Nat. Volatiles & Essent. Oils, 2021; 8(5): 1821 - 1843

NVEO
Natural Volatiles &
Essential Oils

Modeling Of An Efficient Lightweight Resistive Mechanism For Gray Hole Attack Prediction In Wireless Sensor Networks

C.Gowdham, Dr. S. Nithyanandam,
1 PhD Scholar, Department of Computer Science and Engineering, gowdhamchinnaraju@gmail.com,
Department of Computer Science and Engineering,
PRIST Deemed to be University, 613403.
2 Professor, Department of Computer Science and Engineering,
PRIST- Deemed to be University, Mail ID: snsirvp@gmail.com, 613403.

Abstract-
In Wireless Sensor Networks (WSN) security and performance are determined to be the most crucial requirement. However, network security needs to fulfill the performance, availability, and integrity of WSN. It assists in the prevention of significant service interruptions and improves productivity by maintaining and preserving network functionality appropriately. As there is no proper centralized network infrastructure, the nodes are more vulnerable and susceptible to packet drops, eavesdropping, and attacks. In a gray hole attack, neighborhood or adjacent nodes are not properly placed and trustworthy in message forwarding to successive nodes. It is extremely critical to predicting illegitimate nodes which congest and isolate host node from the network which is a complicated task. Here, the resistive mechanism towards the gray hole attack is anticipated for predicting malicious nodes over the network under certain packet drop attacks. The prevailing LEACH is integrated with the resistive mechanism to achieve reliability in attack prediction by disabling the malicious nodes with the authentication process using the Lightweight Resistive Mechanism for Gray hole attack prediction (LRM-GHA). In the anticipated LRM-GHA method, routing overhead, jitter, and packet drop rate at various pause time needs to be reduced to 8%, 0.10% respectively. Packet drop rate varies due to the mobility speed when one/two gray hole nodes.

Keywords- Wireless Sensor Network, gray hole, authentication, lightweight resistive mechanism, susceptible.

1. Introduction

Wireless Sensor Networks (WSNs) are de-centralized with no proper infrastructure in nature [1]. Also, this nature is more suited for various kinds of applications. Sometimes, the centralized nodes are not trusted in which the nodes are scaled to form a huge wireless network. With theoretical and practical analysis the overall size of these networks can be identified [2]. The faster deployment and minimal configuration of these wireless nodes are more appropriate for emergency conditions like natural disasters and military conflicts [3]. The availability of certain dynamic and adaptive routing mechanism facilitates wireless connection to be formed more quickly. These wireless connections form ad-hoc networks, mesh networks, and so on [4]. The occurrence of packet drop attacks is encountered in these kinds of networks frequently. The pictorial representation of these kinds of networks is shown in Fig 1.

Wireless networks possess various kinds of architectures that are typically considered to be the wired network, where the host cannot provide information regarding the shortest path to the destination [5]. With this, the traffic is re-directed to a host that is compromised, and sometimes the host will drop the packets [6]. Therefore, it is observed that the ad-hoc nature of the wireless connection and the hosts are vulnerable to collaborative attacks where the available hosts are

compromised and mislead the host over the network [7]. The prevailing protocols intend to provide resistance to gray hole attacks by discomforting nodes being overloaded. This provides routing reliability with appropriate factor by immobilizing connectivity as defective and acquires newer proficient route towards destination [8]. To handle the gray hole attack based packet dropping, an appropriate factor is selected by evaluating the weighted links. If sums of weights of certain selected routes are higher, that is, it specifies lower reliability, and attacking nodes are predicted [9].

The connected nodes preserve their weight where attained weight is accumulated to the requested routing payload. By evaluating the reliability of nodes' rate, the malicious nodes are differentiated from the normal nodes [10]. The performance of the prevailing protocols can be enhanced when compared to prevailing approaches and considering the factors like routing overhead, jitter, and packet drop ratio [11]. Similarly, node detection is also considered as another factor which depicts that failure over the nodes shows some impact on the routing packets. Therefore, these nodes have to be isolated and predicted to eradicate network segmentation which influences the network survival rate [12]. The nodes that are failed can be typically predicted with routing protocols. Then, node isolation is explained based on the scenarios explained below. The consequences of the selfish and failed nodes need to be evaluated. Assume, a node as a failed node and other node initiates route discovery to the destination node [13]. The unsuccessful node does not forward any packets attained from downstream nodes. The neighborhood nodes are failed, and then the successive nodes cannot able to communicate with the other nodes [14]. Therefore, the nodes are considered to be isolated by corresponding neighbors. The selfish nodes are shown in Fig 2. When the successive node initiates the route discovery process to neighborhood nodes, the selfish nodes are unwilling to forward a request from the source. In some cases, nodes behave like failed nodes. The nodes discard packets and forward the control packets that need to be forwarded. Therefore, communications among these nodes are not fulfilled [15]. When the neighborhood nodes are determined to be selfish, it cannot be competent of transmitting with successive nodes are forwarded from a one-hop distance. Even though selfish nodes can initiate broadcast with other nodes, it is characterized by corresponding failed nodes.

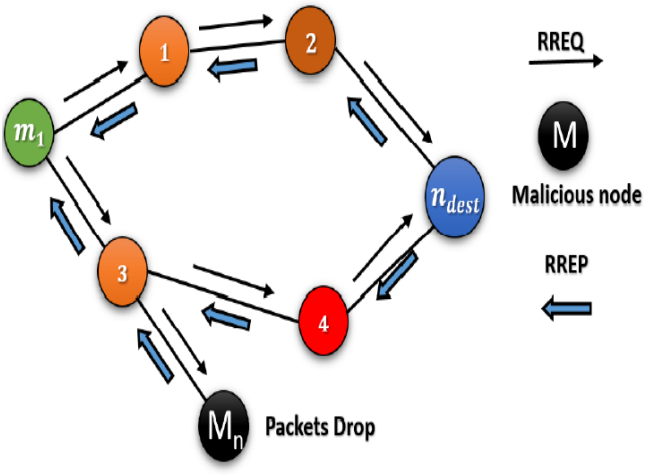

Fig 1: Injected gray hole

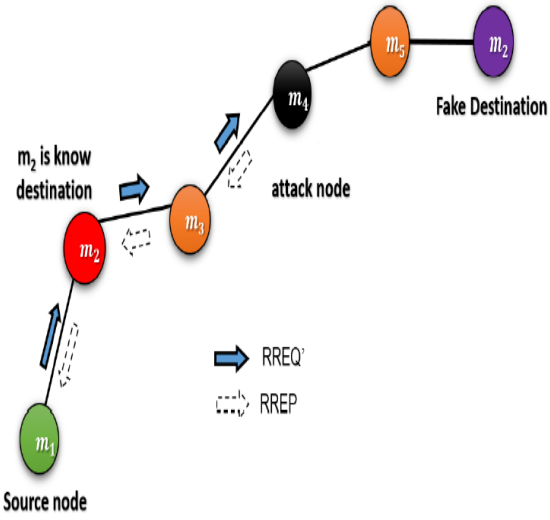

Fig 2: gray hole attack prediction

The prevailing protocols are not modeled to provide resistivity among the gray hole attacks by eliminating the nodes being overloaded. It can attain reliability during the routing process with some reliable factors by misleading links or by attaining some newer effectual route towards the destination. This research work concentrates on providing some contribution to the Wireless Sensor Networks and security-based factors. Some extensive reviews among diverse protocols are performed to handle the gray hole attacks in WSN. Here, a Lightweight Resistive Mechanism for the Gray hole attack prediction (LRM-GHA) model is anticipated for predicting malicious nodes over a network under a gray hole attack. The

the anticipated protocol is merged with various prevailing models for WSN like DSR and AODV respectively. The significant contributions of the work are:

1) To model an efficient prediction model for gray hole attack using Lightweight Resistive Mechanism for Gray hole attack prediction (LRM-GHA) model.

