International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-3, February 2019

Gray Hole Attack Detection Prevention and Elimination using Sdpegh in Manet

Marepalli Radha, M. Nagabhushana Rao

ABSTRACT --- Mobile ad hoc network (MANET) is a wireless network which transmits the data from source to destination without any connection. Currently, this network is extensively utilized all around the world as it doesn't need any fixed wired network to establish communication concerning the source as well as the destination. The complete network can be established by utilizing a transmitter, receiver, processor and the battery. In today's scenario, the MANET is preferred in many real-time applications for example military surveillance, disaster management, air pollution monitoring, etc. MANET is an ad-hoc network which may modify positions then arrange itselfby transferring the nodes. As MANETs are moveable, it prefers wireless links to communicate numerous networks which doesn't include infrastructure or any consolidated administration. MANET areexposed to various security assaultsespecially gray hole. In gray hole attack, selective dropping of packets arises, and the packetunable to transmit further. This paper proposes Secure Detection Prevention and Elimination Gray Hole (SDPEGH) technique. In this study, DSDV is considered and the recommendedmethodis implemented in NS-2 software. The performance metrics similar to throughput, Packet Delivery Ratio (PDR), security and consumption of energy are analyzed.

Keywords:DSDV, Gray hole attack, MANET, SDPEGH, NS-2.

1. INTRODUCTION

A MANET is a cluster of movable nodes which unite and send packets to other nodes [1]. Certain networks prolong the restricted range of wireless communication of every node through multihop packet sending, and as a result, these are perfectly appropriate for scenarios in which pre-deployed substructure support doesn't exists [2]. MANETs possess certain distinctive features like untrustworthy wireless connections utilized for communication amongst hosts, continuously varying topologies of the network, restricted bandwidth, less battery power, and so on. But these features are necessary for the flexibility of MANETs, they present particular issues regarding security that are either vanished or less austere in wired networks [3].

Intrusion limitationprocessessimilar to strong validation and redundant transmission ought to be supplementedvia detection approaches to perceive the security standard of these systemsbesides recognizing the malevolent performance of any contributing nodes [4]. One such serious issues in MANETs is the safety exposures of routing protocols. Nodes can cooperate in a specific manner that it could not be probable to simply notice with malevolent performance. such nodes produce novel routing communications to promote nonexistent connections, deliver inappropriaterelates state data, in addition to flood additional nodes through routing traffic, consequently imposing a byzantine failure [5]. Here, we consider one specific attack recognized as grayhole Attack on the extensively utilized DSDV protocol.Method is offered to perceive and protect the networks beside an attack that could introduce together through a set of malevolent nodes.

Grayhole attack is considered as a one of the serious security risk that not partly drops a packet and also tradeoffs the process of communication**.** The source node accepts a reply from the authorized node that offers a direct route which is near to the sink and malicious node reply to a sender that the information is received. Source gets confused with two replies. The malicious node gets to be a sender node, and complete information is considered by it. During this procedure, the information packet completely dropped by a source [6] - [8]. The remaining section is prepared as: section 2 deliberates the existing works, section 3 defines the proposed SDPEGH method, and the implementation of a recommended solution is described in section 4, and the experimentation of implementation is offered in section 5. The outcomes in addition to performance metrics are offered in section-6, and section-7 lastly discusses the conclusion.

2. LITERATURE SURVEY

2.1 Related and similar problems

Various researchers are estimated and implemented some solutions, but the most importantbenefits were the trust-based security. Security is a bithard in MANET. A lot of researchers recommended various techniques and modified the existing protocols, and some researchers suggested new protocols. Hence, the complete network performance is damaged by different attacks. In this research, we consider a familiar packet dropper attack known as grayhole attack.

2.1.1 Related studies on Gray hole attacks:

Arya et al. (2015) concerned towardsdistinguishing and evading the wormhole and collaborative gray hole attack through routing. In the route discovery, the value of trust was also verified for all the neighbour nodes. To identify the malevolent node behavior, in this system every node contained a trust table.

Manuscript published on 28 February 2019.
***** Correspondence Author (s)
Marepalli Radha*, Research Scholar of Rayalaseema University, Department of Computer Science and Engineering, Kurnool, AndhraPradesh, India.
Dr. M. Nagabhushana Rao, Professor, Department of Computer Science and Engineering, Ramachandra College of Engineering, Eluru, Andhra Pradesh, India.

It possessed2 columns. Mainly the identifier or else neighboring node name and then its status of connection over the contiguous node that could be reliable or unreliable [9]. Advantages: more throughput, more PDR and little energy consumption. Disadvantages: Value of trust of other attacks on MANET was not determined.

Chaube et al. (2015) TSDRP and AODV for making it safe to avoid gray hole attack. TSDRP protocol was capable to send packets to the sink even in the existence of a spiteful node byraisingthe size of a particular network. By means of the purpose of making the result further precise, TSDRP and AODV performance was verifiedconcerning dissimilar metrics and observation, determined that for gray hole attack TSDRP validateenhanced performance [10].Advantages: TSDRP validateenhanced performance in almost all metrics. Disadvantages: In the regular scenario, once there is no malicious node in the network, performance is practicallyalike.

Aishwarya et al, (2017) suggested CRCMD&R for the effective and transmission of data. CRCMD&R strategy was anticipated in current research. CRCMD&R recommendedconsolidating MANET into various groups and every node contained a particular prime number that achieved as node ID. CRCMD&R utilized validitybesides level of reputation of tables handled by respective node to choose besides utilize a secure path concerning source and sink. From these metrics the CH nodes ignore or embrace the nodes from openpath and chosefaithfulway to anexactend point. Involvement work was transfer message in encoded format for data security [11]. Advantages: Raises packet route lengths, causing packets to be handledthrough a number of nodes that is independent of count of hop alongside the shortest path amongst the adversary and packet destination. Disadvantages: In this simulation, the authors send data in encrypted format for data security. The secure packet forwarding phase of clean slate routing protocol and prevent packets from Gray Hole attacks. But we have not secured discovery phase.

