Effect Of Grayhole Attack With Ids Technique For Aodv Routing Protocol Using Network Simulator

Garima Neekhra*[1],Sharda Patel[2],Ashok Verma[3],Ashish Chaurasia[4]
[*1]Research Scholar, CSE,Gyan Ganga Institute of Technology And Science,Jabalpur,M.P,India.
[2]Assistant Professor,CSE, Gyan Ganga Institute of Technology And Science,Jabalpur,M.P,India.
[3]Assosciate Professor,CSE, Gyan Ganga Institute of Technology And Science,Jabalpur,M.P,India.
[4]Assistant Professor,CSE, Gyan Ganga Institute of Technology And Science,Jabalpur,M.P,India.

Abstract--- **In MANET, the Gray Hole attack, is a node in the network start behaving like a Gray hole node that selectively drops and forwards data packets after advertises itself as having the shortest path to the destination node in response to a route request message. Mobile ad hoc networks (MANET) are widely used in places where there is little or no infrastructure. A number of people with mobile devices may connect together to form a large group. Later on they may split into smaller groups. This dynamically changing network topology of MANETs makes it vulnerable for a wide range of attack. Many researchers have given different solutions for preventing and detecting this attack. We have discussed a methodology in this survey. We are using AODV protocol for sending packet to the destination. and then introducing a grayhole node which drops the packet. To improve the performance we are using IDSaodv technique, which enable us to minimize the attacks on integrated MANET-Internet communication efficiently. In this paper we have used AODV routing Protocol for route discovery. When malicious node starts dropping packets we use Intrusion Detection scheme to report violation of policy and the nodes whose packets are dropped again try to establish new paths using Route Requests (RREQ) messages. In our paper the NS2 scenario shows that the throughput is improved than traditional gray hole attacks.**

Keywords-- **MANET, AODV, Routing Protocols, grayhole node, malicious node.**

I. INTRODUCTION

In a MANET, a collection of mobile hosts with wireless network interfaces form a temporary network without the aid of any fixed infrastructure or centralized administration. There are a wide variety of attacks that target the weakness of MANET. For example, routing messages are an essential component of mobile network communications, as each packet needs to be passed quickly through intermediate nodes, which the packet must traverse from a source to the destination. Malicious routing attacks can target the routing discovery or maintenance phase by not following the specifications of the routing protocols. There are also attacks that target some particular routing protocols, such as DSR, or AODV. MANET often suffers from security attacks due to its basic features like open medium, cooperative algorithms, dynamic changes in network topologies, lack of a clear line of defense, lack of centralized monitoring and management point. While these characteristics are important for the pliability of MANETs, they introduce specific security concerns that are either absent or less intense in wired networks. MANETs are permeable to various types of attacks including passive eavesdropping, impersonation, active interfering and denial-of-service

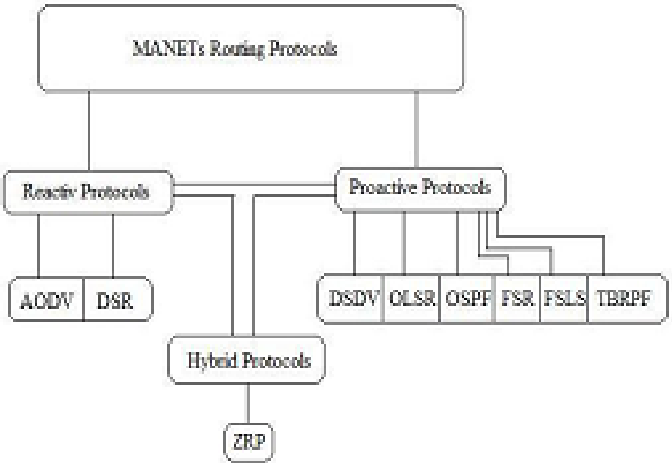


Fig.1.Types of routing protocol

II. SECURITY ATTACK

[5] The attacks in MANET can roughly be classified into two major categories, namely passive attacks and active attacks, according to the attack means. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET. Table 1 shows the general taxonomy of security attacks against MANET. Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay. The attacks can also be classified into two categories, namely external attacks and internal attacks, according the domain of the attacks. Some papers refer to outsider and insider attacks. External attacks are carried out by nodes that do not belong to the domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows valuable and secret information, and possesses privileged access rights.