2) To establish authentication among nodes to provide routing from source to destination.

3) To achieve network security measures like performance, availability, and integrity using Lightweight Resistive Mechanism for Gray hole attack prediction (LRM-GHA).

The remainder sections are provided as: section 2 is related works; section 3 depicts the anticipated Lightweight Resistive Mechanism for Gray hole attack prediction (LRM-GHA) model to provide better prediction over the attack. Section 4 is numerical results and discussions; section 5 is a summary with future research direction.

2. Related works

There are various challenges in WSN based on security concerning gray hole attack. There are some dark environments where the nodes fail to deal with the attacks. Some data are generated from the malicious nodes that are unacceptable in some environment. After establishing the connection, the packets can perform any activities like packet dropping, congestion, and so on. The attacks can occur either in the interior or exterior over the network connection. Based on [16], the attacks provide some functionality over the connected nodes that degrade the system performance.

Prasad et al., [17] anticipated a work based routing model that evaluates the connectivity among the nodes and the dependency over the nodes. Salman et al., [18] examine the dynamic routing information generated from the routing table which is preserved over the nodes to analyze the previous information regarding the message received. Moreover, the corresponding information is attained from the neighborhood nodes. Various investigators have used this form of routing information and allocate the nodes for further processing over the boundaries in each node. For example, the solidness, ranking model, and trust evaluation of available nodes are determined based on their ability. Khalaf et al., [19] anticipated a model for extensive analysis of the attacks on the trust-based prediction model. The acknowledgment process is performed with two-ACK which integrates various prevailing approaches for achieving the ACK scheme.

Zhang et al., [20] anticipated the prevailing approach termed Resource Efficient Accountability (REACT) which uses some specialists for distinguishing various nodes and reduces the communication among the nodes. The author further analyses an approach termed as Best effort fault-tolerant routing which provides superior efficiency towards the nodes cluster when the node is placed in the far-away region. Similarly, the author concentrates on the cooperative bait detection approach which is reactive and proactive and integrated for further collaboration among the neighborhood nodes. The watchdog timer process is suggested by Zhang et al., [21] based on the guarding time and corresponding schemes. The prevailing approaches are used for offering a better plan among the nodes to reduce the interruption which causes system degradation. Le et al., [22] recommends the open and proactive mode with stochastic neighborhood nodes. Similarly, the Cluster Head Gateway Switch Routing model that recommends a threat model based on the missing ratio.

Paul et al., [23] anticipated CBDS based model integrate delicate and productive protection approaches. Nayyar et al., [24] recommend a refreshed kind of CBDS scheme termed ECBDS. Le et al., [25] proved an enhanced CBDS model that concentrates on packet delivery ratio that initiates from source to destination to fulfill throughput. As an outcome, the anticipated model shows some deficiencies regarding the connected nodes and better throughput. Kumar et al., [26] anticipated the soft-security method as a complete distribution among the trust-based key management approaches for WSN. However, there is some hard security among the approaches to reduce security vulnerabilities. This work targets at enhancing performance by providing security requirements and concentrates on perceived trust. Similarly, composite trust management was anticipated to reduce performance by vulnerability mitigation. The trusted threshold was set among the nodes to determine whether the trust is established among the nodes.

Alsaedi et al., [27] anticipated a security model termed as Resilience evaluation model for routing protocol dependent on various malicious faults insertion and quantitatively examined the consequences of the routing protocols. The preliminary target of the anticipated model is to i) reducing uncertainty in sources during protocol deployment; ii) device fault-tolerance method that handles various sub-problems; and iii) select/evaluate routing protocol that optimizes robustness and network performance. The methodological factors are based on fault injection in routing protocols which is extensively examined.

Keerthika et al., [28] anticipated a distributed and robust access control method based on trust-based for network protection and stimulates better cooperation among the misbehaving nodes isolation. The responsibility of access control is observed based on two diverse contexts termed as global and local. With local context responsibility, neighborhood nodes pretend to notify the suspicious nature of the global context. Similarly, global context analysis information accumulated from the nodes where the decision should be penalized the malicious nodes with voting strategy. It is proven experimentally that the integration of trust strategy and voting strategy is provided based on accurate, precise, node exclusion, and classification method during constrained monitoring.

Sherubha et al., [29] demonstrate ad-hoc nature that functions effectively if and only if when the works are performed efficiently and trustworthy. A dynamic trust prediction approach is offered for

computing nodes trust-based on the node's historical and further characteristics utilizing fuzzy logic. However, the anticipated trust-prediction approach is merged with the route method. This approach termed as trust-based source routing protocol provides a feasible and flexible model for selecting the shortest path to fulfill the security requirement for transmitting packets. The anticipated model enhances PDR by diminishing the average E2E delay by performing experimentation for the prediction of malicious nodes and providing nodes resistivity.

Sherubha et al., [30] concentrated on the Anti-black hole method that evaluates the suspicious values of the provided node based on the abnormal differences among the RREPs and RREQs which are broadcasted from the nodes. Similarly, intrusion detection systems are utilized to predict and eliminate the selection of black hole attacks [31]. When the intermediate nodes are not directed towards the destination and it will never broadcast the RREQ for a certain route; however it forwards the RREP for the successive routes. Simultaneously, the suspicious values are incremented by 1 to the neighborhood ID's nodes suspicious table [32]. When the values of the suspicious value exceed the threshold value, the blocking messages are transmitted by the IDS node to connected nodes over the network for establishing isolation among the vulnerable node communally [33]. With the ABM process, the nodes are deployed over sniff nodes to evaluate the suspicious value based on abnormal characteristics during the broadcasting process [34]. When estimated values are determined to be exceeded, then the IDS node that is placed nearer is intended to broadcast the block message turns transmits the notification information to the nodes where these nodes have to perform isolation process cooperatively [35]. During the route discovery process, the gray hole attack participates aggressively by RREQ packets forwarding for route identification to destination. When the routes are established over a gray hole node, the packets should broadcast the packets selectively [36]. Therefore, gray hole nodes are identified more effectively.

3. Methodology

This research work targets to secure the network against the Gray hole attack. The detection or resistivity process is carried out using Lightweight Resistive Mechanism. Generally, the network nodes are connected to a certain width and length modeled for deploying an 'N' number of nodes over the system model. Here, $N = 50\ or\ 100$. The network model is set over a heterogeneous environment where nodes' communication range is determined dependent on various metrics such as nodes co-ordinates, packet delay, and energy consumption. After deployment of nodes', source and destination are depicted. Then, with the AODV routing model, a data transmission procedure is carried out. With AODV, the route is identified only during the data wants to be broadcasted. The process is done with two processes. They are Route Request (RREQ) and Route Reply (RREP). The source node needs to transmit data to the destination, the data packets comprise of RREQ message is transmitted with the coverage region of the source. After receiving the message packets from the neighborhood nodes, it maintains the node over the routing table and checks the data from the datastore from the previous table. When the data is unmatched, then forward the data to nearby nodes. The data packets reach the destination with multiple paths. Using the AODV protocol, the appropriate routes are considered with distance measurements. After receiving data packets, the destination node transmits the route request packet to the destination node via the shortest path. The route discovery process is shown in Fig 3. The connectivity nodes represent the route request

generated from the neighborhood nodes. The destination nodes have to be chosen. Here, the AODV routing mechanism is considered.