Gray hole Attack with multipath method was recommended in [12]. Singh et al. offered a packet update structure and even recommend the eradication scheme through determining all spiteful nodes. Complete simulation performances were establisheda gray-hole consequence offers an improved outcome and even standardize the grayhole influence network that outcomes in standardizing gray-holeeffects.Notion has presented the enhanced outcome after removal of such assaults in output. Advantages are: gray hole attack scenario offers a decent outcome and even standardize the gray hole influence. Disadvantages are: To determine the complete malicious node, repeat the complete procedure that can take additional time and resources too. It doesn't review attack contents [12].

CRCMD&R: Cluster and Reputation-based Cooperative Malicious Node Detection & Removal structure was explained in [13]. CRCMD&R scheme proposed establishing the MANET into clusters& each node in a network has a particular prime number which performs as Node Identity. Disadvantages are Connection amongst nodes that connect with one another. MANET has Vulnerable environment that makes it susceptible for different security risks. These susceptibilities allow the attacker to tradeoff the network and diminishits performance. Overall study determined that a practical operation is not a possible solution [13]. Advantages are: the CRCMD&R scheme outperforms standard AODV with greater overall throughput. Disadvantages are: However, the utilized techniques are outdated that were suggested by further investigators excluding the innovative notion of utilizing cluster method.

Network-Layer Security in MANETs was explained in [14]. The unified network-layer security solution in adhoc networks, which safeguards routing in addition to packet forwarding functions in the background of the AODV protocol. The advantages of leveraging existing IDS matching technologies. Implementation directly using Network Layer Protocol. Disadvantages are: Insecure routing protocol and do not include any mechanism to perceive and avoid communication from malevolent effect [14].

A Relative Scrutiny on Routing Protocols was suggested in [15], and also DSDV, AODV, DSR, TORA, OLSR, WRP, DSDV routing protocols was suggested in this study. These protocols are separated into 3 classes viz. proactive, reactive and a hybrid class. This organization of routing protocols was function as per their technique. Advantages are: supported the researchers to acquireanexisting classes outlineand suggested that protocols could implement well concerning varying between network scenarios. Disadvantages are: A single routing protocol couldn't achieve best in every circumstance.

SET for CWSN Using Election Procedure for verification in addition to Security Using SHA512 was proposed in [18] and the authors considered ABS and ABOOS as the core base of the system. The SHA512 Election algorithm helped to elect better cluster head, and transmission of data is achieved in good fashion. Advantages are: Decrease the time delay. It offers the optimum security. Disadvantages are: not tested the system on evaluation parameters like energy consumption and work on intra clustering and test the system for set of large nodes like set of 50 or more.

Two procedures based on False Reply Count (FRC) as well as True Link. FRC is utilized to perceivebesideseliminatinggrayholein the path establishment procedurewas recommended in [19]. The false responseswere computed on RREQand RREP. True Link is preferredforvalidating recognizedroute. Grayhole can modify honest state to malevolentlater the route established incommunication. Advantages: it is helpfulto grayhole without raising traffic. Disadvantages: True Link is enabled for path verification. As FRCmethodeffectsin route discovery, any truthful node can change in the blackhole after route formationamongst source and sink. Henceforth it is noteworthy to distinguish gray-hole in addition toauthorizeconnection.

Grayhole attack was considered in [20] as study aimed and deriveda technique to spot and halt MANETs from security risk. The completemechanismallowed forGray hole prevention in MANET on AODV protocol.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Advantages: This solution can moreoverhave evaluated on other simulator such as Quaint, OPNET to spot the influence on additional tools. Disadvantages: the development was not done for performance enhancement.

2.2 Research challenges in our problem

The security concerns of MANETs[16] are newchallenge in case of a multicasting background with a number of dispatchersin addition to receivers. There arevarious sorts of attacks in which spiteful nodes may damage a network then also create the communication to be untrustworthy. Such assaultsiscatalogued as active and passive attacks. An active attack interferesusualnetwork action throughadjusting the network packets. A passive attack occurs whenan attacker diverts the data without disturbing network performance. Specific attacks that are raising at the network layer are black hole, wormhole, gray hole, rushing, link spoofing, Sybil attack, etc.

Gray hole is a node that can differ from black hole. Therefore,it is not easy todistinguishthe attacker simply meanwhile it acts as a normal node. Grayhole has 2parts as given below:

Phase 1:Malevolent node prefersAODV protocol forcommunicatingfor a valid route to sink, to enable disturbing packets of fake path.

Phase 2: Here, the nodes send interrupted packets over an assured probability and finding the gray hole is a toughprocedure. Generally, in grayhole an attacker performs malevolently aimed at the periodtill the packets dispatchedthenformerlyvariation to consistentactions. Both regular node as well as attacker are same. Due to this performance it is toodifficult to recognize in a network for understanding certain attacks.

In gray-hole attack selective dropping of the packets arises, and the information couldn't further have communicated.

- We examine the proper solutions and advanced the appropriate solution to avoid the network from the gray hole attack.
- Black hole attack's variation is the gray hole attack that the nodes may drop the packets in a specific way. Selective forward attack is of 2categories. they are:

- Drop all UDP packets buttransfer TCP packets.
- Drop50% of dropping or packets them through a probabilistic distribution. These are assaultshunt for disturbinga network without got detected by safety measures.

2.3 Research Objectives

The main objectives of this study are as follows:

- ✓ To detect the gray hole attack using SDPEGH methodology.
- ✓ To prevent and eliminate the gray hole attack using SDPEGH.
- ✓ To enhance security, PDR and throughput and to reduce energy consumption

2.4 Problem statement

MANETs are self-configuring network that are interconnected through wireless links that creates a random topology of portable nodes. Topology of these network changes rapidly and randomly. Without infrastructure support,each node functions as a router besides any nodes couldinterconnect and leavea network. Security is a significant worry in all networks. MANETs are tremendously susceptible to security assaults as linked toward further wired systems. Offering security toward these network is difficult as these sort of networks grieves for numerous malicious attacks. One suchassault that are more complex to detect in the MANET is Grayhole. Malicious node performs as an interruption in the secure route as it will engross the information and consequently decrease delivery of a packet, reduce the performance and throughput. In our investigation, gray-hole attack is considered. To secure a network, evading this attack is very vital task.