Table 1: Security Attacks Classification

Passive Attacks	Eavesdropping, traffic analysis, monitoring
Active Attacks	Jamming, spoofing, modification, replaying, DoS

III. PROTOCOLS USED IN MANET

In MANET nodes communicate with each other by using some routing protocols. According the dynamic topology and characteristic there are three main routing protocol used in MANETs. These all are discussed below.

A. Reactive (On-Demand) Routing Protocol:

This protocol starts functioning whenever any node wants to transmit data to other node. In this protocol network bandwidth is not wasted and network is less congested. This protocol is less secure than the proactive protocols. Two kinds of protocols are there in it Adhoc On Demand Distance Vector (AODV) protocol, Dynamic Source Routing (DSR) protocol.

B. Proactive (Table Driven) Routing Protocol:

This protocol is also called as table driven protocol because in this protocol each node in the network maintains its detailed routing table. These all are discussed below.

In the routing table each node maintain complete path to the reachable node with its hop count. In this, each node periodically broadcast their routing information to the neighbors. Periodically update and large routing table generate large amount of overhead in the network which makes this protocol unusable. There are two main kind of this protocol optimized link state routing
(OLSR) protocol and destination sequenced distance vector routing (DSDV) protocol.

C. Hybrid Routing Protocol:

This protocol combines advantages of both proactive and reactive routing protocol. Two types are: Zone routing protocol (ZRP) and temporally ordered Routing protocol (TORA). At the initialization phase this follows proactive characteristic after that in between when network topology has changed it follows reactive characteristic.

IV. OVERVIEW OF AODV ROUTING PROTOCOL

AODV (ad hoc on demand distance vector) as the name suggests, it works when any node need to communicate or transmit data to other node. This routing protocol is developed by inheriting the property of DSDV protocol. The protocol uses four types of control messages RREQ, RREP, RERR and HELLO. The format of RREQ and RREP packets are in Fig 1.1 and 1.2 respectively.

Src_ addres	Src_ sequence	Broad_ Cast_id	Dest_ addres	Dest_ sequence	Hop count

Fig 1.1 AODV RREQ Field

Src_ addres	Dest_ addres	Dest_ sequence	Hop Count	Life time

Fig 1.2 AODV RREP Field

Packet format RREQ packet contains source address, destination address, destination sequence number, hop count and life time. In this protocol every node only records next hop information in its routing table. When a node (sender) needs to send data to other node (Destination) and destination node is unreachable from sender then route discovery process is started. In this process first of all it will initialize a RREQ for getting the route. It broadcasts RREQ to all its neighbors; all the intermediate nodes receive RREQ. If there is any node which has fresh route to the destination then it
sends RREP to the sender, when sender finds RREP it immediately starts sending data to that node which sent RREP to the sender .Whenever there is topology change or connection failure in network route maintenance process is started for it source node informed by the RERR packet then it utilizes routing information to decide other routing path or restart the route discovery process.

