*International Journal of Engineering & Technology*, 7 (1.2) (2018) 110-116

International Journal of Engineering & Technology

*Website: www.sciencepubco.com/index.php/IJET*

***Research paper***

# Intrusion detection and avoidance of black and grey hole attacks using AODV protocol based MANET

**Uzma Shaikh *, Arokia Paul Rajan**

*Department of Computer Science Christ University Bengaluru, India*
**Corresponding author E-mail: uzma.shaikh246@gmail.com*

## Abstract

Mobile Ad-hoc Network (MANET) is a mobile network which has a large scale of self-directed nodes which is powerful to form a short-term means of communication network, without any use of prior communications. Due to its uniqueness like partial resources, varying loops and shortfall of controlling the networks, these networks are exposed to diverse network layer issues. The “Ad hoc on demand distance vector” is a self-starting directing procedure whose security is compromised with the distinct form of attack named as “Black-Hole” and “Grey Hole” attacks. This “malicious node” publicize as such, it contains the supreme track to the target during the route discovery process and thus interrupt the real communication and corrupt network performance. This paper introduces a new method in which a base node is introduced in the network that increases the probability of detecting multiple malicious nodes in the network and further separate them from taking part in any communication. It detects the corrupted nodes and prevent it by causing an effect for the communication. The proposed method has been experimented using NS2 and the results found to be efficient.

***Keywords***: *MANET; Routing Protocol; Black-Hole Attack; Grey-Hole Attack.*

## 1. Introduction

MANET contains dynamic topology, does not rely on the static communications and neither it contains any kind of base control station into the networks hence this made a challenging area of research in networks. It has a limited amount of range of the commu-nication and capabilities of power consumptions hence in real time scenario, it can be used in the military during the battle fields, during the disastrous earthquake and recovery from those disasters [1].

MANET‟s are wireless networks which make use of the electro-magnetic radio waves for the communication. There are various propagation of radio waves some of the im-portant signal modulation mechanism, multiple access techniques, error control mechanisms, etc. being familiar with this fundamental of wireless transmission is essen-tial for understanding the issues which are in wireless networks [2].

MANET hubs play out the directing capacities themselves. Because of the restricted remote transmission extend, the steering by and large comprises of different bounces. In this manner, the hubs rely upon each other to forward bundles to the goals. In MANET each hub goes about as a switch which passes information for another hub while they are not in each other's transmission range in MANET are more powerless against harmful attack on account of its element like progressively evolving topology, open medium, absence of important checking administration these assaults are wormhole attack, black gap assault, jellyfish attack, granola attack, denial of administration attack, snooping assault and so onwards.

Giving security to the hubs and their information imparting in such situations is basic. Every hub is outfitted along radio transmitter where it enable to speak up to the different hub where the wireless correspondence extend. All together a hub onward a bundle for next hub which is not present in the range, here different hubs participation in the system are required it is said to be many recoil uniformity. In this every hub must go for both as a host and as well as a switch.

Intrusion Detection Systems are recognizing the pernicious movement and give the alarm or alarm to alternate hubs. IDS framework has two sorts. Oddity based and Signa-ture based, both movements recognize the vindictive action. In Signature based, some predefined information put away in database to identify the malignant movement. In anomaly based, unusual conduct recognized in organize than it gives the alarm to alter-nate hubs in the system.

### 1.1. Reactive protocols

This kind of protocols makes courses just when they are required by the source hub. Reactive Protocol has brought down overhead since routes are resolved to request. It globally seeks concept. Continuous updating of the route tables with the most recent course topology is not required in on request plan. Reactive protocol looks for the route request way, then set bond where it expresses along with an acknowledge file container from a source hub to target hub [16]. Route determines process is utilized as a part of on request directing by flooding the route ask for (RREQ) packets all over the networks. Example for this protocol‟s are Dynamic Source Routing, that is DSR and Ad hoc on Demand distance vector routing protocol, that is AODV respectively.

### 1.2. AODV protocol

AODV utilizes a remarkably infrequent method to keep up navigation data. AODV protocol is both an on request and a table driven convention. It takes up flat directing tables, one entry is made for each target.

AODV consolidates a few belongings have DSR along with DSDV which utilize direction revelation procedure which adapt the route request premise. This is a reactive protocol which utilizes navigation tables for keeping up route data and doesn't need to store up directions for the hubs which aren‟t conveying. It grasps direction disclosure operation with route request. i.e. RREQ SMS. This SMS is communicated with next nearest hubs. The SMS goes by communication till desire goal having a significant new direction is attained. Series information is deployed to ensure the flexibility Operation of the AODV protocol is given in above figure1 here, node 1 at the start which wants to be in touch with node 4 which is the target. Node 1 generate and transmit the RREQ SMS to the node 2 and 5 because node 2 and node 5 which doesn‟t contain any path to node 4 so then later again, it transmit the RREQ SMS to node 3 and node 4 yet again Node 3 transmit the RREQ communication to node 4.

