Journal of Computer Science 2012, 8 (11), 1788-1802
ISSN 1549-3636
© 2012 Science Publications
doi:10.3844/jcssp.2012.1788.1802 Published Online 8 (11) 2012 (http://www.thescipub.com/jcs.toc)

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

Received 2012-07-21, Revised 2012-08-29; Accepted 2012-09-05

ABSTRACT

Mobile Adhoc Networks (MANETs) are dynamic in nature. Any nodes can join and leave the network at any time. Hence any type of intruders can attack the communication at any time, especially the routing mechanism between the nodes. In this study, we study and understand two types of attacks which cause more damage to the routing performance of MANET; the attacks are Black Hole attacks and Gray Hole attacks and compare the impact of these attacks on MANET. "Send Fake Route Reply to the nodes" type of attack is used to understand the behavior of these two types of attacks. Existing AODV protocol is modified in order to study these types of attacks in MANET. Performance evaluation of the proposed method is carried out using NS-2. In the presence of these attacks the network performance degrades for various network attributes. The performance of MANET under attack is thoroughly investigated, by applying it on various network parameters with various node densities. Not only had that which attack causes more damage to the environment also studied.

Keywords: Mobile Adhoc Networks (MANETS), Black Hole Attacks, Gray Hole Attacks, AODV, Security, Hop Count, Sequence Number

1. INTRODUCTION

Mobile adhoc networks are self deployable i.e., each node in MANET acts as a router and allows other users to communicate through their mobile devices. Any user can communicate with other user within a particular range. So the nodes move arbitrarily, hence node topology of these network changes frequently which causes frequent disconnection in their communication. Unlike the cellular networks which rely on infrastructure, MANETs does not require any expensive base station. These MANETs can be used in situations such as tsunami, earthquake and military communications and so on. Mobile adhoc networks support portability and mobility but are vulnerable to various types of security attacks **Fig. 1.** Security is an important issue for these applications.

MANETs suffer for various security problems. Improving the security of the mobile adhoc network is still a research issue. MANETs suffer from various kinds of attacks in its protocol stack. For e.g., MAC layer (Marti *et al.*, 2000) suffers from jamming attacks, routing layer suffers from worm hole attacks and so on. Most of research work has been done on improving the security of MANETs (Hu *et al.*, 2002). MANETs are highly vulnerable because nodes can be eavesdropped due to the infrastructure less networks.

Hence security in MANET is challenging issue. The intruders can violate the routing protocols and exploit it. Routing protocols (Royer and Chai-Keong, 1999) in MANET are classified into various types. They are unicast routing protocols, multicast routing protocols, secure routing protocols, network layer routing protocols. Network layer routing protocols are further classified into various types. Wireless Routing Protocols (WRP), Fisheye Routing Protocols (FSR), Adhoc On demand Distance Vector (AODV), Dynamic Source Routing (DSR), Zone Routing Protocol (ZRP) and so on. Routes in MANET are multi-hop relaying and the radio waves propagate up to 250 meters of wireless radios. Nodes in MANET are free to move or remain stand still because of their adhoc nature. So the connection between any nodes may lose at any time. Routing protocols are responsible for maintaining routes and establishes connection between nodes.

Corresponding Author: Usha, Department of Computer Science and Engineering, Faculty of Information and Communication Engineering, Anna University, Chennai, 600 025, India

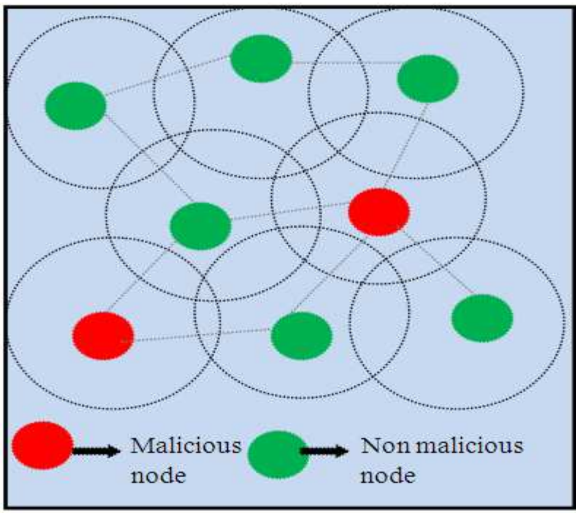


Fig. 1. MANET Environment with normal and malicious node

The challenging task of routing protocol is to deliver routing messages efficiently from source to destination. Even though many protocols involved in this delivery process, every protocol has their own methodology to route data between nodes. In the absence of dedicated routers, providing security is more challenging in MANET than wired networks.