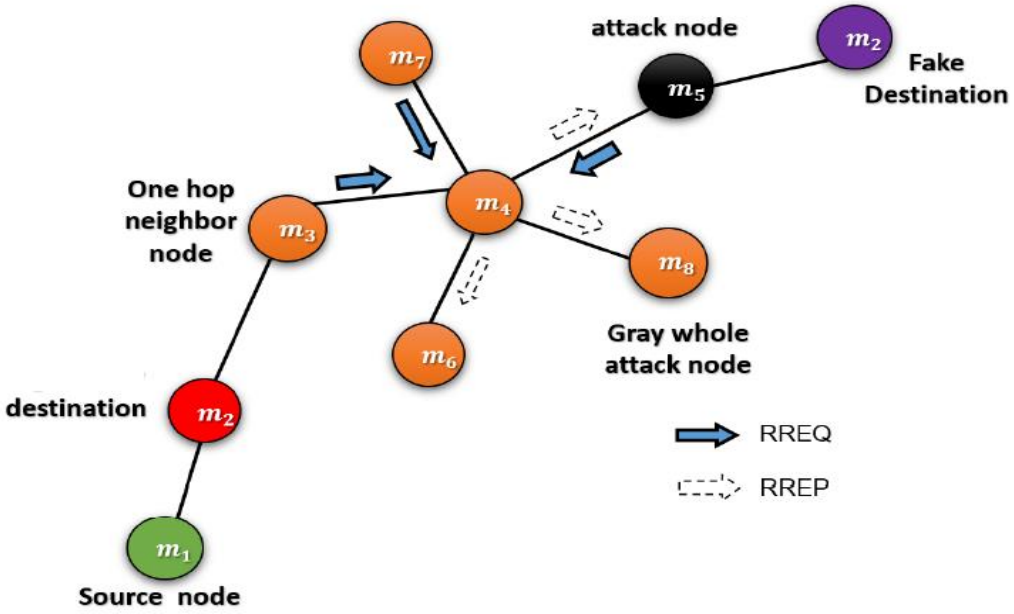

Fig 3: Gray hole attack environment

After route discovery, the gray hole attack is deployed over the network. The attacker nodes are predicted dependent on data property that transfers over the network. When the malicious gray hole node operates as a source node, then it is not an appropriate node. When the node functions as a relay node/intermediate node over the established route and partially data drops, then it is a gray hole attack. Based on the node's property, nodes are distinguished based on communicating and abnormal nodes. Then, abnormal nodes are termed as gray hole nodes. Here, resistivity's against these nodes is given using the Lightweight algorithm with reduced computational complexity.

a. Energy model

The topology is designed in a cluster model. Generally, Cluster Heads (CH) are not destroyed by malicious attacks like gray hole attack and are not restricted by the resource constraints. The members are always over the coverage region. The energy consumption of nodes is recorded based on the residual energy at various points. It is expressed as:

$$E_{i,t} = \{(t, e_{i,t}), (t + \tau, e_{i,t+\tau}), \dots, (t + l\tau, e_{i,t+l\tau})\} \quad (1)$$

Where $'i'$ is node number, $'t'$ is an initial time of node residual energy monitoring, τ is interval time, $l\tau$ is working cycle, $e_{i,t+l\tau}$ is node residual energy with $t + l\tau$. It reduces the sequential time and expressed as:

$$P_{i,t} = (p_\tau, p_{2\tau}, \dots, p_{l\tau}) \qquad (2)$$

The reference power consumption is expressed as:

$$\overline{P_t} = (\overline{p_\tau}, \overline{p_{2\tau}}, \dots, \overline{p_{l\tau}} \qquad (3)$$

Based on the Pearson correlation coefficient, the value is assigned as [-1, 1]. The values occur nearer to 1. The linear correlations among the sequences are provided in a strong manner which shows the energy consumption in a periodic manner. The correlations among the nodes are weaker to make the probability of abnormal nodes occurrence. The covariance is expressed as:

$$\rho_{p_{i,t},\overline{p_t}} = \frac{cov\ (P_{i,t}, \overline{P_t})}{\sigma\ (P_{i,t})\sigma(\overline{P_t})} \qquad (4)$$

Here, energy consumption based on prediction value relies on the working period of nodes.

b. Trust establishment

The node's information is maintained in a matrix format. If there is any change, it is observed that a gray hole has attacked the network connectivity. It is expressed as:

$$Cluster\ member = \begin{bmatrix} ID_1 & X_1 & Y_1 & e_{1,residual} \\ ID_2 & X_2 & Y_2 & e_{2,residual} \\ ID_n & X_n & Y_n & e_{n,residual} \end{bmatrix} \qquad (5)$$

Here, $e_{i,residual}$ is updated residual energy of nodes, $'n'$ is several sensor nodes. CH verifies the message senders' position and ID when the message packet receives at the CH node. When the node is strong-minded as the cluster member, the energy consumption verification is triggered; else the message is deleted from CH. The abnormality over the residual energy is expressed as:

$$e_{i,residual} - e_{i,t+l\tau} = \begin{cases} \epsilon\ (\Delta e_{i,t} - \varphi, \Delta e_{i,t} + \varphi) & else \\ \epsilon\ (\Delta e_{i,t} - \varphi, \Delta e_{i,t} + \varphi) & add\ N \end{cases} \qquad (6)$$

Here, $e_{i,residual}$ is residual energy in last working cycle, $e_{i,t+l\tau}$ is residual energy preserved over the working cycle. It specifies the energy consumption where the numerical values lie in φ. When the value exceeds the range, the energy consumption is considered to be an abnormal condition. Therefore, routing through those nodes are considered to be unsafe. Thus, the total number of iterations is also higher. The values are updated periodically to validate power consumption. CH transforms the sequence of energy consumption provided by the nodes where the correlation is expressed as:

$$\rho_{p_{i,t},\overline{P_M}} = \begin{cases} \in (\rho, +1) & source\ included \\ \in [-1, \rho) & destination\ included \end{cases} \quad (7)$$

A strong correlation is established among the CH and other connected nodes. Then, the trust value is computed to maintain the historical node situation by establishing interaction among the matrix based on the updated window value. The window size is provided as to Δ where the time avoids interactive records and adds interactive records. CH receives the data from sensors based on aggregated information, cluster, and transfers it to BS along with position, ID, and CH establishment process.

c. Effect of the gray hole over network connectivity

Assume, when there are two or more malicious gray hole nodes that do not possess the characteristics of selfish nodes. However, it randomly drops drop packets and does not harm any node by injecting data traffic. However, the nodes not able to communicate with other nodes and establishes traffic. Therefore, nodes are isolated from the corresponding malicious neighborhood. The compromised nodes attain control over unfair nodes with attempts to establish malicious activities. The nodes are independent and cannot avoid malicious activities to perform communication. As the compromised nodes vary their location very often and nodes can add or leave from the network irrespective of place and time. Therefore, it is extremely complex to monitor malicious activities. With this analysis, the misbehaving nodes (gray hole) perform isolation process with complex tasks. It also performs node connectivity. Based on the node isolation process, it is noted that when the node does possess a gray hole and nodes have to be isolated over the network. It is essential to depict the path of the node. When the path among the nodes is not less than two different ways, then the path among source and destination is termed as out-going paths. This path is accessible to facilitate a node for transmitting with nodes beyond range. When the path includes a selfish node, it can isolate neighborhood nodes. Fig 4 depicts the flow diagram of the proposed LRM model.