If a RREQ message with the iden-tical RREQ ID is established and node rejects the recently established RREQs. Here Node 4 get two RREQ messages so the node 4 inaudibly rejects the newly received RREQs. When the end mobile node or middle mobile node which holds a clean sufficient path to the end receive than RREQ SMS which generate RREP SMS and modernize mobile node's direction covering counter to collect leap tally and the sequel of target mobile nodes. Later the RREP SMS broadcast to the starting mobile node and mobile Node 4 broadcast reply to mobile Node 1 with its new sequence number. Figure 1 shows RREQ and RREP packet flow.

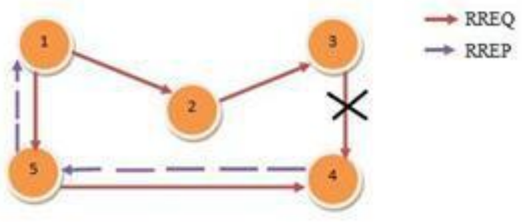


**Fig. 1:** The Coordinator Plane of RGL.

### 1.2.1. RREQ

Sender which requires to be in touch with nearby nodes which broadcast RREQ communication. Here the AODV which sends these communications, with the increasing loop method. It has a range to keep up the value for every RREQ SMS and the significance of time to live order the series of bound RREQ which must be broadcast.

### 1.2.2. RREQ

The mobile nodes which contains request or whichever middle mobile node which have direction of the requested mobile node can produce direction to reply RREP SMS and later it get reverse to the created node.

### 1.3. Black hole attack

The malicious mobile node present oneself as if it contains shortest track into the formed network and the transmission of the data into the network, hence fail to hold up the data back to send ahead for its nearest mobile nodes. This is most frequent and stand-ard attack into the networks hence known such as a Denial of Service (DOS) attack [15]. Particularly here mobile nodes which induce a request SMS and proceed the same to its nearest mobile node, this malicious mobile node publicly, says that it holds the correct way for the end mobile node hence later when it gets the RREQ SMS by the starting mobile node it quickly response a false reply SMS to the mobile nodes. The first mobile node gets the false reply SMS and then its start forwarding the data to the target mobile node by the route which is discovered then the mobile node which contains the malicious route starts discarding all the data which is flowing and it is called “swalling the data”.

### 1.4. Grey hole attack

The malicious mobile node which attempts to pass half data and swallow other half data into the network Every in between mobile nodes are placed within the range so that it can get the RREQ SMS and has the input present into the table which is formed for the routing which had forward the RREQ SMS. The next nearest hop mobile nodes along a new correct route till the other mobile nodes starts transmission of data from the start till the target gets the RREQ reply SMS to the nearest mobile nodes by the others which have got the RREQ SMS in the network. A gray hole attack is launched by a single mali-cious node or hand in glove with a collection of malicious nodes [3]. The malicious node is the node which acts anomalous into the mobile network which causes a lot of issues in the network communication and does not have a reliable commu-nication. Figure2 represents a malicious node activity.

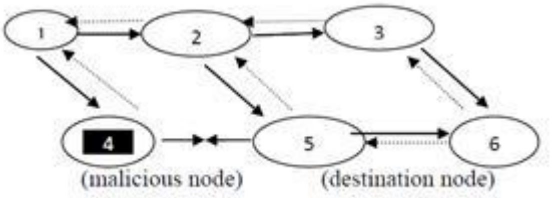


**Fig. 2:** Malicious Node.

The figure2 represents that it contains 6 nodes from all of which the first node is said as the start mobile node which produce the RREQ SMS to find the nearest correct way till the target mobile node which is the 6th node The rest all in between nodes are the middle mobile nodes of 1st node and 6th node. Here the middle mobile node gets the RREQ SMS which is produced by the 1st node and there contain a malicious node as the 4th node which publicly appeal that it has the correct way till the target mobile node once got the RREP SMS from the mobile node 4th than the mobile node 1st starts sending the original data by that route than the mobile node 4th dose not send the data to other mobile node hence it starts swalling the data.