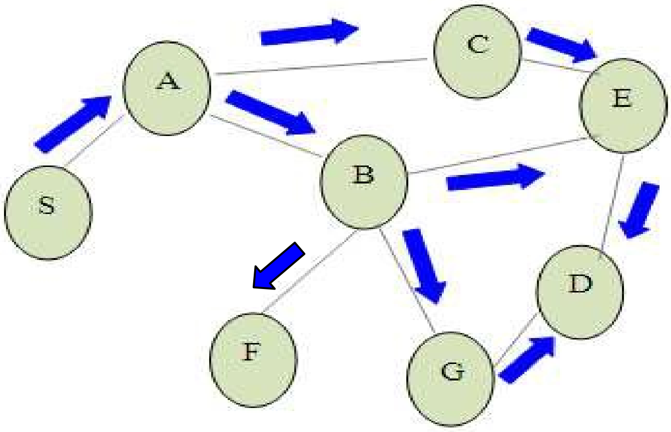


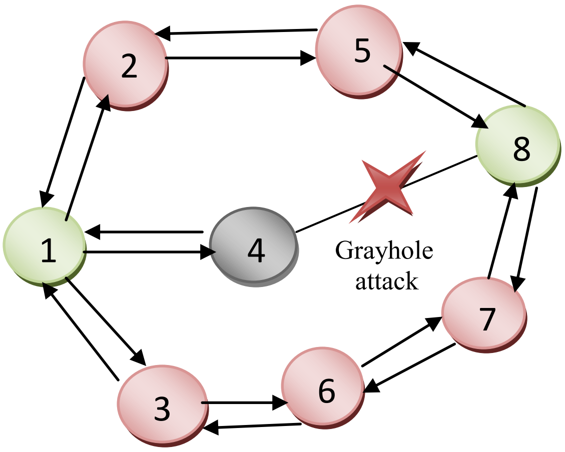
Fig. 2. AODV route discovery using RREQ Packet

V. GRAY HOLE ATTACK

[1] In gray hole attack, a node that is a member of the network, gets RREQ packets and creates a route to destination. After creating route, it drops some of data packets. This kind of dropping against black hole, does not drop all data packets. Attacker drops occasionally packets. It means attacker sometimes acts like a normal node and other times as a malicious node.

[4]The Gray Hole attack has two phases. Initially, a malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious.

Next, the node drops the intercepted packets with a certain probability. This attack is more difficult to detect than the black Hole attack where the malicious node drops the received data packets with certainty. A Gray Hole may exhibit its malicious behavior in various techniques. It simply drops packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of Gray Hole attack is a node behaves maliciously for some particular time duration by dropping packets but may switch to normal behavior later. A Gray Hole may also exhibit a behavior which is a combination of the above two, thereby making its detection even more difficult.



1-source node
8-destination node

VI. LITERATURE REVIEW

A. S Banerjee et.al.[6] have proposed the algorithm to prevent Black/Gray hole attacks.

[6] In this paper we have studied the work that attempt to detect black or grayhole or cooperative black and gray hole attack. Finally they proposed a feasible solution for detection and removal of chain of cooperative black and gray hole attack in AODV protocol. In solution each node can locally maintain its own table of black listed nodes whenever it tries to send data to any destination node and it can also aware the network about the black listed nodes. This list of malicious nodes can be applied to discover secure paths from source to destination by avoiding multiple black/ gray hole nodes acting in cooperation.

B. Onkar V.Chandure ME-I.T. (2nd Year) Sipna's College of Engg & Tech Amravati (MS) INDIA.

[10]In this paper we have implemented the AODV protocol with PDR & e2e term & also analyze the impact of gray hole attack on adhoc network, with their PDR & e2e value. Simulation of AODV as well as gray hole attack is carried out by using ns-2 tool & performance of AODV implementation is carried out before the gray hole attack on adhoc network as well as after the gray hole attack on AODV protocol.

C. Marti, S., Giuli, T. J., Lai, K., and Baker, M. 2000. In Proceedings of the 6th Annual International Conference on MOBICOM, Boston, Massachusetts, United States, 255-265.

[12]By using watchdog timer, malicious node can be detected. Each node monitors its next node in the route. If it finds any packet forwarding misbehavior or any packet dropping in a predefined period of time for its next node, it will introduce the next node as a malicious node to the source.

Advantages

- This is a simple method, so that one node should just listen to its next node in the route.

Disadvantages

- In watchdog, each node should always monitor its next neighbors.
- Source node should trust the other node's information about one node's misbehavior.

It does not use predefined limit to distinguish malicious nodes and as previously mentioned it increases numbers of mistakes to find gray hole attacks.

D. Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., and Nemoto, Y. 2007.

[13] Another algorithm is considering a limit for sequence number. When source node receives RREP packets, it checks them with a threshold for sequence number of that route and if the received RREP sequence number is higher than that, source enters that node ID in a blocked list and announces that node as malicious to all nodes by broadcasting its ID; because in Gray hole, attacker starts dropping packets by announcing itself as a node has the freshest route to destination. This sequence number threshold is calculated by average of table's entries sequence numbers in a certain period of time.

Advantages

- Main benefit of this method is simplicity.
- On the contrary of other methods, no energy is consumed for monitoring.

Disadvantages

- This algorithm does not detect any grayhole attacks.