3. PROPOSED METHODOLOGY

Gray hole attack is considered as a serious route misbehavior attack. Certain kind of attack drops some data packets this gray hole node performs similar to a legitimate node and go to contribute into full communication. The malicious gray hole attacker node participates two dissimilar phases. In route discovery, the node endorses itself having its correct routein the direction ofsink. In the subsequent stage, update the source route cache as well as routing table as the shortest route. Formerly, source node continuously considers malicious node as subsequent node and sends a packet to same. The attacker node stops all the inward packets but drop on a random manner. The whole phenomena make toughness alongside. The functionalities of a gray hole node are each received UDP packets are released partly through a random selection procedure. This type of attacker node can change character from genuine to a sinkhole. As it acts as a normal node change over to malicious node, it also improves characteristically to recognize the state whether it us original or else malicious node [17].

In grayhole, a spiteful node discards to referparticular packets besidesto dropit. The attacker perfectlysends the packets producing from one IP address or else addressessequencefurther sending the remaining packets. In MANET, grayhole nodes are more efficient. Respective node encompasses a routing table which includes info of the consecutivehop nodetosink, once a source needs to senddatatowards sink, it choosesanexact path if thatspecificroute is existing in its routing table. Also, nodes present a route discovery stage by collaborating RREQ to its adjacent nodes. On getting RREQ packet, neighbor nodes develop their routing tables for anopposite path to source. A RREP is return to source once the RREQ extents either the sink itself or any additional node holds a current path towardssink. Multipath routing is a method that uses the underlying physical network resources with multiple source destination routes. It is preferred for a number of requirements, involving bandwidth aggregation, reducing E2E delay, raising fault-tolerance, improving reliability, balancing of load, and so on.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

The notion of using multiple paths has been existent for specific time and it has been examined in different networking areas. Multipath is a propagation phenomenon that outcomes in radio signals reaching the receiving antenna by 2 or more than 2routes.In this study, 2-ray ground is utilized for attaining the multipath propagation.

3.1 Secure Detection Prevention and Elimination Gray Hole (SDPEGH) technique

In this study, the proposed SDPEGH technique detects, prevents and eliminates the gray hole malicious node that participates in route discovery. Then it provides the latest source routing table as a shortest path. Then, the source constantlyprefers the malicious node as the succeeding hop node for sending the packet to the alike nodes. Malicious node deliberates all the inward packets, then the dropping process will be on a random basis. But here SDPEGH methodology is contrary for the process of releasing all the received UDP packets and partial dropping of UDP packets through the random selection procedure. This study focusses on security in a route discovery phase during the communications. Figure 1. demonstrates the flowchart of the proposed method. The malevolent node could initially act as a trustworthy node and will modify its state to spiteful and vice versa. This particular node might release every packet or specific data packets. Grayhole attack is very complex to identify blockage, overload and also malevolent environment besides capability of varying conditions.

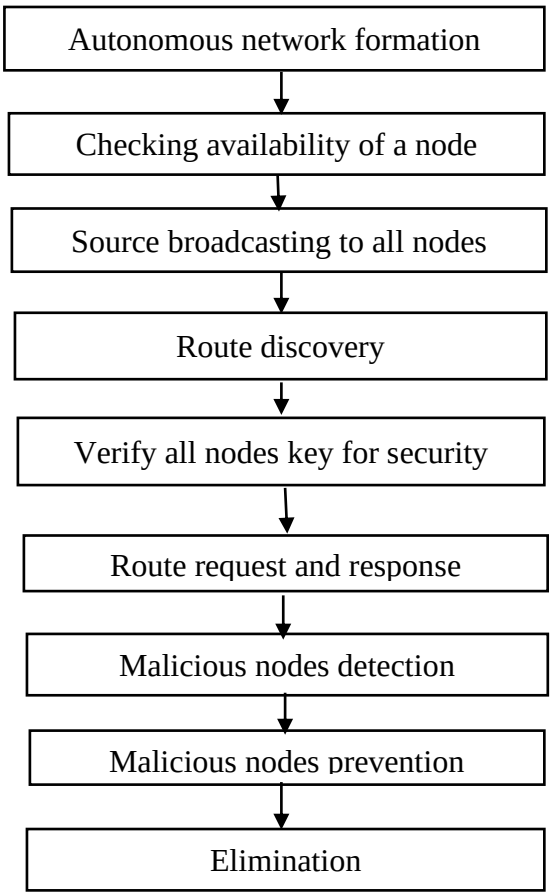


Figure 1. Flow diagram of the Proposed method

Firstly, an autonomous network is created in an NS-2 environment, and then the accessibility of node will be checked. The communications of the source to all the nodes are achieved in the next stage. Then the process of route discovery will take place. In this stage, the source introduces the route discovery only once there is a requisite. The source node inspects its route cache to validate which routes are existing between destination and source. If no route is recognized, it begins a route discovery phase. The packet referred by a source contains the information of addresses of the destination and the intermediate nodes. After this route discovery, the verification process of all the nodes key is done for security in application layer. Route request and response is obtained after the verification process. Malicious nodes detection is done after obtaining the RREQ and RREP. After this process, the prevention or elimination of the grayhole attacks is done by using the novel secure detection prevention and elimination gray hole technique. Further, the performance metrics for instance PDR, throughput, security and energy consumption is analyzed and compared with an existing technology which will be discussed in the subsequent parts.