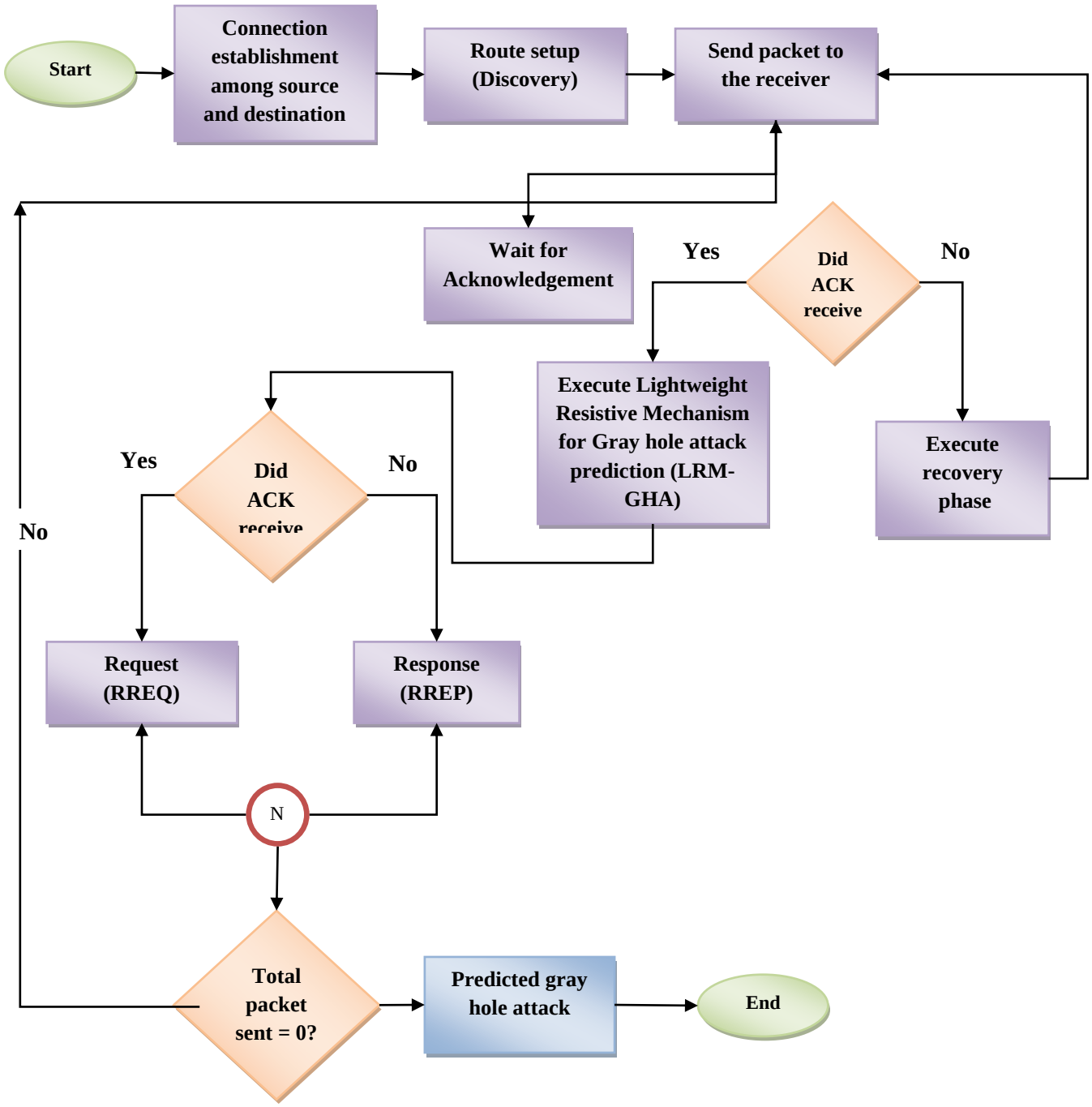

Fig 4: Flow diagram of Lightweight Resistive Mechanism for Gray hole attack prediction model

The degree of the outgoing path needs to be determined as that of the maximal amount of outgoing path from the source. The state of the outgoing path and the connected nodes are determined. The nodes communicate with other nodes through successive links. Therefore, the connectivity of the nodes have to be determined, When the cooperative nodes' degree is a gray hole,

then cooperative nodes are represented. In the gray hole attack, the malicious node repudiates the message forwarding strategy that passes through them. Then the attack is dropped potentially based on host throughput to a minimal level. CBR and AODV protocol is proposed to strengthen the

resistivity against the gray hole attacks by node thwarting from being overloaded. It maintains reliability and routing by disabled links in a defective manner. It attempts to acquire newer effectual routing towards the destination. The protocol model offers efficient security towards a gray hole attack. The nodes potentially drop host throughput to a minimal level, and the nodes are predicted based on a lightweight algorithm. Fig 5 and Fig 6 shows the file format when the gray hole node is identified.

Type	**Source**	**Destination**	**Reserved**	**Hop count**
RREQ ID				
Destination address (IP)				
Destination sequence number				
Source IP address				
Source sequence number				

Fig 5: File format

Type	**A**	**Reserved**	**Hop count**
RREQ ID			
Destination address (IP)			
Destination sequence number			
Source IP address			
Source sequence number			

Fig 6: Modified file format

The above message format is the modified format of RREQ/RREP frames. The reserved bits are utilized for examining the total amount of packets transferred by source and destination. The authentication based on route request and replay is utilized for validating the transmission rate. The authentication process is attached to the mitigation of messages from message tampering. In the lightweight model, the authentication request with route request pretends to accumulate transmission rate. The gray hole can be identified by validating the difference among the nodes with threshold values and hop neighborhood.

Algorithm 1: Route establishment

Input: number of sensor nodes, source node, destination node,

Output: route establishment

//Initiate routing

1. Connected nodes transmits the request message towards the neighborhood nodes
2. Generate request with source nodes, destination node, and hop count information
3. Initially routing counter is empty
4. Initiate routing from source
5. While the destination is not found

6. Send a request to the neighborhood node and maintain the hop count details.
8. neighbor receives request //requirement verification
9. If (source, destination, hop count) = neighborhood nodes
10. Route = source to intermediate nodes to destination
11. neighborhood nodes transfer the response to the source
12. Hop count is set as '1'
13. else
14. route = neighborhood
15. Transfer response to the source
16. Hop count is incremented to 1
17. end if
18. update and repeat the previous step until destination not found
19. Route $R = R_1, R_2, R_3, \dots, R_N$
20. for coverage range 'R'
21. discovered route = R_1
22. Compute distance measurements from source to destination
23. If $'D'$ is minimal then
24. Destination = route from intermediate nodes
25. else
26. verify route condition
27. end if
28. end for
29. end while
30. identify route from source to destination
31. end process

Algorithm 2: Lightweight algorithm

Input: sensor nodes (Packet drop rate, jitter, routing overhead)
Output: optimized destination
1. Initiate the process
2. For route optimization, establish a lightweight routing process
3. set initial routing parameters
4. Compute route length
5. Set variables to optimize nodes property