This method may also make mistake when a node is not malicious, but according to its higher sequence number may be entered into blocked list.

E. Vishnu K B.tech V sem MNNIT Allahabad INDIA. 2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 22.

[9]The main idea behind this method is to list out the set of malicious nodes locally at each node whenever they act as a source node. As mentioned in the Assumption our protocol uses the concept of Core Maintenance of the Allocation Table i.e., whenever a new node joins the network, it sends a

broadcast message as a request for IP address. The backbone node on receiving this message randomly selects one of the free IP addresses. The new node on receiving the allotted IP address sends an acknowledgement to the BBN. Now since the allocation is only under the control of the Back Bone Nodes (BBN) the dynamic pool of unused/restricted IPs of the network at any point of time is known only to the BBN.

VII. IMPLEMENTATION AND METHODOLOGY

Intrusion Detection System

An IDS is a second protection for MANETs security. An intrusion detection system is system software used to analyze malicious behaviors network and generate reports. It can be defined as a process of monitoring the events occurs in the computer system or network and analyzing for an intrusions dealing with confidentiality, integrity and availability of a computer system.

Implementation

The proposed protocol used is called IDSAODV (Intrusion Detection System AODV). To explain the Gray Hole Attack we added a malicious node that exhibits Gray Hole. For implementing gray hole we have done changes in tcl file in ns2. We have addad grayholeaodv in ns-lib.tcl.then we also add grayholeaodv in make file present in ns-2.34 folder, this line is added in ns-lib.tcl.

```
grayholeAODV {
                              set    ragent    [$self
create-grayholeaodv-agent $node]
                    }
```

For creating grayholeaodv agent add the following code in ns-lib.tcl.

```
Simulator  instproc  create-grayholeaodv-agent  {
node } {
     # Create grayholeAODV routing agent
          set  ragent  [new  Agent/grayholeAODV
[$node node-addr]]
     $self  at  0.0  "$ragent  start"        ;#  start
BEACON/HELLO Messages
     $node set ragent_ $ragent
     return $ragent
}
```

Add graholeaodv protocol in make file by adding code given below.

```
grayholeaodv/grayholeaodv_logs.o
grayholeaodv/grayholeaodv.o                         \
grayholeaodv/grayholeaodv_rtable.o
grayholeaodv/grayholeaodv_rqueue.o \
```

Similarly for adding IDSaodv protocol the same changes have to be done as we did for grayholeaodv protocol.e have to add idsaodv protocol in ns-lib.tcl and make file.
Now for creating traffic and movement the commands aregiven below
For generating traffic also known as scen file the command is

```
./setdest -v 1 -n 20 -p 2.0 -s 10.0 -t 200 -x 500 -y
500 >scen-20-test
and the output will be written in a file called scen-
20-test.
```

For generating movement also known as cbr file the command is

```
./ns cbrgen.tcl -type cbr -nn 20 -seed 1 -mc 20 -rate
1 >c20
```

Then make a tcl script aodv.tcl .For seeing the effect of aodv routing protocol, write AODV in adhoRrouting in aodv.tcl script. In the same way for taking the reading of grayhole attack write grayholeAODV in adhocRouting and for ids write idsAODV in ahdocRouting in aodv.tcl.

Simulation

We use NS-2 (v-2.34), a network simulation tool to simulate wireless and wired communication network. NS2 is discrete event simulator developed by the University of California in Berkeley. It provides a good platform for MANET simulation. We simulate our model for 15, 25 and 35 nodes. The random waypoint model is selected as a mobility model in a rectangular field (500 x 500 m2). RP-AODV is used for simulation at network layer. Nodes send constant bit rate (CBR) traffic at varying rates. We have repeated the experiments by changing the number of node 15, 25 and 35 to see the performance of network under attacks.

The simulation parameters are given in Table I

Parameter	**Definition**
Protocol	Aodv, Grayholeaodv, idsaodv
MAC layer	IEEE 802.11
Simulation duration	100s
Pause time	5s
Node placement	Random
Simulation area	500m x 500m
Traffic sources	CBR
Number of nodes	15, 25,35
Version NS-2	2.34

Performance Metrics

Some important performance metrics can be evaluated:-

 Packet delivery fraction — The ratio of the data packets delivered to the destinations to those generated by the CBR sources.