Existing routing protocols like AODV, DSR failed to provide security mechanisms. In a MANET, packet delivery is achieved through two operations-routing packets and forwarding packets. Hence as a result, vulnerable behavior can be achieved by malicious nodes in both the operation.

In this study, we discuss how a malicious node exploits AODV protocol and yields attacks in routing and forwarding packets. There has been lot of simulation work done in literature to study the behavior of routing protocols. In our work we have elaborately discussed about the impact of the black hole attack and gray hole attack and compared the vulnerability of black hole attack and gray hole attack. If one wants to secure MANET against these kinds of attack, they should understand the behavior of these attacks. In order to achieve this, we explored and compared the behavior of these two attacks in detail.

Our methodology is to study about Black Hole and Gray Hole attacks and compare which attack causes more damage to routing behavior. The goal (Ning and Sun, 2005; Aad *et al*., 2008; Nguyen and Nguyen, 2008) of black hole nodes is to increase the overhead of all traversing nodes in the communication path and results in low packet delivery ratio. Gray hole attack (Jaydip *et al*., 2008; Davide *et al*., 2008; Panagiotis and Haas, 2002; Liu and Kaiser, 2003; Gao and Wei, 2007; Sen *et al*., 2007) the attacker node initially forwards the packets and participates in routing. The Gray Hole node advertises itself as having a valid or shortest path to the destination node initially. But later, it disobeys to protocol rules. We have preferred AODV protocol because it is widely used and it is vulnerable to these attacks because of the methods it employs. We have made our simulations using Network Simulator 2 (NS-2).

2. MATERIALS AND METHODS

AODV (Perkins *et al*., 2003) is source initiated a routing protocol. AODV protocols are different from traditional proactive protocols since in proactive the routing mechanism is based on periodic updates this leads to high routing overhead. The key goal in designing this protocol is to reduce overhead. Routing messages in AODV can be divided into path discovery and path maintenance messages. Path discovery includes the Route Request (RREQ) **Fig. 2** and a Route Reply (RREP) **Fig. 3**, while the latter includes Route Error (RERR) and Hello message. As shown in **Fig. 2** the RREQ message contains broadcast id; destination IP address; destination sequence number; source IP address; source sequence number; hop count. Likewise in **Fig. 3**, RREP packet also contains the destination IP address; destination sequence number; originator sequence number; RREQ ID; These information's of RREQ and RREP message headers are used when the node participates in routing.

In AODV no routing structure is created prior. The route discovery process of AODV consists of two key methods. First one it is source routing. Second one is backward learning. Since this protocol uses the concept of periodic updates it is adapted to network dynamics. Source initiated means source floods the network with a route request packet when a route is required for a destination. The flooding is propagated outwards from the source. The flooding transmits the request only once. On receiving the request from the source node the destination replies to the request if it has the valid path. Reply from destination uses reversed the path of the route request. Since the route reply is forwarded via the reverse path which forms a forward path. Thus it uses forward paths to route data packets. AODV protocol uses hop-by-hop routing. That is each node forwards the request only once. In the meanwhile unused paths expire based on timer. AODV uses the concept of optimization that is any intermediate nodes can reply to route request if it has valid path which makes the protocol to work faster. But the major problem with optimization causes loops in the presence of link failure. Each node maintains sequence number. It acts as a timestamp. The most interesting feature of the sequence number is, it signifies the freshness of the route. When a node maintains highest sequence number, makes it up to date in the routing.

Type count	R	A	Reserved	Hop
Destination IP Address				
Destination sequence number				
Originator IP address				
Life time				

Fig. 2. RREQ Packet Format

Type	J	R	G	D	U	Reserved	Hop
RREQ ID							
Destination IP address							
Destination sequence number							
Originator IP Address							
Originator sequence Number							

Fig. 3. RREP Packet Format

Whenever a source node wants to communicate, it broadcasts a Route Request (RREQ) message for the specified destination. Intermediate nodes forwards (i.e., broadcasts) message towards the destination. For example in following **Fig. 4** the source node S floods the RREQ (Route request) in the network. Each node in the network checks its own routing table and checks whether it is the destination or it has a route to the destination. Simultaneously reverse path is set up along the way which it forwards the packets. If it is not the destination node the nodes forward the packets. In above **Fig. 4** node A is not destination node, so node A again broadcasts the packets in the network.