3.2 Proposed SDPEGH Algorithm

SDPEGH:

```
Begin
egin
Initialize network
Set nm[i][i]; // where i=node ‘x’ position, j=node ‘y’ position
Set source=sn;
Set key[]=nm; // nm denotes number of mobile nodes
Set Neighbor[i][j]=nid;
Set Location[i][j]=L;
Set TopoRange[i][j]=Tr;
For {set i 1} {i<=nm} {incr i}
{
For {set j 1} {j<=nm} {incr j}
{
Location[i][j]=nm[i][j];
}
}
End
Begin
```

Checking topology Range

```
For {set i 1} {i<=nm} {incri}
{
For {set j 1} {j<=nm} {incr j}
{
TopoRange[i][j] =nm[i][j];
}
}
End
Begin
```

Route Discovery with Key

```
For {set i 1} {i<=nm} {incr i}
{
For {set j 1} {j<=nm} {incr j}
{
```


Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Neighbor [i][j] =nm[i][j];
Route req_sent->sn;
}
}
End
Begin
GH (key, packets)
{
If (next! =receiver)
{
Key=neighborkey;
Malicious (key, packets)
}
}
End
Begin
Malicious (key, packets)
{
If (closest-neighbor! =listed)
{
Forward packet (key, packet)
}
}
End

Gray hole attack detection

Begin
For {set i 1} {i<=nm} {incri}
{
For {set j 1} {j<=nm} {incr j}
{
If (nm[i] packets.equals (drop))
{
Blocklist[i] =nm[i];
Message (gray hole attack detected);
}
Else
{
Message (Packets send to sink);
}
}
}
End

Gray hole attack Prevention

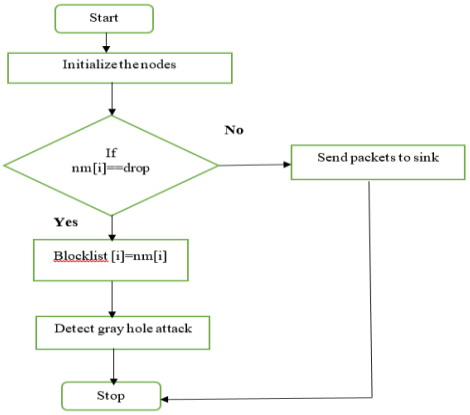
Begin
For {set i 1} {i<=nm} {incr I}
{
For {set j 1} {j<=nm} {incr j}
{
If (key. Equals (null) &&ipaddress.equal (redundant) &&UDPpacket (dropped))
{
Blocklist[i] =nm[i];
}
If (key! =null &&ipaddress (unique) &&UDPpacket (send)&&consume_energy&& session)
{
Send[i]=nm[i];
Message (legitimate packets send to sink)
}
Else
{
Message (node cannot receive legitimate packets)
}
Else
{
Message (default communication)
} } } End

Gray hole attack elimination

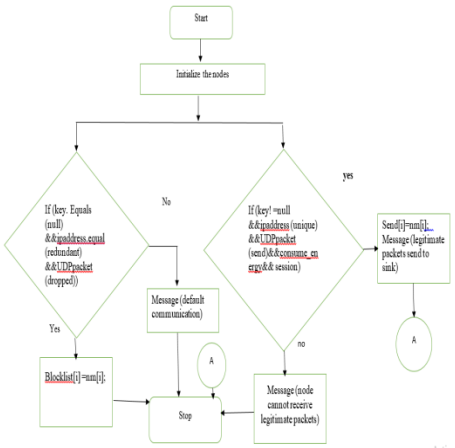
Begin
For {set i 1} {i<=nm} {incr I}
{
For {set j 1} {j<=nm} {incr j}
{
If (nm[i]!=key &&txtime.equal(high) &&nm[i](exists in blacklist))
{
Remove_nm[i] = from Location[i][j];
Message (gray hole eliminated from network);
}
}
}
End
End

3.3. Flowcharts

3.3.1 Gray hole detection

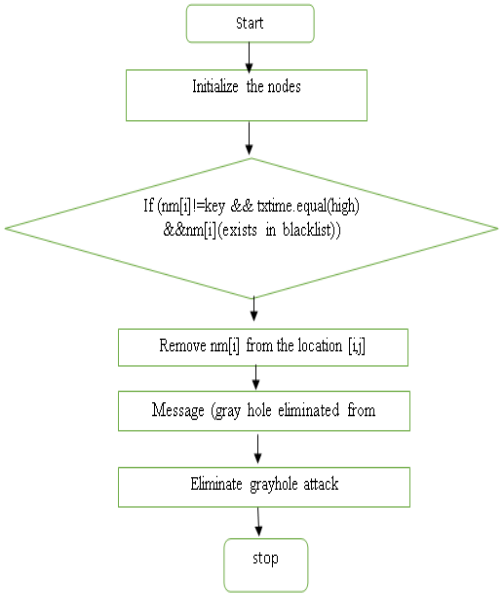


3.3.2 Gray hole Prevention



3.3.3 Gray hole elimination

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)



4. EXPERIMENT

The experimental setup considered for the study is given in this section. It mainly includes Network simulator two software tool with the version Ns-allinone 2.34. TCL is the front-end, then C++ is a back-end. The number of nodes considered is 45, and the performance metrics used for evaluating the proposed technique is the PDR, Throughput, The consumption of energy, and Security. The experimental setup details are deliberated in the below-given table 1.

Table 1. Experimental Setup

Experimental Setup	
Tool	NS2
Version	Ns-allinone 2.34
Front End	TCL
Back End	C++
Number of Nodes	45
Performance Metrics	PDR Throughput Energy consumption Security

5. RESULTS AND ANALYSIS

The simulation parameter details are as presented in the table 2. It shows the particulars of the simulation parameter along with its values. It mainly includes the quantity of nodes which is considered here as 45. The range of the topology as (1386,1500), the type of the Antenna is omnidirectional; the propagation model is a two-ray ground, the application is UDP. The size of the packet is 1000, and then the protocol used for routing is DSDV.

Table 2. Simulation Parameters

Parameters	Values
Total nodes	45
Topology range	1386,1500
Type of the Antenna	Omnidirectional antenna
Propagation model	Two-ray ground
Application	UDP
Packet size	1000
Routing protocol	DSDV
Simulation time	40 seconds
Phy/WirelessPhy set RXThresh, CSThresh	$1.42681e^{-12}$

5.1 RESULTS OBTAINED IN THE EXPERIMENT

This section mainly discusses the simulation parameters along with the process of Autonomous network formation, checking the availability of node, source broadcasting to all nodes, route discovery, verify all nodes key for security, route response and request, malicious nodes detection, prevention, elimination and performance metrics.