## 2. Related work

Jain & Khuteta proposed method the deployment of the base node in the network is made so that increases the probability of detecting multiple malicious nodes in network and further isolate those malicious nodes from taking part in any communication in networks [4]. Kshirsagar & Patil proposed method to detect and prevent the Blackhole attack by means of real time monitoring suspected node by its neighbor node. The AODV routing protocol is modified to simulate the detection and prevention methodology. The Node which replies to RouteRequest (RREQ) by source is monitored in promiscuous mode and the neighbor node of RouteReply (RREP) sender node is actually detecting malicious node [5].

Parineet D.Shukla et al. proposed the method in which it shows an analytical ap-proach towards detection and removal of gray hole attack in the network. The probability of the each and every node is calculated and depending on that calculation the node can be detected as malicious and removed from the network. The solution for these malicious nodes depends on the behavior of the node in the particular network [6]. Chaitanya et al. This paper scrutinizes the misappropriate juices and advanced the advisable juice so that the structure of the gray-hole beat [7]. Vaishali Proposed method to eliminate the gray hole affects by finding all the malicious nodes which are present in the network and send broadcast to the whole network for the elimination of malicious nodes. Throughput and delay are the parameters for the performance measurements of the network.The simula-tion work is carried out by OPNET Modeler [8].

Kusumlata et al. gives brief details about all the security threats and AODV routing protocols along with gray-hole attack to investigate and analyse the need of preventive mechanism for better the efficient performance [9]. Bhandare et al. analyzed the network performance without, with one and multiple malicious nodes, by varying their location. The network performance for MDSAODV is analyzed with the same scenarios using NS-2 simulation [10]. Abdelshafy et al. Introduces a new concept of Self-Protocol Trustiness (SPT) in which detecting a malicious intruder is accomplished by complying with the normal pro-tocol behavior and lures the malicious node to give an implicit avowal of its malicious behavior and present a Blackhole Resisting Mechanism (BRM) to resist such attacks that can be incorporated into any reactive routing protocol. It relies on locally applied timers and thresholds to classify nodes as malicious. Using NS2 simulation, performance of networks using AODV under black hole attacks with and without our mechanism to SAODV, showing that it significantly reduces the effect of a black hole attack [11].

Jadhav et al. performed simulation and measured DSR algorithm for normal condition and same parameters are measured after applying disaster condition on nodes and the simulation results of disaster prevention condition are mentioned. It is observed that the performance of the network after application of prevention condition is nearly same as the normal performance. The performance is evaluated in terms of Network Throughput, Packet Delivery Ratio, and Average end to end delay [12].

Dixit et al. proposed a novel intrusion detection system for detecting black hole attack and gray hole attack which is based on table driven approach using Ad hoc on demand routing protocol and on the basis of behavior of node the computation of the vote for node and negative voting trunk the node from path nodes create a secure path using highest vote number, in this work simulation done on NS-2.35, result shows that network performance increased by the proposed principle.

## 3. Problem description

Wireless sensor networks have wide application in fields such as home, industry, environmental observation, military monitoring, and disaster relief [1]. Recent advances in wireless communications and electronics have enabled the development of low-cost sensor nodes that communicate over short distances. Wireless sensor networks are comprised of several sensor nodes that communicate via wireless technology.

## 4. Proposed model

The plan which is put forth in this model is taken up with stimulation tool that is network simulator also known as "NS2" where in the MAC layer is 802.11. These are applied to get the simulation and carry out the results and analyze them. There contain a better edition of a random way point which is used for mobility by the mobile nodes. The actions are evaluated by the protocols as follows.

i). Taking up regular typical AODV protocol in the mobile networks.
ii). The AODV along with 2 wicked mobile nodes that is blackhole and greyhole. NS2-2.35 is used to validate the detection and prevention of attacks in AODV protocol.

The process involves step by step description of the each task which takes is perform into the network that is:

1) Creation of nodes
2) Development of nodes
3) Creation of Neighboring Tables
4) Topology formation
5) Routing Table
6) Formation of Path
7) Tracking and prohibition

### 4.1. Creation of nodes

For the connections in the mobile networks, a mobile network node is having a re-lation to the other nearest mobile nodes which relay in the range which collect, store, post data along the way. Here each and every mobile node check up for the target mobile node for the transportation has an outline facility to analyse, check and proceed the transporta-tion with different network mobile nodes.

### 4.2. Deployment of nodes

The planner knows how many mobile nodes have to be deployed in the network. Mobile node deployment can be specified as an escalation of topology in mobile net-works can be just done by modifying the point of those mobile nodes and then form a desire mobile network which later meet up the command of tracking at low deployment. The worth of the deployment of these mobile nodes decides the configuration and settings of the restricted things such as energy in mobile networks, connections and bandwidth.

