D. Pelusi, and C. Vuppalapati, Eds. Singapore: Springer, 2022, pp. 599–611.

[10] P. R. Krishnan and P. A. R. Kumar, ''Detection and mitigation of smart blackhole and gray hole attacks in VANET using dynamic time warping,'' *Wireless Pers. Commun.*, vol. 124, no. 1, pp. 931–966, May 2022.

[11] L. Yang, A. Moubayed, and A. Shami, ''MTH-IDS: A multitiered hybrid intrusion detection system for Internet of Vehicles,'' *IEEE Internet Things J.*, vol. 9, no. 1, pp. 616–632, Jan. 2022.

[12] S. Lakshmi, E. A. M. Anita and J. Jenefa, "A Hybrid Approach Against Black Hole Attackers Using Dynamic Threshold Value and Node Credibility," in *IEEE Access*, vol. 11, pp. 91595-91603, 2023

[13] A. Malik, M. Z. Khan, S. M. Qaisar, M. Faisal and G. Mehmood, "An Efficient Approach for the Detection and Prevention of Gray-Hole Attacks in VANETs," in *IEEE Access*, vol. 11, pp. 46691-46706, 2023

[14] 5,6, Hemavathi; Akhila, S.R.; Alotaibi, Y.; Khalaf, O.I.; Alghamdi, S. Authentication and Resource Allocation Strategies during Handoff for 5G IoVs Using Deep Learning. *Energies* 2022, *15*, 2006. https://doi.org/10.3390/en15062006.

[15] Veena S, Akhila S, "Detection Of Blackhole In Under Water Acoustic Sensor Networks", International Journal For Technological Research In Engineering Volume 5, Issue 12, August-2018, ISSN (Online): 2347 – 4718.],

[16] Anitha S Sastry; Chitlapalli, Sadhana; S, Dr. Akhila, "A Novel approach for Detection and avoid Sybil attack in MANET", 16th International Conference on Remote Engineering and Virtual Instrumentation, REV 2019, Feb. 2019