5.1.1 Network Formation

Figure 2 demonstrates the formation of an autonomous network in the environment of a network simulator. It includes a mobile nodes set in which every node should possess some kinds of identification which is like mobile nodes as mn1, mn2, mn3, mn4, mn5, mn6, mn7……mnn. In this figure 1, brown color nodes represent the node attributes which specifies that the normal node presents or exists in a network. Blue color specifies the source and destination nodes i.e., node-21 (source node) and node-35 (destination node).

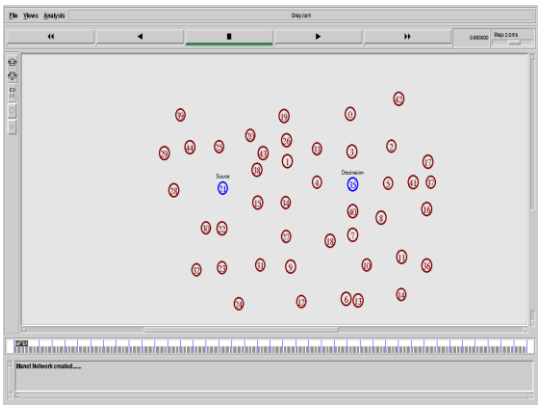


Figure 2. Network Formation

5.1.2 Route Discovery

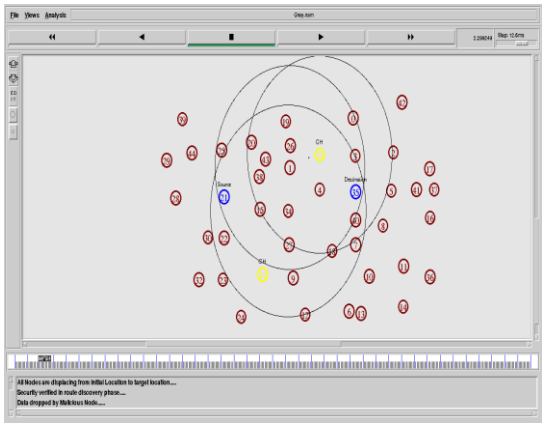


Figure 3. Route Discovery(t=0.9sec)

Figure 3 demonstrates the phase of route discovery. Here, all nodes are displacing from initial location to target location. Security is verified in the route finding phase, and then the data or packet is dropped by the malicious node.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

All Nodes are checking transmission range for before transmission. In this phase, the source will forward a broadcast request to all the neighboring nodes for the purpose to discover a route. The process of route discovery occurs at 0.9 seconds.

5.1.3 Route Discovery with verification by ID

Figure 4 shows the route discovery phase with verification by ID. Here, the gray hole attack is detected. In this route discovery phase, all the nodes are verifying the key for secure communication. If any node comes into a network without a key, then that node is added into the block list. The process of the verification was achieved at the time of 1.22 seconds. In the below figure yellow color nodes are recognized as gray hole attacks.

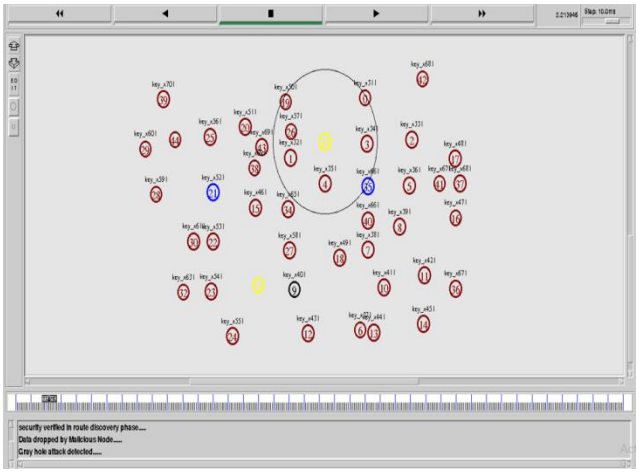


Figure 4. Route Discovery with verification by ID

5.1.4 Gray hole Attack Detection

The grayhole attack detection is achieved as presented in figure 5. The grayhole attack detected without a key. Here, the yellow color node represents a grayhole attack which attacks dropping incoming and outgoing message from the source. The process of the gray hole detection occurs at 2.18511seconds.Figure 6. Shows the simulation diagram of the gray hole attack detection before elimination.

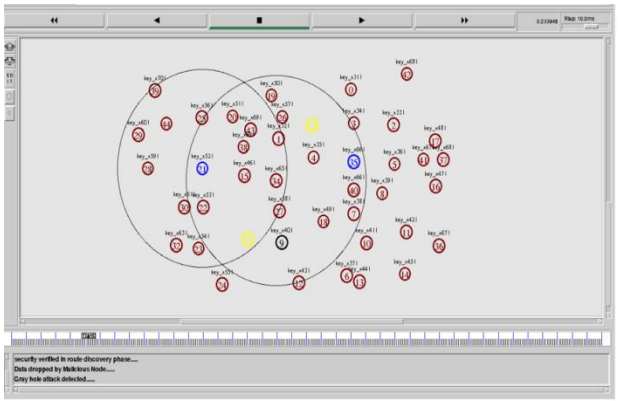


Figure 5. Gray hole Attack Detection (t=2.18511sec)

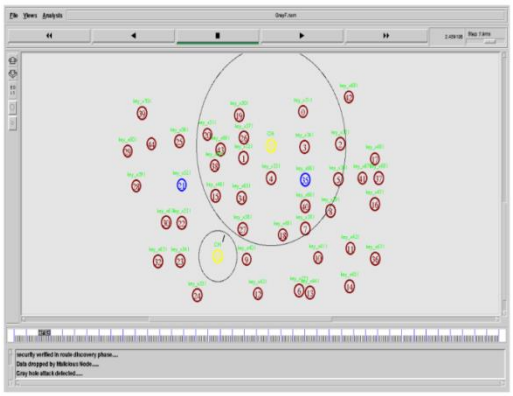


Figure 6. Screenshot showing the implementation process before grey hole elimination

5.1.5 Grayhole attack Elimination

Figure 7 represents the elimination of the grayhole. In this module, attacker eliminated from this network for reduced network traffic. Figure 8. displays the simulation diagram of the gray hole attack after the elimination.