The quality of these mobile nodes can also affect on the services worth for the mobile network and the connections decide the mobile networks to be into random way or static fashion.

### 4.3. Creation of neighboring tables

This table consists of information of neighbour routers whose information is col-lected using Hellos. It consists of all directed neighbours. This will position the nodes in the given area. The neighbour relationships are tracked in this table which is the basis for routing and union activity. The address and the interface of a neighbour is discovered and recorded in a new entry in the neighbour table, whenever a new neighbour is discovered. These tables are used for reliable and sequenced delivery of packets.

### 4.4. Topology formation

This Segment of the process holds the entire detail about the performance and the rage of the capabilities of the awk scripts which are useful in making the topology. This module contains the making up of the mobile network topology which contains the mo-bile nodes, each mobile node functions with different varying direct channel. Here it con-tains the 2 steps which are as follows:

#### 4.4.1. Set mobile network topology

This contains surrounding management set-tings of the mobile nodes which are configure are placed into topology.

#### 4.4.2. Set bandwidth of mobile network

Here every single mobile node in the mo-bile network topology will be having a particular bandwidth and a particular topology form for that mobile network.

### 4.5. Routing table

The routes of particular destinations are stored in the routing tables. The information contains the network topology that is immediately around it. The primary goal of routing protocols and routes is the construction of routing tables. Network id, cost of the packet path and next hop are the details are available in the routing table.

### 4.6. Formation of path

In the standard algorithm named as Dijkstra‟s" algorithm is extremely like another algorithm of minimum spanning tree that is

Prim‟s algorithm wherein it generates a shortest direction from the source. This contains mainly 2 sets which have 1set of vertices which are in the forming direction and another set of vertices which are not into forming of the direction from the source till the destination. In each and every step of the algorithm it catches hold of vertex because it is into another set and has minimum distance from the source till the destination. The path formed here are maintain in the table for the record of all the actions of the mobile nodes into the network and than transfer the packets from the path.

### 4.7. Tracking and prohibhition

The standard protocol AODV is organized and a clearly said as "on demand" direction gaining schema as the mobile nodes which are not in the formation of direction does not contain any kind of information and even does not contribute in table formation of all the routes. While a mobile node which act as sources if willing to transmit SMS to the mobile node which is targeted, but do not have a proper route to the target mobile node, thus it set off a new finding of the direction to get the location of another mobile node.

This Transfer a request by the source mobile node as RREQ to the nearby nearest mobile nodes which then later transfer the command to their nearby nearest mobile nodes hence this process goes on unless the target mobile node is having a new sufficient direction is formed. In this the board-cast RREQ which transmits all into the networks where the AODV make use of the target order number to make sure that the directions for all the mobile nodes are loop free and can hold the fresh direction.

Every mobile node sustains on its self series number which even contains the board-cast Id and there is a rise in this Id for every RREQ introduce into the network. The beginning of the mobile node gets the IP address which individually identifies the RREQ along with its self series number and board-cast Id.

The Middle mobile nodes do respond to the RREQ if and only if it has a direction way to the target mobile node which is related to the target series number shall be larger than or may be equal to so that to get the control in the RREQ.

During this entire procedure of the transferring the RREQ from the mobile node which is a source node to the other mobile node which is target node it keep the track in the table of the directions which contains the neighbour address so that the 1st duplicate of the information which has been board-cast gets received by introducing the backward direction way. Suppose the extra replica of matching RREQ which are in last arriving are left over there itself and are not involved.

When the RREQ achieve the target mobile node once with a new efficient direction path than the target mobile node and the middle mobile nodes starts responding back by RREP to the neighbours by which they received the RREQ request first.

While the response RREP done by the direction backward path which had contain the path entries of received RREQ holds into the route table where it knows from which mobile node the RREQ had come and pass back by the same.

These directions by which is it forwarded the RREQ have the entries in the table which clearly points out to the active direction ahead. Every mobile node entry in the direction contains the timer that the reason the entry deletion occurs if its not utilize in the specific duration because the transmitted RREP with the direction recognize by the RREQ and symmetric links are used to support only by the AODV.

The directions are preserved if the source mobile node travels so it is capable to ini-tiate the direction finding protocol till it finds the fresh path till target mobile node. If the mobile nodes travels into the direction properly than its neighbour see the travels which is upstream and transmits a warning of the connection is crash to each and every neighbours which are active so that it removes that component.The mobile nodes which transmit the crash of the connection warning to the neighbours this is done unless and until the source mobile node is achieved.