6. For coverage region-based route length
7. Compute properties from current nodes
8. Set threshold property
9. property = route establishment without malicious node interruption
10. end for
11. end for
12. optimize the connected nodes' property
13. end process

Algorithm 3:

Input: Number of nodes, evaluation of nodes properties (delay, packet drop rate, routing overhead)
Output: route validation, route from source to destination, discard route
1. Initiate routing
2. Set the routing properties
3. Initialize parameters that connect successive nodes
4. network structure = (nodes, cluster)
5. Connected sensor nodes = SN properties with route establishment and properties
6. Nodes characteristics = nodes structure
7. If sensor nodes are valid then
8. $Node = valid$
9. else
10. need an update with nodes property for analyzing the occurrence of gray hole nodes
11. if packet drops are maximum due to gray hole
12. Then execute lightweight properties
13. end if
14. end if
15. validate route from source to destination //to identify gray hole attacks
16. end process

4. Numerical results and discussion

The simulation has been performed to verify the isolation and detection of the anticipated Lightweight Resistive Mechanism for Gray hole attack prediction (LRM-GHA) against gray hole attack nodes. The simulation region and the coverage range are set as 1000m * 1000m with 100 normal

nodes that are randomly distributed and executes the routing protocol. Here, the gray hole nodes are randomly injected which pretends to drop the incoming packets from the random location. A couple of nodes are randomly selected for performing data communication. The transmitted data bit rate is provided as 10 kbps CBR. The nodes move with a random speed of 0 – 15 m/s. The node's pause time is set as 5sec, 10 sec, 15 sec, and 20 sec respectively as shown in Table 1.

Table 1: Parameter setup

Parameters	Value
Number of nodes	100-2000
Clusters	4
Coverage region	1000m * 1000m
Bit rate	10 kbps CBR
Pause time	5/10/15/20
Header size	25 bytes
Transmission range	200 m
Protocol	LEACH & AODV
Simulation time	3500 seconds
Energy	5-10 Joules

a. Packet drop rate

The dropping rate of packets is increased by 65% when the randomly located gray hole nodes perform their malicious functionality with a pause time as 5/10/15/20 seconds respectively. Even with the occurrence of gray hole nodes, the packet drop rate is attained as 12.7%. With the adoption of the proposed Lightweight Resistive Mechanism for Gray hole attack prediction (LRM-GHA) model, the drop rate is drastically reduced to a considerable amount even in case of misbehaving nodes over the abnormal routing condition. PDR is increased when malicious nodes are higher over the network connectivity.

b. Jitter

The value of jitter is raised to 0.60% when there are randomly placed gray hole nodes at a diverse location with a pause time of 5/10/15/20 seconds correspondingly. The total amount of delay in the anticipated model is achieved at 0.15%. With the Lightweight Resistive Mechanism for Gray hole attack prediction (LRM-GHA) model deployment, the rate of jitter is successfully diminished by 0.15% rate. Fig 7 shows node creation and cluster formation is shown in Fig 8.

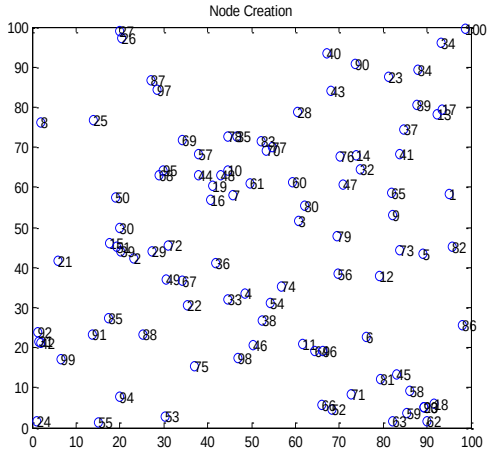

Fig 7: Node creation

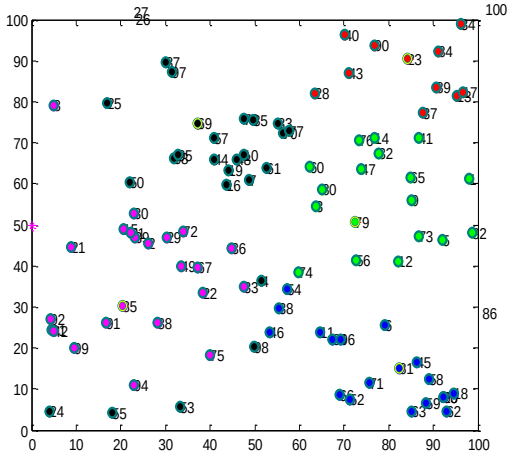

Fig 8: CH formation

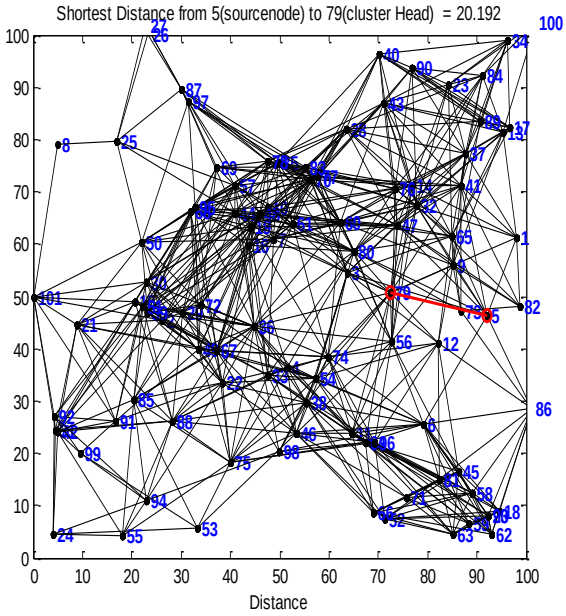

Fig 9: Shortest path prediction

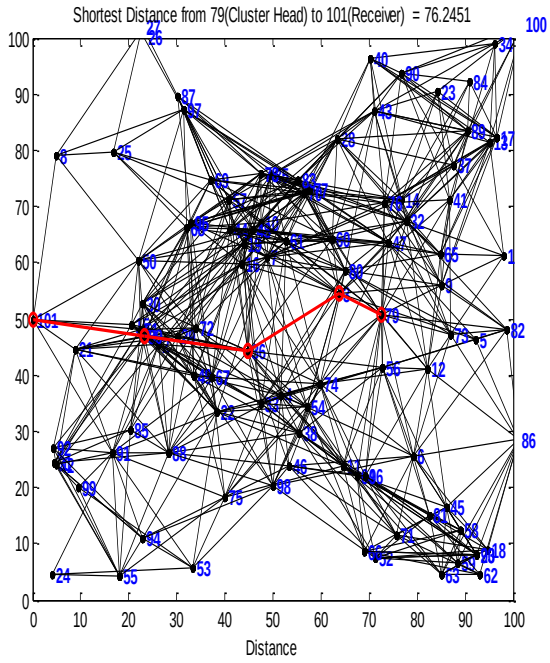

Fig 10: Route establishment

c. Routing overhead (RO)

The overhead during the routing process is raised to 78% when gray hole nodes are positioned randomly with a pause time as 5/10/15/20 seconds respectively. With the gray hole presence, the RO of prevailing approaches was 56%. With the deployment of the Lightweight Resistive Mechanism for Gray hole attack prediction (LRM-GHA), the RO was reduced successfully to 45%. When the normal, healthy nodes are distributed randomly over the coverage region, 1 or 2 malicious gray hole nodes are also available independently. Assume that, the gray hole nodes are moving randomly over the coverage region. The total PDR during the occurrence of one or two gray hole nodes is shown. The drop rates of packets are changed due to the various mobility ranges of the malicious nodes. PDR is depicted as the number of failed packets that reach the destination to the number of packets transmitted from the network source node. Fig 9 and Fig 10 shows the shortest path and route discovery process. Table 2 to Table 9 shows the comparison of various performance metrics. The performance of LRM-GHA is higher when compared to an existing model like AODV, AODV-ABC, ABM, and RSDA respectively. The packet drop rate, jitter are reduced; while throughput is higher for LRM-GHA. Some metrics are compared concerning pause time. Routing overhead for LRM-GHA is lesser in the case of one/two gray nodes. However, it ensures higher reliability of sensor nodes even in case of gray holes. Thus, the anticipated LRM-GHA gives better performance than the other models.