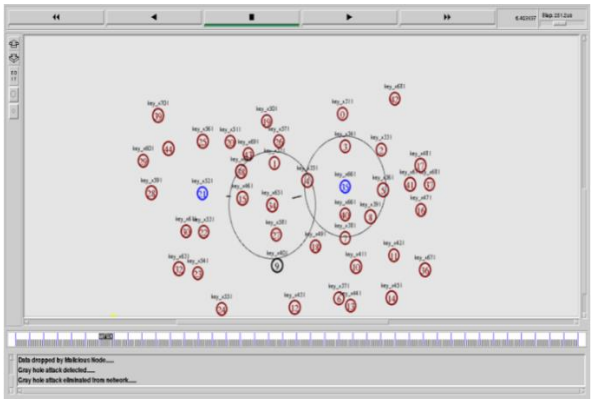


Figure 7. Eliminationof the gray hole (t=5.318sec)

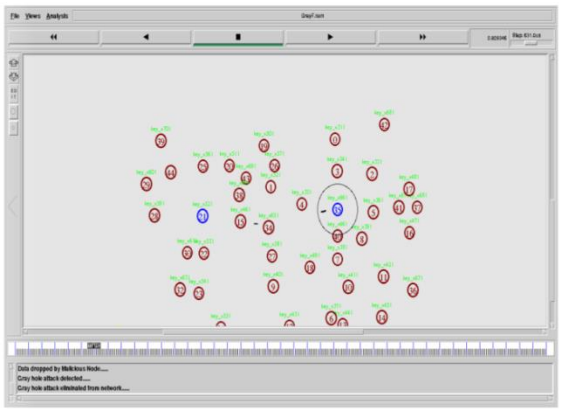


Figure 8. Screenshot showing the implementation process after grey hole elimination

5.1.6 Communication End

Figure 7 shows the ending process of communication. In this module, after eliminating the grayhole attacker from this network and data communicated successfully without delay and reduce energy consumption. The process of communication is successfully competed at the time of 8.9825 seconds.

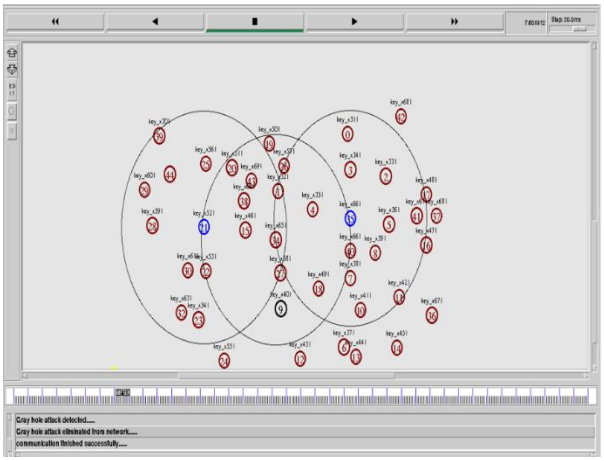


Figure 7. Communication End (t=8.9825s)

Trace file:

The following figure shows the trace file of the proposed method.

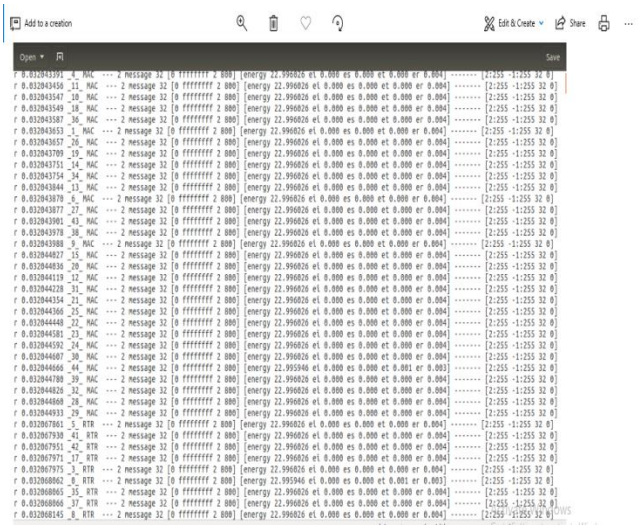


Figure 8. Trace file of the Proposed method

6.1 Performance metrics

6.1.1 Throughput Analysis

The quantity of packets which pass passing over a channel in a specific unit of time. This performance metric demonstrates the total number of packets that have been effectively carried from source to sink, and it could enhance by increasing its speed.

$$Throughput = \frac{numberofdatapacketsreceived * packetsize * 8}{simulationtime} \quad (2)$$

Here, calculated throughput states to an average data rate of fruitful data or else message conveyance over a particular communications link. Throughput is mentioned in kilobits per second (kbps) between existing CRCMD&R, Gray hole technique and Novel SDPEGH. The green color output specifies the performance of the proposed SDPEGH for throughput. The red color and blue color results shows the performances of the existing CRCMD&R and Gray hole techniques respectively.

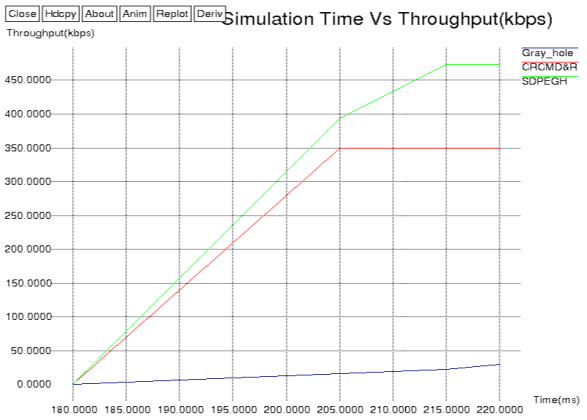


Figure 9. Throughput Analysis

The throughput achieved for SDPEGH is 446.66 kbps, and for the existing CRCMD&R technique, it was observed as 350 kbps. SDPEGH throughput is better compared to CRCMD&R and gray hole [19].