Now we explain about malicious behavior using RREP packet. Node A in **Fig. 4** which is a malicious node can forge a RREP message to the source node S. When source node S receives faked RREP message from node A, it updates its route to the destination node through attacking (non-existent) node. When node A receives the data packets it drops the packets.

Node A in **Fig. 4** which is a malicious node, can forge a RREP message in following mechanisms:

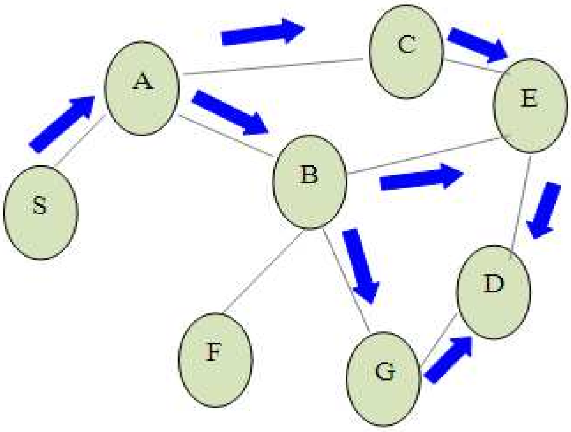


Fig. 4. AODV route discovery using RREP Packet

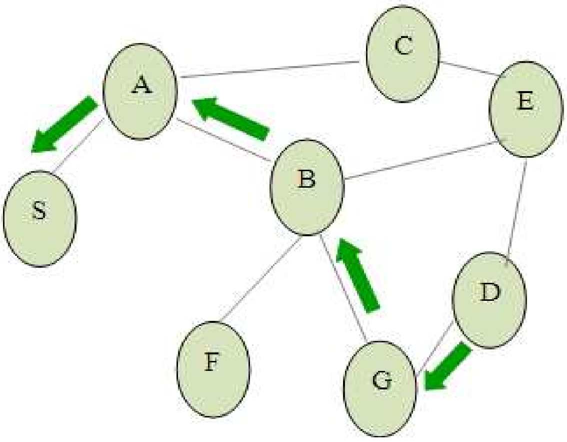


Fig. 5. AODV route discovery using RREP Packet

- Set the hop count field to 1
- Increasing the destination sequence number by at least one
- Set the source IP address to a non existing IP address
- Unicasting the faked RREP message to the source node, when source node receives the faked RREP message, it updates its route to destination node through attacking (non-existence) node

Due to the invasion of Node A which is a malicious node, sends the faked RREP message to node S. Node S will update node A as the next hop to node D. Now node A has successfully become a part of the route from node S to node D. Hence node a does all the vulnerable behavior in the network and it doesn't allow to forward the packets further or it simply drops the packets and so on. Finally when the node D receives the broadcasted message it confirms that it is the destination node and uses the reverse route to reply node D. The simple idea behind this routing is flooding done with nodes in the network. Not only that each node forwards the request only once. Each node in the communication path maintains a sequence number which also act as a timestamp. The timestamp gets incremented whenever it starts sending any message or participates in the communication. Each route from source S also has S's sequence number associated with it. Sequence number signifies the freshness of the route. The node which has highest sequence number specifies up-to-date information about routing. Intermediate node reply only when it has the highest sequence number instead of forwarding the message. The following **Fig. 5** illustrates this Route Reply (RREP) concept in detail. When the RREQ packet reaches node G which has routes to node D, node G verifies that the destination sequence number is less than or equal to the destination sequence number it has recorded for node D. Node E may forward the RREQ packet, but the receiver node D recognizes that packet as duplicates; hence it won't use that path via node E for communicating further. When node D receives a RREQ packet and it confirms that it has a current route to the target source S using routing table. After this process the node D unicasts a Route Reply (RREP) packet to the reverse path which it received the RREQ packet early? The unused path expires based on the timer. Thus the destination node D starts forwarding and receiving packets with source node S using the reverse path in the networks.