Table 2: Packet drop rate

Number of nodes	Under gray hole attack	AODV	AODV-ABC	LRM-GHA

100	45	59	83	94.8
200	48	61	85	95.9
400	53	65	88	97
600	56	68	89	97.2
700	59	69	91	97.8
900	61	71	93	98.25
1000	63	73	94	98.70

Table 3: Throughput (kbps)

Number of nodes	Under gray hole attack	AODV	AODV-ABC	LRM-GHA
100	58.98	68.03	80.26	85.65
200	60.26	72.95	82.60	86.99
400	62.58	75.37	85.26	88.03
600	63.88	78.76	87.95	89.65
700	65.95	79.26	88.93	90.58
900	66.33	80.26	89.26	91.90
1000	67.86	82.68	90.05	92.97

Table 4: Average delay (s)

Number of nodes	Under gray hole attack	AODV	AODV-ABC	LRM-GHA
100	0.14	0.12	0.100	0.060
200	0.20	0.14	0.13	0.061
400	0.23	0.146	0.134	0.064
600	0.27	0.160	0.143	0.067
700	0.29	0.168	0.152	0.074
900	0.30	0.175	0.160	0.17
1000	0.31	0.180	0.163	0.23

Table 5: Packet drop rate Vs. Pause time

Pause time (sec)	PDR (%)			
	AODV-gray hole	ABM	RSDA	LRM-GHA
5	70	10	10	8
10	60	15	13	10
15	60	20	13	11

20	10	25	15	12

Table 6: Jitter Vs Pause time

Pause time (sec)	Jitter (s)			
	AODV-gray hole	ABM	RSDA	LRM-GHA
5	0.02	0.12	0.1	0.01
10	0.02	0.13	0.10	0.01
15	0.04	0.15	0.12	0.03
20	0.05	0.16	0.14	0.04

Table 7: Routing overhead Vs Pause time

Pause time (sec)	RO (packet/seconds)			
	AODV-gray hole	ABM	RSDA	LRM-GHA
5	30	60	45	20
10	40	50	40	35
15	45	45	35	40
20	40	55	40	35

Table 8: Gray hole (one) Vs Pause time

Pause time (sec)	PDR (%)			
	AODV-gray hole	ABM	RSDA	LRM-GHA
5	85	8	10	90
10	80	6	12	85
15	85	8	12	90
20	85	5	11	95

Table 9: Gray hole (two) Vs Pause time

Pause time (sec)	PDR (%)			
	AODV-gray hole	ABM	RSDA	LRM-GHA
5	90	10	20	95
10	90	10	20	95
15	92	12	23	94
20	93	13	24	94

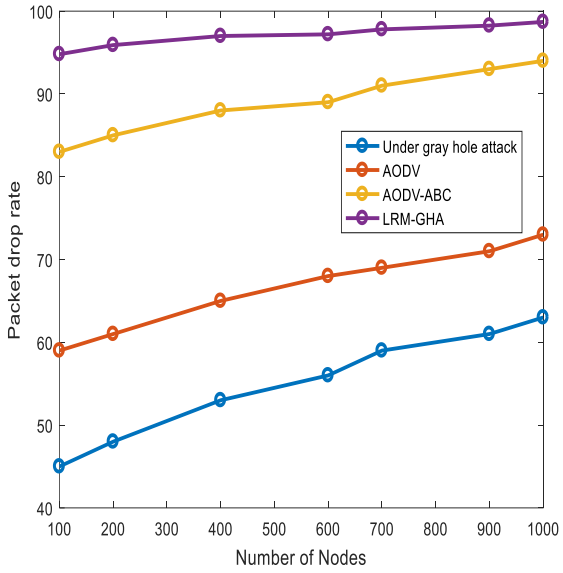

Fig 11: Comparison of PDR

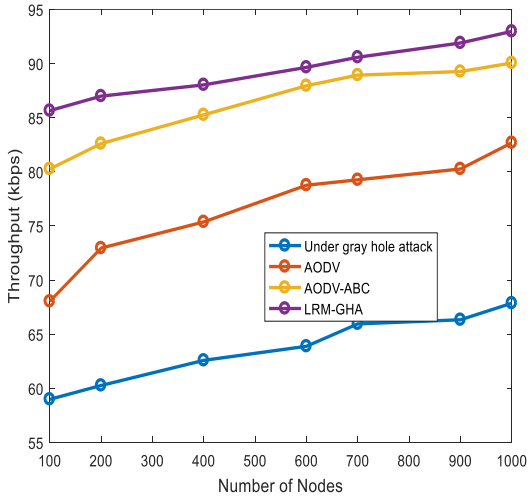

Fig 12: Throughput comparison

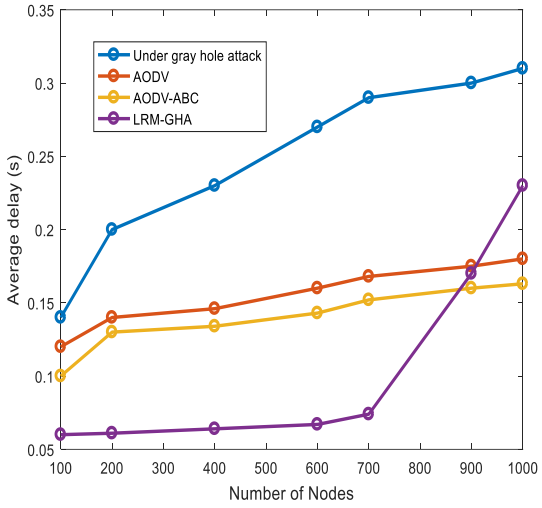

Fig 13: Average delay

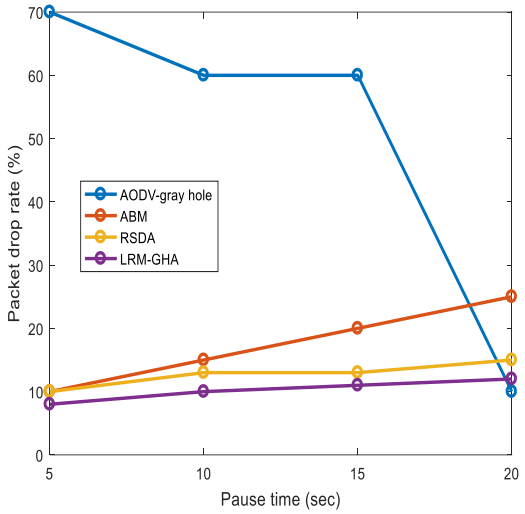

Fig 14: Packet drop rate Vs Pause time (s)