The source mobile node initiates the direction path choice to the target mobile node only if the path really wishes to do.The hello SMS is used as an extra feature of the pro-tocol which is part by part limit the board-cast by mobile nodes because to notify the connection into the network for the neighbours to know it. This SMS is utilized to keep the connection between the mobile nodes so there is direction path is saved and then later the mobile nodes pay attention for the data for transmission and hence confirm the target mobile node and choose the new route for the transmission of the data and its packets which are efficient and is secure.

### 4.8. Designed algorithm

The following are the factors present:
MNID = ID of mobile nodes
MMN-ID = Malicious ID of Mobile Node
SS-MNID = ID of Source Sequence Mobile node
TS-MNID= ID of Target Sequence Mobile node
Step 1: Starting of the procedure which initialize Phase of Initialize the finding of the path from the source mobile node.
Step 2: Procedure of Storing
Each and Every RREP of TS-MID along with MNID are accumulated into the table of route reply.
Step 3: Eliminate the harmful Nodes when it's recognize and is fetched from the table of RREP.

- If the TS-MID is larger than the SS-MID then the entry which is in RREQ table is removed
- "Select TS-MID from table RREQ"

If (TS-MID>=SS-MID)

{

Mobile Malicious node = ID of Mobile Node entrance is removed from the Table.

}

Step 4: Choosing of the Mobile Nodes
The RREQ table contents entries are arranged properly in manner using the DS-MID.
Step 5: Pick the MNID which is contains the maximum DS-MID entries in the Routing table.
Step 6: carry on with the default process.
Invokes the procedure of the RREQ with a default AODV protocol. Hence the pro-cedure identifies and avoid the malfunction of the nodes and even it's not involved in the routing table in the network
Step 7: Transmit the data from the committed shortest direction.
Step 8: Stop

## 5. Experiment set up & evaluation matrics

The procedure which is put forth is carried out with NS-2 which means network simulator with 802.11 MAC layer. The Metrics which are involve in this mobile network and hence are evaluated and check the impact of these attacks on networks

i). Overhead
ii). Average end to end delay
iii). Packet delivery ratio

These calculations are done by using AWK scripts for a normal network, network with black-hole attack and grey-hole attack network.

The simulation which is done by the use of NS-2 tool with the area of plan as 1500m*1000m, where the number of mobile nodes use are 39 within which there are 2 mobile nodes which are malicious nodes. Black hole and Grey hole nodes which cause destruction for the route while transferring packets to the destination node. There are various traffic which is into the networks here the traffic use is CBR. Figure 3 clearly shows the actions which involve in the procedure step by step. This flow chart helps to understand the workflow of the procedure.

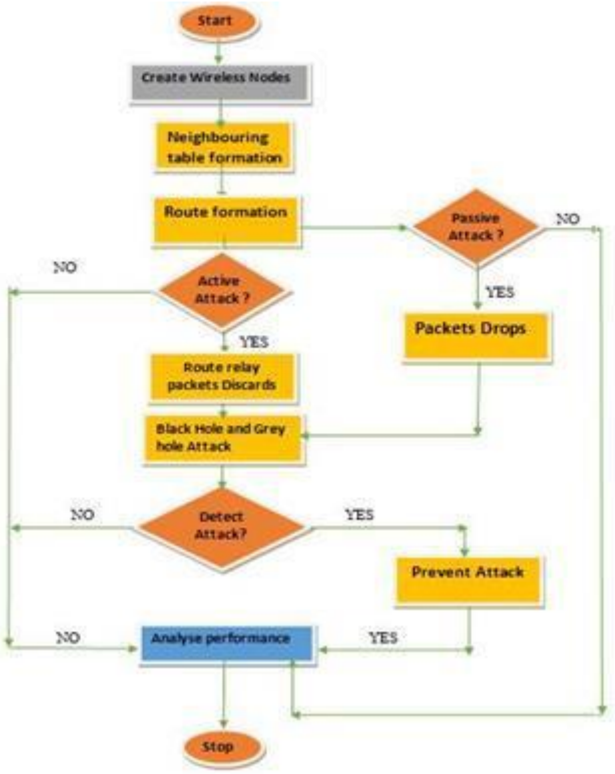


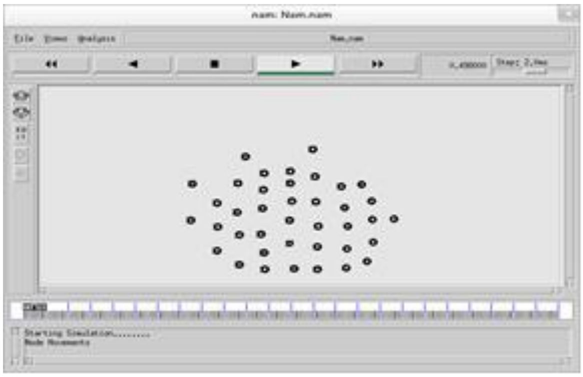
**Fig. 3:** Flow Diagram.