2.1. Black Hole Attack in Detail

As we have discussed above, when a node requires a route to a destination, it initiates a route discovery process within the network. In our simulation we considered the case in which the intruder sends fake RREP packets. In AODV after receiving a RREQ message, an inside attacker may forge a RREP message as if it had a fresh enough route to the destination node.

In order to suppress other legitimate RREP messages that the source node receives from other nodes, the attacker forges a faked RREP message by increasing the destination sequence number.

An attacker may disrupt the route between the victim nodes to a given destination, or invade in the route between by suppressing other alternative routes. These kinds of nodes are known as Black Hole nodes. After receiving a RREQ message from nodes, an inside attacker may forge a RREP message as if it had a fresh enough route to the destination node. In order to suppress other legitimate RREP messages that the source node may receive from other nodes, the attacker may forge a faked RREP message by increasing the destination sequence number.

2.2. Gray Hole Attack in Detail

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.

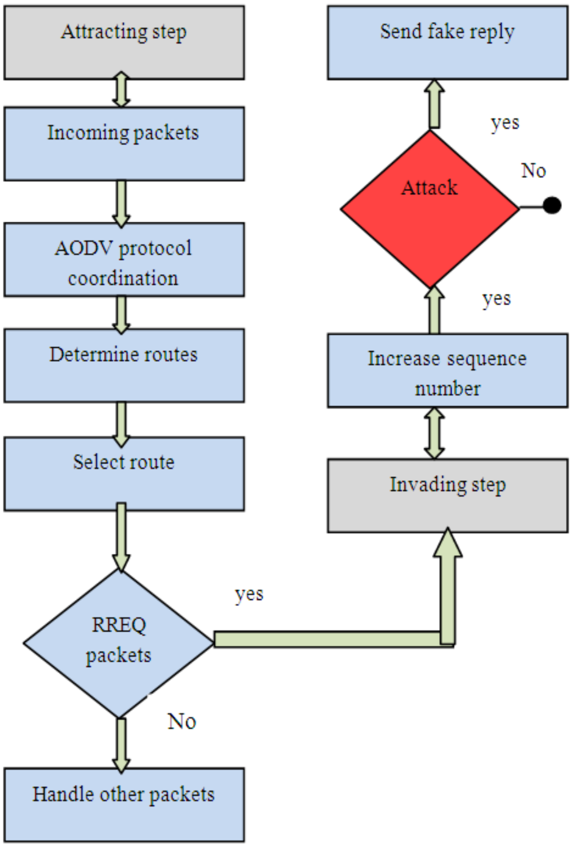


Fig. 6. Simple framework for attack generation

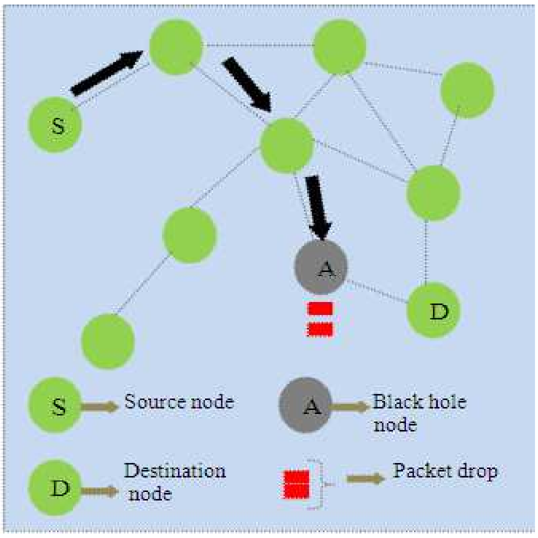


Fig. 7. Example of Black Hole attacks by Fake RREP

2.3. Proposed Framework for Black/Gray Hole Attack

Black hole and Gray hole attack involves in dropping packets. Black hole attack drops all received packets intended for forwarding, whereas gray hole attack drops packets at certain frequencies. Both the attacks consist of two steps: (1) Attracting step-where the nodes attract other nodes by falsely sending information in the communication (2) Invading step-where the node invades the communication process and drops packets. The simple framework of these attacks is over AODV protocol is shown in **Fig. 6.**

During the attackers step, the attacker has to identify whether the incoming packets are AODV packets .Then the attacker determines the route and selects the routing process by sending RREQ packets. First, the attacker coordinates in routing by sending RREQ packets. During Invading step, the attacker starts increasing its sequence number and advertises itself that it has the highest sequence number compared to other nodes in the network. Thus it induces attack by sending a fake reply to the nodes in the network.