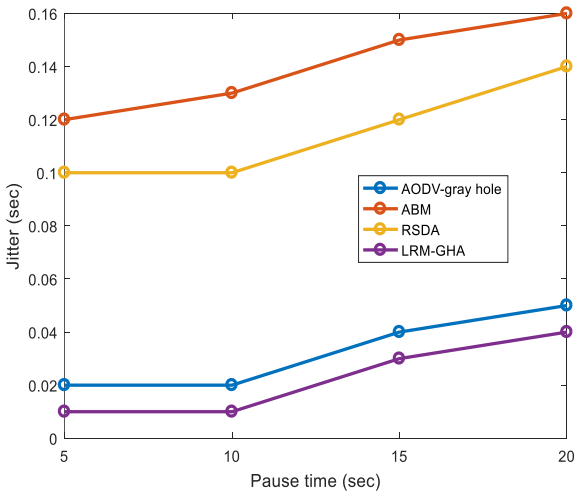

Fig 15: Jitter Vs Pause time (s)

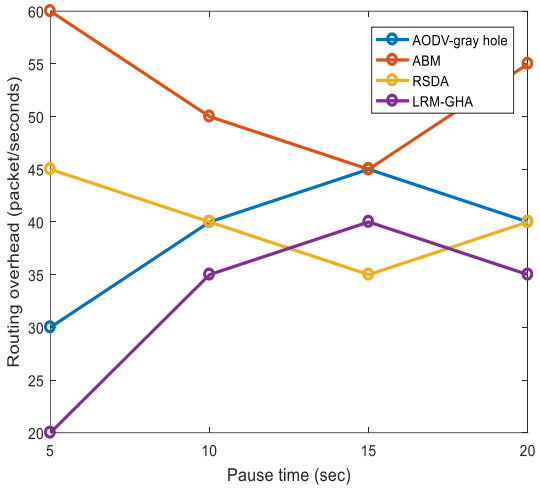

Fig 16: Routing overhead Vs Pause time (s)

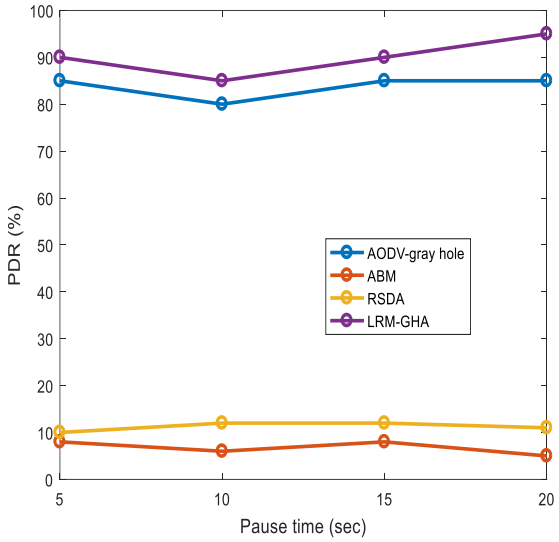

Fig 17: PDR Vs Pause time (s) with one gray hole nodes

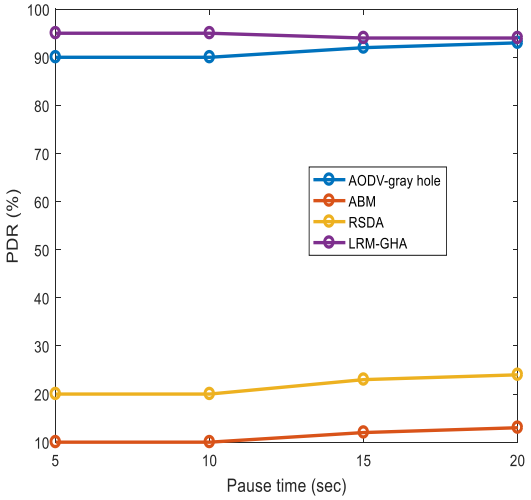

Fig 18: Packet drop rate Vs Pause time (s) with two gray hole nodes

Fig 11- Fig 18 depicts the graphical representation of various performance measures like jitter, throughput, routing protocol, pause time, and PDR respectively. The network can miss the packet because of mobility, congestion, traffic without the occurrence of gray hole nodes. In case of malicious nodes' absence, the total PDR for all mobility speeds using AODV protocol is 8.97% with all the randomly moving nodes. The PDR raises to 86% when the gray hole nodes are encountered in various regions of the network. By deploying Lightweight Resistive Mechanism for the Gray hole attack prediction (LRM-GHA) model, the PDR is drastically reduced by 12%. Similarly, during the absence of AODV mobility, the rate is 8.5% with random movement of nodes. The drop rate is increased by 95% when there are two or more gray hole nodes that are fixed randomly over various positions. The proposed Lightweight Resistive Mechanism for Gray hole attack prediction (LRM-GHA) model is deployed and successfully reduces the packet drop rate. It is observed that the PDR rate is significantly reduced when the network scalability is achieved. Also, the security level is attained with a lesser key size.

5. Conclusion

The resistivity against the gray hole attack is provided by the proposed Lightweight Resistive Mechanism for Gray hole attack prediction (LRM-GHA) model. This model provides efficient security towards the node over the network. It is essential that malicious nodes are identified which causes host overloading and isolate nodes over the network during the transmission process. During the gray hole attack, the corresponding neighborhood nodes do not forward the packets to the next connected nodes. Moreover, malicious nodes enter into the node path which denies certain message forwarding processes. The gray hole nodes have to be identified which makes the host overloading and pretends to stop the transmission process. Therefore, the nodes which perform these malicious activities sometimes make the transmission of messages unpredictable. With the gray hole attack, the nodes refuse to forward the message among other nodes. The anticipated model helps to overcome these issues and improves certain metrics like RO, jitter, and packet drop rate successively. The security of WSN over gray hole nodes are increased with the proposed idea and provides mitigation against the attack types.

REFERENCES

[1] T. Singh, J. Singh, and S. Sharma, ``Energy ef_cient secured routing protocol for MANETs,'' Wireless Netw., vol. 23, no. 4, pp. 1001_1009, May 2017.
[2] Chavan, D. S. Kurule, and P. U. Dere, ``Performance analysis of AODV and DSDV routing protocol in MANET and modi_cations in AODV against black hole attack,'' Procedia Comput. Sci., vol. 79, pp. 835_844, Jan. 2016.
[3] Ochola, L. F. Mejaele, M. M. Eloff, and J. A. van der Poll, ``MANET reactive routing protocols node mobility variation effect in analyzing the impact of black hole attack,'' SAIEE Afr. Res. J., vol. 108, no. 2, pp. 80_92, 2017.
[4] El-Seminary and H. Diab, ``BP-AODV: Blackhole protected AODV routing protocol for MANETs based on the chaotic map,'' IEEE Access, vol. 7, pp. 95185_95199, 2019
[5] Mohanapriya and I. Krishnamurthi, ``Modi_ed DSR protocol for detection and removal of selective black hole attack in MANET,'' Comput. Electr. Eng., vol. 40, no. 2, pp. 530_538, Feb. 2014.