6.1.2 PDR Analysis

The ratio of packets of the data carried to sink to those created using CBR sources. PDR demonstrates the way that a protocol performs delivering packets successfully from sender to receiver. The higher values improve the outcomes. It describes both the comprehensiveness and exactness of a routing protocol. Its efficiency gives reliability of routing protocol. Here, sum of packets transmitted is 196 and packets received is144.

$$PDR=\frac{numberofpacketsreceived}{thenumberofpacketssent} \quad (1)$$

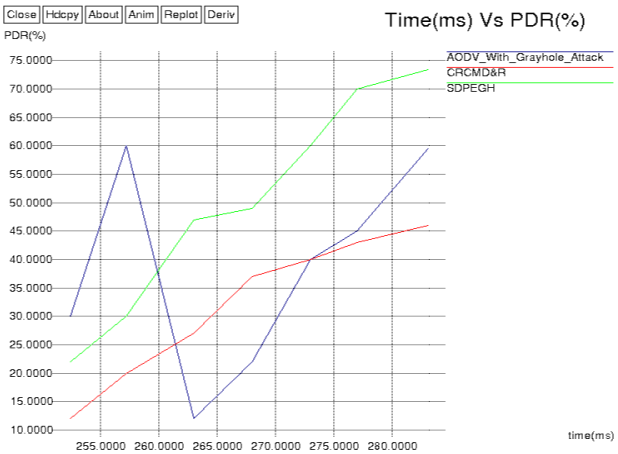


Figure 10. PDR Analysis

Figure 10 demonstrates the PDR analysis. Here, PDR is computed from generated packets and received packets after successful transmission between existing CRCMD&R and Novel SDPEGH. The PDR of the proposed algorithm is 48%, and for existing technique, it is 31.6%. The Packet delivery ratio is better in the proposed method as compared to CRCMD&R and AODV with gray hole attack[19].

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

6.1.3 Energy Consumption Analysis

From the energy saving point of view significant consideration which express you regarding the average consumption of energy of the complete network. It is computed as relation of total energy used up to the quantity of nodes in a network. For improved performance average energy consumption have to be less.

The total energy consumed is described as the difference of the initial energy of all nodes to itsresidual energy.

$$Total\ energy\ consumed = (No.of\ nodes * initial\ energy) - (Remaining\ energy)$$

The energy consumption analysis is shown in figure 10. Here, consumption of energy vs. No. of nodes for the proposed SDPEGH technique. But the existing work CRCMD&R doesn't concentrate on energy consumption.

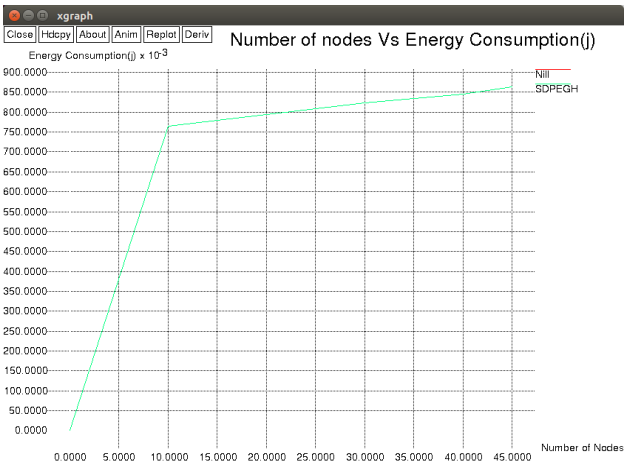


Figure 11. Energy Consumption Analysis

6.1.4 Security Analysis

Security is calculated through the trust value which is described as the relationconcerning the forward count of the data besides the received count of the data packet of the node.

$$Trust\ value = \frac{forward\ count\ of\ the\ data\ packet\ [node]}{received\ count\ of\ data\ packet\ [node]}$$

The security analysis is shown in figure 12. Here, security vs. number of nodes is mentioned for the proposed SDPEGH technique. But the existing work CRCMD&R doesn't concentrate on the security metric.

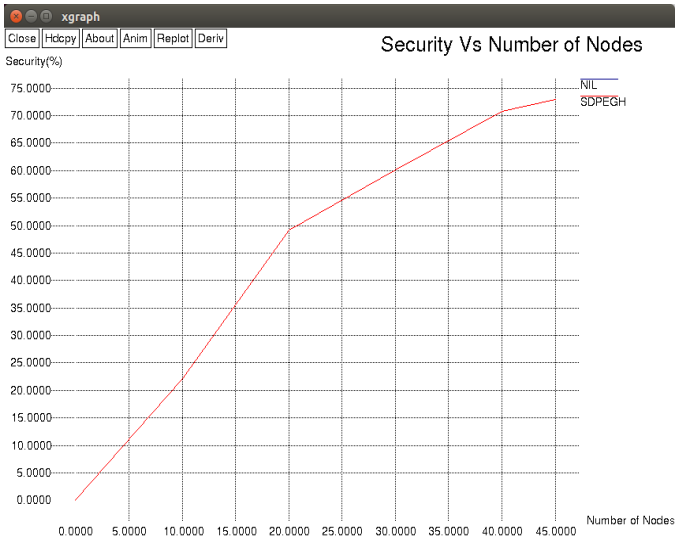


Figure 12. Security Analysis

1.1 Comparison of results with existing techniques

The presented table 2 gives the comparison between SDPEGH and existing technique such as CRCMD&R [11]. Table2 Shows the metrics of performance like PDR (%), throughput, energy consumption, and Security is improved by using SDPEGH methodology compared to the existing technique.

Table 2: Comparison table

Performance metrics	CRCMD &R [11]	AODV with gray hole attack [19]	Gray hole [19]	SDPE GH (Pro posed system)
PDR (%)	31.6	Not considered	41.25	48
Throughput (kbps)	350	16.66	Not considered	446.66
Energy Consumption (mJ)	Not considered	Not considered	Not considered	810
Security (%)	Not considered	Not considered	Not considered	64.66

In the comparison table 2. The 1st column performance metric presented the parameters such as PDR, Throughput, Energy consumption, Security etc. The column-2 presented the values PDR and throughput presented by Aishwaryaet al.[11] in CRCMD&R. throughput, energy consumption and security is not considered by the authors in [11]. The column-3 presented the values for throughput presented by Patil et al.[19] in AODV with gray hole attack. The parameters such as PDR, energy consumption and security are not considered in [19]. The column-4 presented the values of PDR presented by Sachan [19] in gray hole. The parameters like throughput, energy consumption and security is not considered in [19]. At last, the last column i.e., column-5SDPEGH presented the values for PDR, throughput and energy consumption, Security which are better compared to the existing techniques.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Thus, the research for grayhole attack detection, prevention and elimination by SDPEGH methodology is fruitful.