The given below table1 gives a clear idea of the parameters used:

**Table 1:** Performance Parameters

| Series No | Constraints | Significance |
|---|---|---|
| 1 | Present Mobile nodes | 39 |
| 2 | Measurement of x and y | 1500x1000 |
| 3 | Various Traffic | CBR |
| 4 | Model of propagation | Two Ray Ground |
| 5 | Type of MAC Layer | 802.11 |
| 6 | Size of Packet Transfer | 512 |
| 7 | Type of Antenna | Omni |
| 8 | Mobile Malicious nodes | 2 |
| 9 | Protocol in use | AODV |

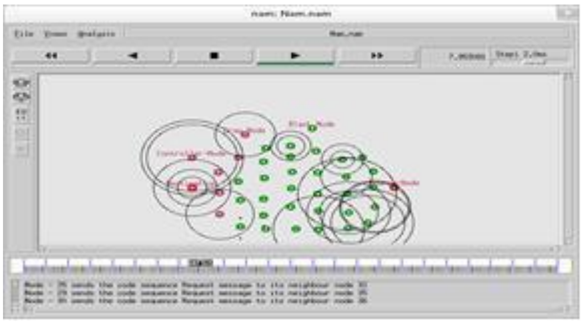
As shown in below figure 4, this is where the simulation takes place visually. Here the simulation first start and then the node deployment in random positions is noticeable. Mobile nodes when in deployment phase which even refer to the optimization of the networks and its topology just by setting the different types of locations for the mobile nodes, thus from the appropriate networks so that it meet the demand which is tracking at the lowest deployment.



```
Starting Simulation........
Node Movements
```

**Fig. 4:** Phases of Deployment.

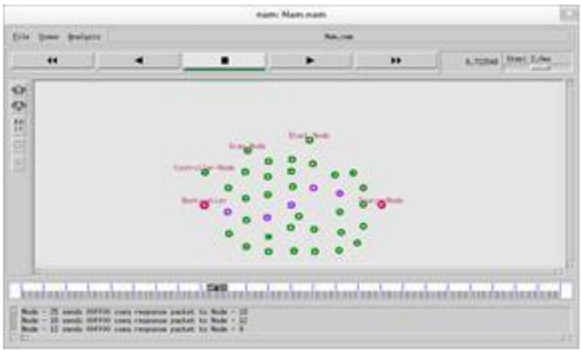
As its given in below figure5, the source mobile node starts connecting to other nearby nodes and keep a record of that neighbor by forming a neighboring table and even of the packets passes through the nodes. This continues until it reaches the destination node. This table is formed using Euler distance formula because the distance between nodes are recorded for the route formation.



```
Node - 25 sends the code sequence Request message to its neighbour node [illegible]
Node - 29 sends the code sequence Request message to its neighbour node [illegible]
Node - 35 sends the code sequence Request message to its neighbour node [illegible]
```

**Fig. 5:** Neighbour Formation to Send Request from Source to Destination.

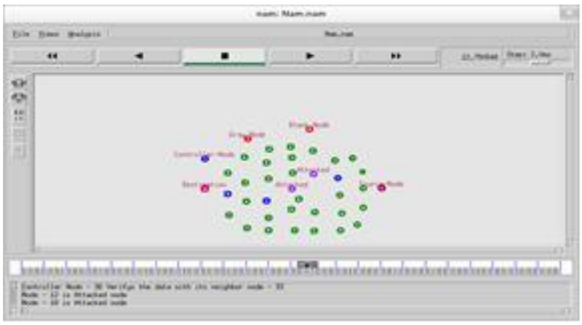
As shown in the below figure 6, the routes of particular destinations are stored in the routing tables. The information contains the network topology that is immediately around it. The primary goal of routing protocols and routes is the construction of routing tables. Network id, cost of the packet path and next hop are the details are available in the routing table.



```
Node - 25 sends [illegible] response packet to Node - [illegible]
Node - 18 sends [illegible] response packet to Node - 12
Node - 12 sends [illegible] response packet to Node - [illegible]
```