 Throughput — The ratio of the number of data packets sent and the number of data packets received.

VIII. RESULT

Following are the results, calculated by using performance.awk script. Using the output we plotted the bar graphs of following parameters .The result is carried out by NS-2Simulator using following Parameters.

- Sending Packet
- Received Packet
- Packet Delivery Ratio
- Throughput
- Dropped Packets
- Dropped Bytes

A. *Sending packet*:-Number of packets send form source to the destination.

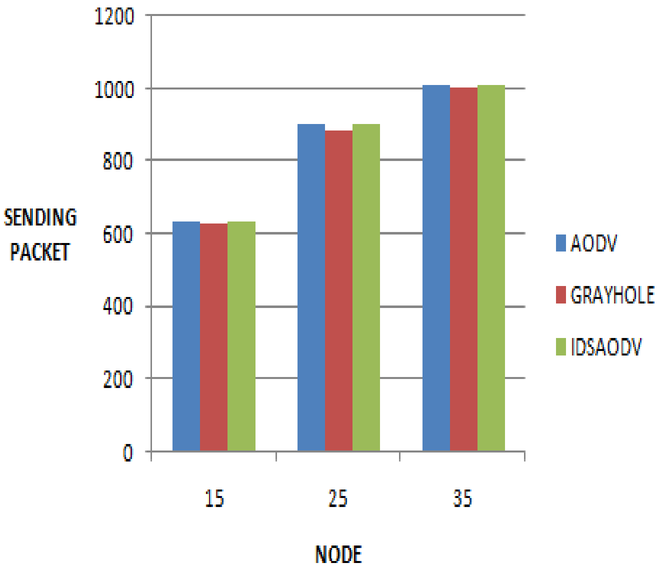


Figure 8(a): Sending packets values for different nodes.

B. *Received packet*:- Number of packets received by destination.

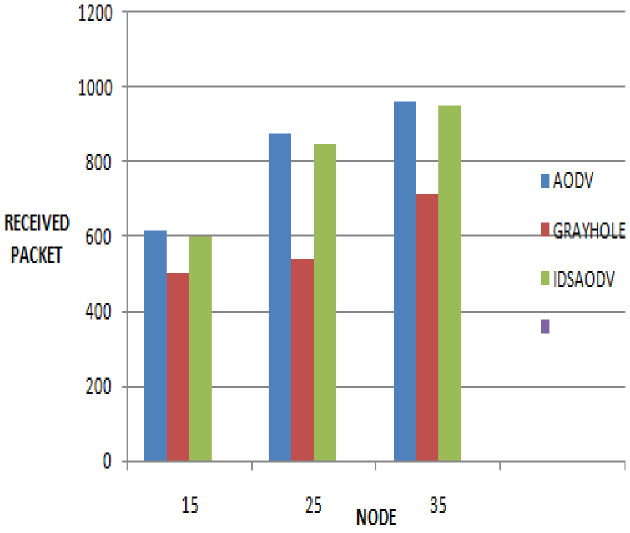


Figure 8(b): Received packets values for different nodes.

C. *Packet Delivery Ratio*: - It is the ratio of the number of data packets received by the CBR sink at the final destinations to the number of data packets originated by the "application layer" at the CBR sources.

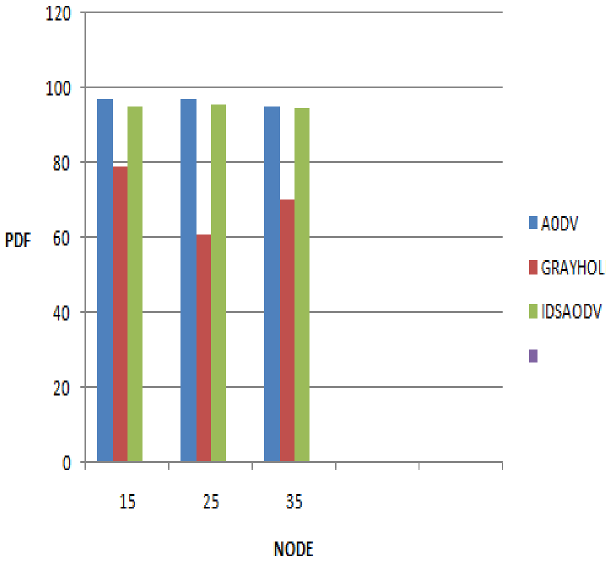


Figure 8(c): PDF values for different nodes.