[6] Schweitzer, A. Stulman, R. D. Margalit, and A. Shabtai, ``Contradiction based gray-hole attack minimization for ad-hoc networks,'' IEEE Trans. Mobile Comput., vol. 16, no. 8, pp. 2174_2183, Aug. 2017.
[7] Jain, V. Tokekar, and S. Shrivastava, ``Security enhancement in MANETs using fuzzy-based trust computation against black hole attacks,'' in Information and Communication Technology. Singapore: Springer, 2018, pp. 39_47.
[8] Shashwat, P. Pandey, K. V. Arya, and S. Kumar, ``A modi_ed AODV protocol for preventing black hole attack in MANETs,'' Inf. Secure. J., Global Perspective, vol. 26, no. 5, pp. 240_248, 2020
[9] Mohammadi, K. A. Memon, I. Memon, N. N. Hussaini, and H. Fazal, ``Preamble time-division multiple access _xed slot assignment protocol for secure mobile ad hoc networks,'' Int. J. Distrib. Sensor Netw., vol. 16, no. 5, pp. 1_18, May 2020.
[10] Li, J. Ma, Q. Pei, H. Song, Y. Shen, and C. Sun, ``DAPV: Diagnosing anomalies in MANETs routing with provenance and veri_cation,'' IEEE
Access, vol. 7, pp. 35302_35316, 2019
[11] Gurung and S. Chauhan, ``A survey of black-hole attack mitigation techniques in MANET: Merits, drawbacks, and suitability,'' Wireless Netw., vol. 26, no. 3, pp. 1981_2011, Apr. 2020.
[12] Gurung and S. Chauhan, ``A novel approach for mitigating gray hole attack in MANET,'' Wireless Netw., vol. 24, no. 2, pp. 565_579, Feb. 2018.
[13] Gurung and S. Chauhan, ``Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET,'' Wireless Netw., vol. 25, no. 3, pp. 975_988, Apr. 2019.
[14] Shams and A. Rizaner, ``A novel support vector machine-based intrusion detection system for mobile ad hoc networks,'' Wireless Netw., vol. 24, no. 5, pp. 1821_1829, Jul. 2018.
[15] Singh and J. K. Mandal, ``Effect of black hole attack on MANET reliability in DSR routing protocol,'' in Advanced Computing and Communication Technologies. Singapore: Springer, 2018, pp. 275_283.
[16] Xiang, X., Li, Q., Khan, S., & Khalaf, O. I (2021). Urban water resource management for sustainable environment planning using artificial intelligence techniques. Environmental Impact Assessment Review, 86, 106515
[17] Prasad, S. K., Rachna, J., Khalaf, O. I. and Le, D.-N (2020). Map matching algorithm: Real-time location tracking for smart security applications. Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika), 79(13), 1189-1203
[18] Salman, A. D., Khalaf, O. I., & Abdulsahib, G. M. (2019). An adaptive intelligent alarm system for wireless sensor networks. Indonesian Journal of Electrical Engineering and Computer Science, 15(1), 142-147.
[19] Khalaf, O. I., & Sabbar, B. M. (2019). An overview of wireless sensor networks and finding the optimal location of nodes. Periodicals of Engineering and Natural Sciences, 7(3), 1096-1101.
[20] Khalaf, O. I., Abdulsahib, G. M., & Sadik, M. (2018). A modified algorithm or improving lifetime WSN. Journal of Engineering and Applied Sciences, 13, 9277-9282.
[21] Zhang, D., Ge, H., Zhang, T., Cui, Y. Y., Liu, X., & Mao, G. (2018).New multi-hop clustering algorithm for vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems, 20(4), 1517-1530.
[22] Le, D. N., Van, V. N., & Giang, T. T. T. (2016). A New Private Security Policy Approach for DDoS Attack Defense in NGNs. In Information
Systems Design and Intelligent Applications (pp. 1-10). Springer, New Delhi.
[23] Paul, M., Sanyal, G., Samanta, D., Nguyen, G. N., & Le, D. N. (2018). admission control algorithm based on the effective bandwidth in vehicle-o-infrastructure communication. IET Communications, 12(6), 704-711.
[24] Nayyar, A., Puri, V., & Le, D. N. (2019). Comprehensive analysis of routing protocols surrounding underwater sensor networks (UWSNs). In Data Management, Analytics, and Innovation (pp. 435-450). Springer, Singapore.

[25] Le, D. N. (2017). A New Ant Algorithm for Optimal Service Selection with End-to-End QoS Constraints. Journal of Internet Technology, 18(5), 1017-1030.
[26] Kumar H, Sarma D, Kar A. Security threats in wireless sensor networks[J]. IEEE Aerospace & Electronic Systems Magazine, 2017, 23(6):39- 45.
[27] Alsaedi N, Hashim F, Sali A, et al. Detecting Sybil Attacks in Clustered Wireless Sensor Networks Based on Energy Trust System (ETS)[J]. Computer Communications, 2017.
[28] Keerthika and N. Malarvizhi, ``Mitigate black hole attack using hybrid bee optimized weighted trust with 2-opt AODV in MANET,'' Wireless Pers. Commun., vol. 106, no. 2, pp. 621_632, May 2019.
[29] P. Sherubha, "A Detailed Survey on Security attacks on wireless Networks and its countermeasures" in International Journal of Soft Computing, Pg. 221-226, Medwell Journals, 2016.
[30] P. Sherubha "An Efficient Intrusion Detection and Authentication Mechanism for Detecting Clone Attack in Wireless Sensor Networks", Jour of Adv Research in Dynamical & Control Systems, Vol. 11, No. 5, 2019.
[31] P. Sherubha "An Efficient Network Threat Detection and Classification Method using ANP-MVPS Algorithm in Wireless Sensor Networks" in International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-11, September 2019.
[32] P. Sherubha, "Design of network Threat detection and classification based on Machine learning algorithms in Wireless Sensor Networks", Caribbean Journal of Science, Volume 53, Issue 2 (May - Aug), 2019.
[33] P. Sherubha, "Crop monitoring using wireless sensor networks" in Materials today: proceedings", Elsevier, 2020,https://doi.org/10.1016/j.matpr.2020.10.373
[34] P. Sherubha, "Graph-Based Event Measurement for Analyzing Distributed Anomalies in Sensor Networks", Sådhanå (2020) 45:212, https://doi.org/10.1007/s12046-020-01451-w

[35] S. P. Sasirekha, P. Sherubha, "An Enhanced Vehicle to Cloud Communication by Prediction Based Machine Learning Approaches", International conference on computing and Information Technology, 2020, https://doi.org/10.1109/ICCIT-144147971.2020.9213784

[36] P. Sherubha, Task-Driven Approach for Deadline Based Scheduling Across Sensor Networks", International conference on computing and Information Technology, 2020, https://doi.org/10.1109/ICCIT-144147971.2020.9213782

[37] Amudhavalli, P. Sherubha "Semi-supervised Learning approach for detecting abnormalities in cloud computing, "International Virtual Conference on Smart Advanced Material Science & Engineering Applications", 2020.

[38] P. Sherubha, An Adaptive Feature Selection and Classification Techniques for Threat Identification in WSNs, "International Virtual Conference on Smart Advanced Material Science & Engineering Applications ", 2020.

[39] Napier, M. Y. I. B. Idris, R. Ramli, and I. Ahmed, "Compression header analyzer intrusion detection system (CHA - IDS) for 6LoWPAN communication protocol," IEEE Access, vol. 6, pp. 16623–16638, 2018.

[40] Linn, B. Gaonkar, T. D. Satterthwaite, J. Doshi, C. Davatzikos, and R. T. Shinohara, "Control-group feature normalization for multivariate pattern analysis of structural MRI data using the support vector machine," NeuroImage, vol. 132, pp. 157–166, 2016.