**Fig. 6:** Route Formation from Source to Destination Node.

As shown in the figure 7, the Controller or the base station node check the route which is form by the source to destination as the request is sent by the source to destina-tion the malicious nodes try to get the data which is confidential sent by the source to destination. The controller node or base station finds faults in networks of nodes and hence broadcast a message saying that the route is having faults and hence detection of the malicious node takes place.



```
Controller Node - 38 Verify the data with its neighbor node - 33
Node - 12 is Attacked node
Node - 18 is Attacked node
```

**Fig. 7:** New Route Formation from Source to Destination Node.

As shown in the figure 8, the detection part is complete than the prevention part occurs where the packets passed from the source to destination is transferred securely hence form a new route to avoid the attacker and transfer the packets trough the new route which is malicious free and hence the data is securely transferred from the source to destination.

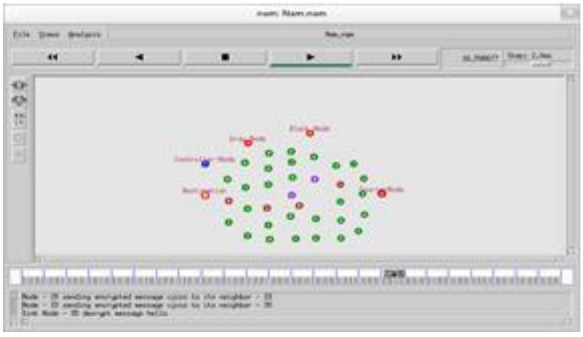


**Fig. 8:** New Route Formation from Source to Destination Node.

## 6. Analysis and results

### 6.1. Packet delivery ratio

The mobile nodes packets delivery rate is the amount by the ratio which is in be-tween the number of packets which are generated and transfer, receive loss and the ratio of the packets is checked from the source to destination, which delivers the packet efficiently with normal AODV and malicious AODV. Here in the below graph there present the x and y axis which indicate packets size and time used to deliver the packets respec-tively is shown in figure 9.

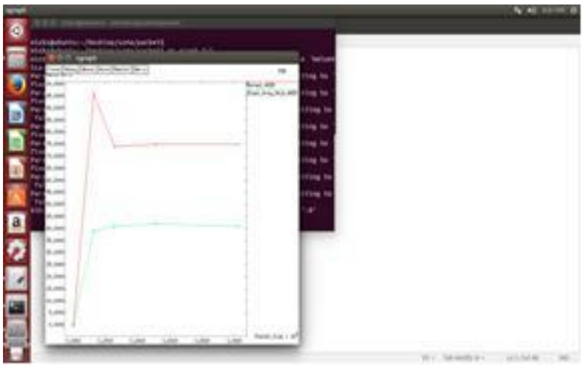


**Fig. 9:** Packet Delivery Graph.

### 6.2. Routing overhead

The overhead of the routing is the direction-finding packets necessary for network communication. Routing Overhead is calculated using AWK script which procedure the trace file and produce the result. This is calculated based on normal AODV and malicious AODV. Here it has 2 axis which are x and y these indicates the packets size and overhead values for the mobile network is shown in the figure 10.

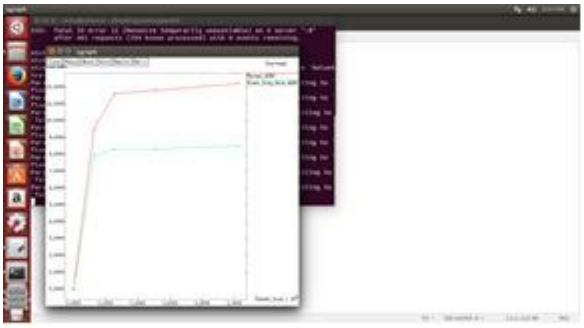


**Fig. 10:** Graph for End to End Delay.

### 6.3. End to End Delay

This is the amount of time required by the packets which is sent by the source mo-bile node to the target mobile node the travel time of the packets are known as End to End Delay with and without Malicious Nodes. This is calculated based on normal AODV and malicious AODV. There are axis such as x and y which represent the packet size and the end to end delay values plot respectively.

## 7. Conclusion

In the proposed methodology a secure and efficient way for the Recognization and Avoidance of malicious attacks in MANET"s are analysed and thus the performance is taken using NS2 2.35 and algorithm for this is essentially implemented in AODV protocol. The proposed algorithm is done using IDS of the nodes in the networks where these IDS keep watch on each and every node actions in the network where this is control by the base station if once the base station get to know that the node in the network is acting maliciously than it broadcast a message to nearby all the nodes to take up a new fresh route leaving those nodes which are malicious in the network as the mali-cious node track is maintained in the routing table.