7. CONCLUSION

This research paper proposed the detection, prevention and elimination of a gray hole by means of SDPEGH in MANET. This research is mainly based on gray hole as a malevolent attack and attempts to discover the prevention as well as elimination method. An innovative method was proposed to perceive and prevent malicious node and to advance a technique to eliminate malicious from a network. The performance metrics such as PDR, throughput, security and energy consumption was analyzed for proposed and existing systems and concluded that the proposed system performance iseffectivecompared to theother techniques.The detection, prevention and elimination of grayhole attack is implemented successfully in this research. In future we can define the Gray Hole attack impact on further routing protocolslike Dynamic source routing, Optimized Link State Routing besides measuringthe network performance. To execute any recognitionmethods, we also required to study the performance factorslikeaverage delay and routing overhead.

REFERENCES

1. Sen, J., Chandra, M. G., Harihara, S. G., Reddy, H., &Balamuralidhar, P. (2007, December). A mechanism for detection of gray hole attack in mobile Ad Hoc networks. In *Information, Communications & Signal Processing, 2007 6th International Conference on* (pp. 1-5). IEEE.
2. Usha, G., & Bose, S. (2013, February). Impact of Gray hole attack on ad-hoc networks. In *Information Communication and Embedded Systems (ICICES), 2013 International Conference on* (pp. 404-409). IEEE.
3. Chandure, O. V., & Gaikwad, V. T. (2012). Detection & prevention of gray hole attack in mobile ad-hoc network using aodv routing protocol. *International Journal of Computer Applications (0975–8887) Volume*.
4. Praveen, K. S., Gururaj, H. L., & Ramesh, B. (2016). Comparative Analysis of Black Hole Attack in Ad Hoc Network Using AODV and OLSR Protocols. *Procedia Computer Science*, *85*, 325-330.
5. Sun, B., Guan, Y., Chen, J., & Pooch, U. W. (2003, April). Detecting black-hole attack in mobile ad hoc networks. In Personal Mobile European (Conf. Publ. No. 492) (pp. 490-495). IET.
6. Xiaopeng, G., & Wei, C. (2007, September). A novel gray hole attack detection scheme for mobile ad-hoc networks. In *Network and Parallel Computing Workshops, 2007. NPC Workshops. IFIP International Conference on* (pp. 209-214). IEEE.
7. Sachan, K., &Lokhande, M. (2016). An Analysis of Gray hole Attacks on Mobile Ad-hoc Networks. *International Journal of Computer Applications*, *146*(14).
8. Tiwari, R., & Jain, J. (2017). Exposure and Mitigation of the Gray Hole Attack from AODV in Mobile Ad hoc Network: An Approach. *International Journal of Computer Applications*, *165*(5).
9. Arya, N., Singh, U., & Singh, S. (2015, September). Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm. In *Computer, Communication, and Control (IC4), 2015 International Conference on* (pp. 1-5). IEEE.
10. Chaubey, N., Aggarwal, A., Gandhi, S., &Jani, K. A. (2015, February). Performance analysis of TSDRP and AODV routing protocol under black hole attacks in manets by varying network size. In *Advanced Computing & Communication Technologies (ACCT), 2015 Fifth International Conference on* (pp. 320-324). IEEE.
11. Aishwarya, K., Chaitali P., Mrunali C., Sapna R., Umesh T., and Jubber N. (2018) "Detection and Prevention of Grayhole Attack by Using Reputation System in MANET." International Journal of Innovative Research in Computer and Communication Engineering, 6(4), 3791-796.
12. Singh, J. P., Goyal, D., Shiwani, S., & Gaur, V. (2017, February). Hindrance and riddance of Gray Hole attack in MANETs multipath approach. In *Computational Intelligence & Communication Technology (CICT), 2017 3rd International Conference on* (pp. 1-5). IEEE.
13. Sharma, S., &Gambhir, S. (2017, January). CRCMD&R: Cluster and Reputation based cooperative malicious node Detection & Removal scheme in MANETs. In *Intelligent Systems and Control (ISCO), 2017 11th International Conference on* (pp. 336-340). IEEE.
14. Hao Yang, J. Shu, "Network-layer security in mobile ad hoc networks IEEE Journal on Selected Areas in Communications", Published in IEEE in Feb, 2006
15. Sharma, R., Sharma, T., &Kalia, A. (2016). A Comparative Review on Routing Protocols in MANET. *International Journal of Computer Applications*, *133*(1), 33-38.
16. Nadaf, S. J. S., & Patil, S. (2016).SET for CWSN Using Election Algorithm for Authentication and Security Using SHA512, In *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, 5(2), 174-183.
17. Parthiban, S., Amuthan, A., Shanmugam, N., & Joseph, K. S. (2012). Neighbor Attack And Detection Mechanism in Mobile Ad-hoc Networks. In *Advanced Computing*, *3*(2), 57.
18. Jeevamaheswari, M., Jothi, R. A., &Palanisamy, V. (2018). AODV Routing Protocol to Defence Against Packet Dropping Gray Hole Attack InMANET.In*International Journal Of Science Research and Technology (IJSRST)*, 4(2). 1464-1471.
19. Patil, Y. S., &Kanthe, A. M. (2016, August). Gray Hole attack detection using false reply count and TrueLink based path authentication in MANET. In *Computing Communication Control and automation (ICCUBEA), 2016 International Conference on* (pp. 1-5). IEEE.
20. Sachan, K., &Lokhande, M. (2016, November). An approach to prevent Gray hole attacks on Mobile Ad-Hoc Networks. In *ICT in Business Industry & Government (ICTBIG), International Conference on* (pp. 1-6). IEEE.