2.4. Simulation Environment

In order to simulate both the attacks we have modified the AODV protocol in NS-2 (Issariyakul and Hossain, 2008). In following **Fig. 7** illustrates a modification done in existing AODV protocol to create INVADEAODV protocol which creates attacks. The following two functions are the most important functions in which a Black Hole or Gray Hole vulnerability can be introduced:

$$\text{AODV} :: \text{recv}\left(\text{Packet } *\text{p, Handler}*\right)$$

$$\text{AODV} :: \text{recvRequest}\left(\text{Packet } *\text{p}\right)$$

Now we discuss how the attack can be happened by using the above functions in NS-2. **Figure 8** discusses about the pseudo code which we implemented. In NS-2, the function “AODV:: recv” will be called for each and every packet arriving at that routing agent. If the packet is an AODV packet, it will be treated accordingly. So, in this function, a routing agent can maliciously drop a packet during certain kind of attacks. The function “AODV:: recvRequest” will be called during receiving an AODV route request packet type “AODVTYPE_RREQ”. On receiving this route request message from any neighboring nodes, the routing agent may try to resolve the route and send a route reply message if a route is available. So, it will call the function “AODV:: send Reply” with appropriate parameters. Hence, an agent will try to send a fake reply for the purpose of attacking a neighboring node by giving wrong routing information; it calls “AODV:: send Reply” and passes wrong routing information to the requesting node. In our implementation, we have used a modified function “AODV:: sendFakeReply” for the purpose of sending wrong information to simulate both attacks.

2.5. Simulation Model

All the simulation and analysis were made on an Intel Core 2 Duo PC with 2 GB RAM. We have used a simulation model based on NS2 in our evaluation. Our evaluations are based on the simulation of 60 wireless mobile nodes that forms a mobile adhoc network over a rectangular (600×600 m). The MAC layer protocol used in the simulation is IEEE 802.11.We randomly selects 0-40% of nodes as malicious nodes. We have varied the network densities from 20, 30, 40, 50 and 60%. **Table 1-3** lists the parameter settings for a simulation environment.

Hypothetical networks were constructed for the simulation purpose and then the simulation was repeated with different parameters. During each run the trace files were saved and finally, the trace analysis was done to measure the performance.

As shown in **Table 1** we have placed nodes randomly within 600m×600m area. We have generated various node mobility scenarios. We setup 1 Mbps IEEE 802.11 protocol at the MAC layer, AODV protocol at the network layer with the random way point model at the physical layer. We vary the percentage of node density, percentage of malicious nodes in the network. CBR agents are used to simulate normal and attack traffic. Four different factors were used to understand these two attacks in Manet (packet delivery ratio, normalized routing load, overhead, routing packets). We have used the Random Waypoint Model (RWP) for each node. In this model, each node selects a random destination within the simulation area and a node moves to this destination with a random velocity, where the speed of a node was randomly chosen from 0 m/s to 10 m/s.

2.6. Traffic and Mobility Model

The trace we used was Constant Bit Rate (CBR). Each node transmits 512 byte of data packets at certain rate (packets/sec). The transport agent we used was UDP.For each set of parameters, we have repeated the simulation for 3 times and calculated the average of the results. For the simulation of normal AODV with 5 different numbers of network sizes and for three repetitions, we run the simulation for 15 times. So for 5 different numbers of network size with black hole attack and 4 different numbers of nodes (malicious), the black hole simulation was run for 40 times. And it was repeated for 3 times and makes it as 120 runs. So the results were then prepared from the output of 135 simulation runs. We have used different network scenarios (20, 30, 40, 50 and 60 Nodes). The scenario generator available in ns2 which is used for generating 5×3 scenarios (for three repetitions). Next we discuss about simulation results and analysis method.

3. RESULTS

In order to clearly analyze and understand the attacks we have implemented the following techniques:

- T1-Analysing normal AODV under various network factors as above
- T2-Analysing Black Hole AODV under same network factors
- T3-Analysing Gray Hole AODV under same network factors
- T4-Comparision of Black Hole AODV and Gray Hole AODV attacks.