## References

[1] R. Kumar, A. Quyoom and Devki Nandan Gouttam, "To mitigate black hole attack in AODV," 2015 1st International Conference on Next Generation Compu-ting Technologies (NGCT), Dehradun, 2015, pp. 307-311.

[2] B .S .Manoj and S. R. Murthy, “Ad Hoc Wireless Networks”, Pearson Education, 2008.

[3] Shani Makwana and Krunal Vaghela, “Cooperative Gray Hole Attack Detection and Prevention Techniques in MANET”, Published in International Journal of Science and Research (IJSR), vol 4, 2015.

[4] Sakshi Jain, Dr. Ajay Khuteta, “Detecting and Overcoming Black hole Attack in Mobile Ad hoc Network”, IEEE. International Conference on Green Computing and Internet of Things (ICGCIoT), 2015. https://doi.org/10.1109/ICGCIoT.2015.7380462.

[5] D. Kshirsagar and A. Patil, "Blackhole attack detection and prevention by real time monitoring," 2013 Fourth International Conference on Computing, Commu-nications and Networking Technologies (ICCCNT), Tiruchengode, 2013, pp. 1-5. https://doi.org/10.1109/ICCCNT.2013.6726597.

[6] P. D. Shukla, A. M. Kanthe and D. Simunic, "An analytical approach for detection of gray hole attack in mobile ad-hoc network (MANET)," 2014 IEEE Internation-al Conference on Computational Intelligence and Computing Research, Coimba-tore, 2014, pp. 1-5. https://doi.org/10.1109/ICCIC.2014.7238296.

[7] M. Chaitanya Kishore Reddy and Boya Sripriya, “A Study on Gray-hole Attacks in Mobile Ad-hoc Networks”, 2017 International Journal of Advance Technology and Innovative Research, vol 9, pp. 1634-1636, 2017.

[8] Vaishali Mittal, “Prevention and Elemination of Grey-hole Attack in Mobile Ad-hoc Networks by Enhanced Multipath Approach”, 2015 International journal of Advance Research in Computer Engineering and Technology, vol 4, 2015.

[9] Kusumlata Sachan and Manisha Lokhande. An Analysis of Gray-hole Attacks on Mobile Ad-hoc Networks. International Journal of Computer Applications 146(14):42-45, July 2016. https://doi.org/10.5120/ijca2016910954.

[10] Bhandare A.S and Patil S.B, “Securing MANET against Co-operative Black hole attack and its performance analysis- A case Study”, 2015 International Conference on Computing Communication Control and Automation, pp. 301-305, 2015. https://doi.org/10.1109/ICCUBEA.2015.63.

[11] M. A. Abdelshafy and P. J. B. King, "Resisting blackhole attacks on MANETs," 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, 2016, pp. 1048-1053.

[12] S. S. Jadhav, A. V. Kulkarni and R. Menon, "Mobile Ad-Hoc Network (MANET) for disaster management," 2014 Eleventh International Conference on Wireless and Optical Communications Net-

works (WOCN), Vijayawada, 2014, pp. 1-5. https://doi.org/10.1109/WOCN.2014.6923074.

[13] S. Dixit, P. Pathak and S. Gupta, "A novel approch for gray hole and black hole detection and prevention," 2016 Symposium on Colossal Data Analysis and Net-working (CDAN), Indore, 2016, pp. 1-6. https://doi.org/10.1109/CDAN.2016.7570861.

[14] Vandna Dahiya et al, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.7, July-2014, pg. 466-473.

[15] M. Patel and S. Sharma, "Detection of malicious attack in MANET a behavioral approach," 2013 3rd IEEE International Advance Computing Conference (IACC), Ghaziabad, 2013, pp. 388-393. https://doi.org/10.1109/IAdCC.2013.6514256.

[16] K. J. Sarma, R. Sharma and R. Das, "A survey of Black hole attack detection in Manet," 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), Ghaziabad, 2014, pp. 202-205. https://doi.org/10.1109/ICICICT.2014.6781279.

[17] K. Ramanarayana and L. Jacob, "Secure Routing in Integrated Mobile Ad hoc Network (MANET)-Internet," Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2007), Istanbul, 2007, pp. 19-24. https://doi.org/10.1109/SECPERU.2007.11.

[18] S. D. Khatawkar and N. Trivedi, "Detection of gray hole in MANET through cluster analysis," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2015, pp. 1752-1757.