D. *Throughput*:- It is one of the dimensional parameters of the network which gives the fraction of the channel capacity used for useful transmission selects a destination at the beginning of the simulation i.e., information whether or not data packets correctly delivered to the destinations.

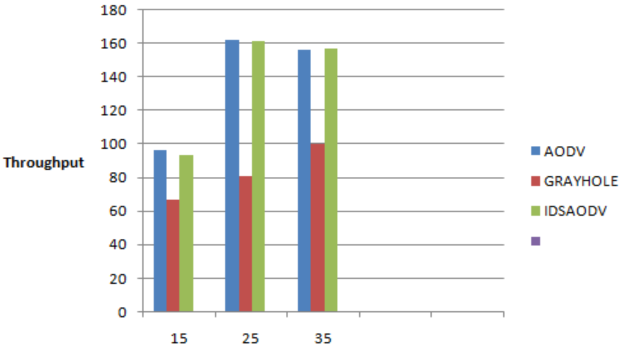


Figure8(d): Throughput values for different nodes.

E. *Dropped packets*: - Number of packets dropped by the grayhole node. The graph shows the comparison between the reading of aodv, grayhole, and IDS.

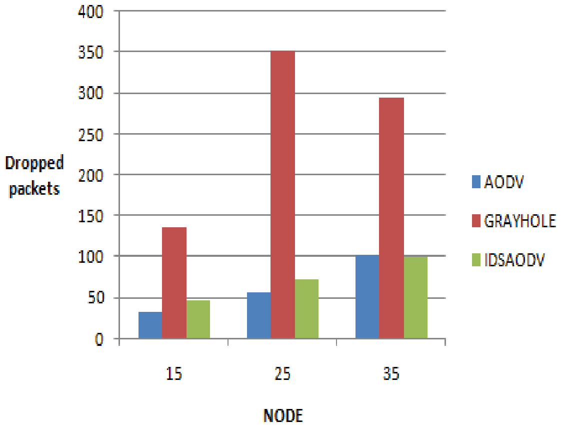


Figure 8(e): Dropped packets values for different nodes.

F. *Dropped bytes*:- Number of bytes dropped by the grayhole nodes. And the graph shows improvement by applying IDS technique.

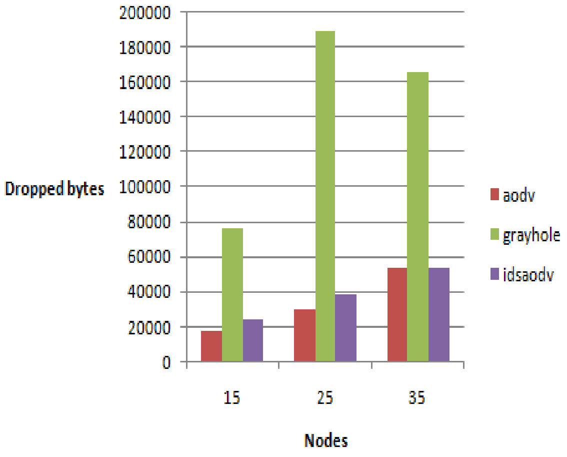


Figure 8(f): Dropped bytes values for different nodes.