3.1. Performance Metrics

3.2. Packet Delivery Fraction

It is the ratio of CBR data packets received by all destinations (sinks) over the total number of packets sent by all the sources within the simulation time.

3.4. Normalized Routing Load

The normalized routing load is known as the ratio between control packets sent to that of receiving data packets.

3.5. Total Dropped Packets

We count all the packets dropped due to any reason as a performance metric.

3.6. Overhead

The overhead is measured in terms of total generated routing packets. It is the count of total packet generated and forward at the network layer.

3.7. Performance Analysis for Normal AODV

In **Table 4** it shows the performance of normal AODV. In Technique1 (T1), we have done our experiments without any attacking nodes with varying node densities and the results are displayed in a table with various network factors. The **Table 4** discusses about Technique-1.

In Technique (T2),we have done our experiments with Black Hole nodes with varying the node densities as in T1.For varying number of Black Hole nodes we analyze the performance using the same network factors. In **Table 5** we can observe the detail list of network factors for analyzing Black Hole attacks. In Technique (T3), we have done our experiments with Gray Hole nodes with varying the node densities as in T1. For varying number of Gray Hole nodes we have analyzed the performance using the same network factors. In **Table 6** we can observe the detail list of network factors which are used to simulate Gray Hole attacks.

3.8. Packet Delivery Fraction for Black Hole Attack

Packet Delivery ratio is a standard measure of throughput. We present packet delivery ratio for normal AODV and AODV with black hole attack. In general without malicious node AODV have got good packet delivery ratio the results are presented for AODV in the absence of malicious node and in the presence of malicious nodes are shown in **Fig. 9** subject to the constraints of prediction accuracy. From the results in **Fig. 9** the following observations can be drawn:

- Packet delivery ratio decreases with increasing node densities and percentage of black hole nodes
- In the case of black hole AODV, with 10% of malicious nodes, the packet delivery ratio decreases from 97.60% (0% malicious nodes) to 67.73%,(10%malicious)when the nodes are moving with the mobility of 10m/s
- With 40% of malicious nodes, the packet delivery ratio has the fall from 97.60 to 39.17%
- We observes that when the black hole nodes are increased the packet delivery ratio gets decreased

3.9. Normalized Routing Load for Black Hole Attack

Normalized Routing load can be evaluated based on messages like RREQ and RREP with the statistics of number of routed packets to that of received packets. **Fig. 10** explains about normalized routing load in the presence and absence of malicious nodes.

From the results in **Fig. 10** the following observations can be drawn:

- No constant trend is observed in normalized routing load
- In the case of black hole AODV, the normalized routing load shows an increase
- With 10% of malicious nodes the normalized routing load increases from 0.38 to 1.75, likewise with 40% of malicious nodes, the normalized routing load shows the increase from 0.38 to 2.26

We also observe that when the black hole nodes are increased the normalized routing load also increased

3.10. Dropped Packets for Black Hole Attack

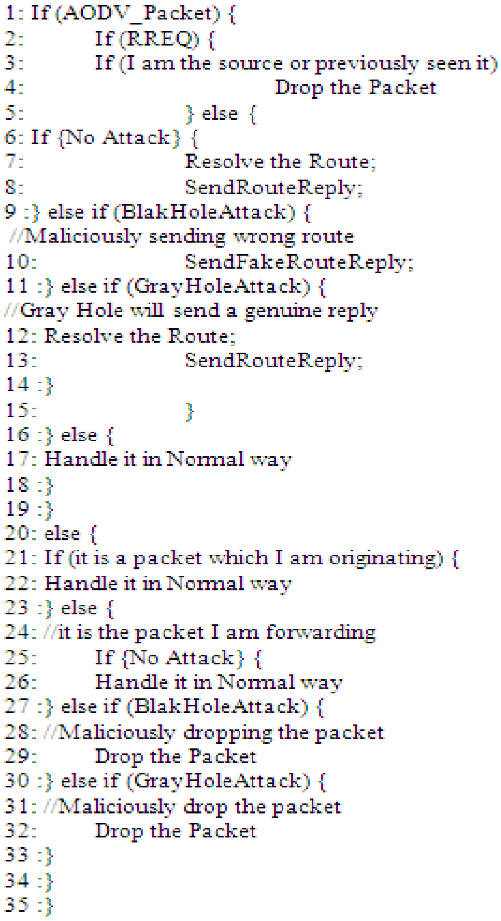
This metric not identifies other reasons for packet loss, but it is useful towards detecting packet drop attacks. From the results in **Fig. 11** the following observations can be drawn:

- Packet drop count increases with increasing node densities and percentage of black hole nodes
- In the case of black hole AODV, with 10% of malicious nodes, the packet drop count increases from 73 (0% malicious nodes) to 413 (10%malicious)when the nodes are moving with the mobility of 10m/s
- With 40% of malicious nodes, the packet drop count has the steepest fall from 73 to 1052
- We observe that when the black hole nodes are increased the packet drop count gets increased

3.11. Overhead for Black Hole Attacks

Overhead is the useful metric for analyzing extra bandwidth consumed to deliver data packets. From the results in **Fig. 12** the following observations can be drawn:

- Overhead increases with increasing node densities and percentage of black hole nodes
- In the case of black hole AODV, with 20% of malicious nodes, the overhead increases
- With 40% of malicious nodes, the overhead increases from 2399.00 to 1338.67
- We observe that when the black hole nodes are increased the overhead gets increased



```
If (AODV_Packet) {
        If (RREQ) {
        If (I am the source or previously seen it)
                                Drop the Packet
                } else {
If {No Attack} {
                Resolve the Route;
                SendRouteReply;
} else if (BlakHoleAttack) {
//Maliciously sending wrong route
                SendFakeRouteReply;
} else if (GrayHoleAttack) {
//Gray Hole will send a genuine reply
Resolve the Route;
                SendRouteReply;
}
                }
} else {
Handle it in Normal way
}
}
else {
If (it is a packet which I am originating) {
Handle it in Normal way
} else {
//it is the packet I am forwarding
        If {No Attack} {
        Handle it in Normal way
} else if (BlakHoleAttack) {
//Maliciously dropping the packet
        Drop the Packet
} else if (GrayHoleAttack) {
//Maliciously drop the packet
        Drop the Packet
}
}
}
```

Fig. 8. Pseudo code for simulating black hole and a gray hole attack in AODV

3.12. Performance Analysis for Gray Hole AODV

3.13. Packet Delivery Fraction for Gray Hole Attack

From the results in **Fig. 13** the following observations can be drawn:

- Packet delivery ratio decreases with increasing node densities and percentage of gray hole nodes
- In the case of gray hole AODV, with 10% of malicious nodes, the packet delivery ratio decreases from 97.60% (0% malicious nodes) to 88.57%, (10% malicious) when the nodes are moving with the mobility of 10m/s
- With 40% of malicious nodes, the packet delivery ratio has the fall from 97.60-84.23%
- We observe that when the gray hole nodes are increased the packet delivery ratio gets decreased

Table 1. MANET environment

Property	Value	Description
Channel type	Wireless channel	Channel used
Propagation model	Two ray ground	The radio propagation model used
Antenna type	Omni Antenna	Type of Antenna
Interface queue type	Drop Tail/PriQueue	Queue used
MAC type	802.11	MAC layer protocol used
Maximum packets in queue	50	Packets in Queue
Topological area	600m×600 m	Area of simulation
Mobility scenario	10 m $\sec^{-1}$	Node's mobility
Pause time	20 Sec	Node's pause time at simulation
Mobility model	Random way point	For mobility of nodes

Table 2. Traffic Parameters for simulation

Property	Values
Traffic agent	CBR
Transport agent	UDP
Traffic source	7
Traffic sink	7
CBR rate	10 Kbytes $\sec^{-1}$

Table 3. Variable parameters for simulation

Property	Values
Routing Protocol	Normal AODV, AODV with Black Hole
Number of black holes	1,2,3,4.
Number of nodes	20, 30, 40, 50, 60.