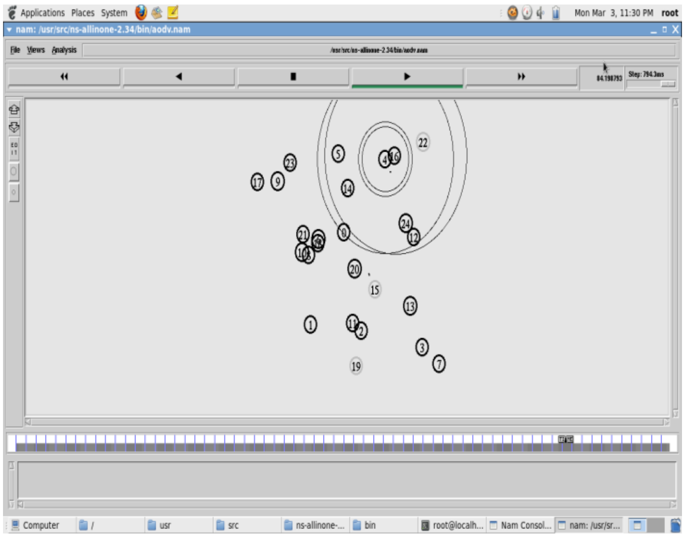


Figure 8(g): Simulation Of GrayHole Attack in Network Animator

VIII. CONCLUSION

Grayhole attacks are the most important security problems in MANET. Detection of gray hole is more difficult than black hole, because the attacker works as normal node then starts dropping of data. In this paper, we introduced some of the comparison between readings of aodv, grayhole, and idsaodv. And we can see that when grayhole node is introduced, performance decreases, and after applying IDS technique performance get improved than grayhole. For comparision we have taken throughput, sending packet, receiving packet, PDF, dropped packet, dropped bytes etc as parameters metrics.

IX. FUTURE WORK

In this paper we have measured the effect of grayhole attack and try to improve performance by using IDS technique by comparing different parameters. The same scenario can also be applied for more than one grayhole node that means for multiple grayhole. In this paper we have used AODV protocol the same work can b done for different protocol like DSR, etc.

REFERENCES

[1] "Methods of Preventing and Detecting Black/Gray Hole Attacks on AODV-based MANET" Marjan Kuchaki Rafsanjani Department of Computer Science, Shahid Bahonar University of Kerman, Kerman, Iran IJCA Special Issue on "Network Security and Cryptography" NSC, 2011

[2] "Grayhole Attack and Prevention in Mobile Adhoc Network" Megha Arya SATI (vidisha) SATI Sagar Road Vidisha M.P ,India. International Journal of Computer Applications (0975 – 8887) Volume 27– No.10, August 2011.

[3] "Comparing the impact of Black Hole and Gray Hole Attacks in Mobile Adhoc Networks", Usha and Bose Department of Computer Science and Engineering, Faculty of Information and Communication Engineering, Anna University, Chennai, 600 025, India Journal of Computer Science 2012, 8 (11), 1788-1802

[4] "A Efficient Way To Minimize the Impact of Gray Hole Attack in Adhoc Network" Mr.Chetan S.Dhamande1, Prof H.R.Deshmukh2

1ME Scholar, CSE (First Year), B.N.C.O.E, Pusad (MS) INDIA
2Associate Professor, Dept of CSE, B.N.C.O.E,Pusad (MS) INDIA.

[5] "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei Department of Computer Science and Engineering Florida Atlantic University WIRELESS/MOBILE NETWORK SECURITY Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. – - – °c 2006 Springer.

[6] "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad- Hoc Networks", Sukla Banerjee, Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[7] "A Literature Survey of Black Hole Attack on AODV Routing Protocol**"** Chandni Garg1, Preeti Sharma2, Prashant Rewagad3 International Journal of advancement in electronics and computer engineering (IJAECE) Volume 1, Issue 6, Sep 2012.

[8] "Advanced Algorithm for Detection and Prevention of Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks"**,** Shalini Jain, ©2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 7.

[9] "Detection and Removal of Cooperative Black/Gray hole attack in Mobile ADHOC Networks", Amos J Paul, ©2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 22.

[10] "Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol" Onkar V.Chandure International Journal of Computer Applications (0975 – 8887) Volume 41– No.5, March 2012.

[11] "Multiple Black Hole Node Attack Detection Scheme in MANET by Modifying AODV Protocol" Nishu kalia, Kundan Munjal, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-3, February 2013.

[12] Marti, S., Giuli, T. J., Lai, K., and Baker, M. 2000. "Mitigating routing misbehavior in mobile ad hoc networks", In Proceedings of the 6th Annual International Conference on MOBICOM, Boston, Massachusetts, United States, 255-265.

[13] Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., and Nemoto, Y. 2007. "Detecting black hole attack on aodv-based mobile adhoc networks by dynamic learning method". J. Network Security. Vol. 5, No. 3 (Nov. 2007), 338–346.