Table 4. Technique-1analysis on normal AODV

Protocol				Routing	
AODV	Nodes	PDF	NRL	packets	Dropped
	20	97.60	0.38	620.33.0	73
	30	97.97	0.61	1008.67	65
	40	98.30	0.65	1079.67	43
	50	98.40	0.73	1206.67	38
	60	96.77	1.46	2399.0	87

Table 5. Technique -2analysing black hole attack

Protocol	Nodes	PDF	NRL	Overhead	Dropped
With black hole 1	20	67.73	0.45	493.33	590
	30	54.13	1.12	938.00	796
	40	67.53	0.91	1003.67	588
	50	65.03	1.18	1323.00	603
	60	79.23	1.75	2355.33	413
With black hole 2	20	44.13	0.72	430.00	983
	30	35.17	1.17	652.00	1125
	40	53.83	1.03	893.67	821
	50	57.87	1.30	1097.00	707
	60	54.00	2.23	1724.33	820
With black hole 3	20	26.87	1.01	445.67	1271
	30	19.93	1.79	596.67	1381
	40	39.50	1.61	731.67	1057
	50	27.07	2.24	839.00	1246
	60	48.60	1.69	1304.67	897
With black hole 4	20	22.53	110.70	350.67	1350
	30	11.73	6.03	563.00	1523
	40	20.13	5.33	764.00	1387
	50	17.00	3.30	933.33	1413
	60	39.17	2.26	1338.67	1052

Table 6. Technique -3Analysing gray hole attack

Protocol	Nodes	PDF	NRL	Overhead	Dropped
With Gray hole 1	20	88.57	00.41	595.00	226
	30	89.10	00.72	1075.00	227
	40	88.13	00.74	1084.67	231
	50	98.40	00.73	1206.67	38
	60	96.77	10.46	2399.00	87
With Gray hole 2	20	84.83	0.40	551.33	283
	30	80.57	0.79	1083.00	373
	40	80.70	0.80	1076.00	355
	50	96.87	0.83	1357.00	67
	60	88.87	1.74	2594.00	227
With Gray hole 3	20	76.80	0.36	465.00	434
	30	78.07	0.80	1070.67	415
	40	81.23	0.69	941.00	329
	50	94.00	0.78	1233.00	113
	60	85.03	1.74	2516.00	291
With Gray hole 4	20	76.70	0.37	474.67	420
	30	74.40	0.81	1011.33	476
	40	76.53	0.71	926.67	409
	50	86.57	0.88	1262.67	236
	60	84.23	1.87	2664.67	303

3.14. Normalized Routing Load for Gray Hole Attack

From the results **Fig. 14** the following observations can be drawn:

- No constant trend is observed in normalized routing load
- In the case of gray hole AODV, the normalized routing load shows an increase
- With 10% of malicious nodes the normalized routing load increases from 0.38 to 0.41, likewise with 40% of malicious nodes, the normalized routing load shows the increase from 0.38 to 1.87
- We also observe that when the gray hole nodes are increased the normalized routing load also increased

3.15. Dropped Packets for Gray Hole Attack

From the results in **Fig. 15** the following observations can be drawn:

- Packet drop count increases with increasing node densities and percentage of gray hole nodes

- In the case of gray hole AODV, with 10% of malicious nodes, the packet drop count increases from 73 (0% malicious nodes) to 595 (10%malicious)when the nodes are moving with the mobility of 10m/s
- With 40% of malicious nodes, the packet drop count has the steepest fall from 73 to 2664.67
- We observe that when the gray hole nodes are increased the packet drop count gets increased

3.15. Overhead for Gray Hole Attacks

From the results in **Fig. 16** the following observations can be drawn:

- Overhead increases with increasing node densities and percentage of gray hole nodes
- In the case of gray hole AODV, with 20% of malicious nodes, the overhead increases
- With 40% of malicious nodes, the overhead increases from 2399.00 to 2664.67
- We observe that when the gray hole nodes are increased the overhead gets increased

Technique 4:

3.16. Comparison on the Impact of Black Hole and Gray Hole on AODV

Now we present the results of the analysis in which we exclusively compare the impact of Black Hole attack with Gray Hole attack on AODV with different network size. As shown in the following **Fig. 17** the packet delivery ratios of nodes in the presence of these two attacks are greatly affected. But if we compare the impact of Black Hole attack with Gray Hole attack, then the packet delivery fraction decreases more than that of Gray Hole attacks.

So, obviously Black Holes and Gray Holes effects network and leads to poor packet delivery in the network.

As Shown in the **Fig. 18**, the normalized routing load gets increases in the presence of Black Hole nodes compared to that of Gray Holes attacks.

And Gray Holes attacks in AODV caused too much packet drops. But if we compare the impact of Black Hole attack with Gray Hole attack, then the black Hole caused much packet drops than the Gray Hole attack.

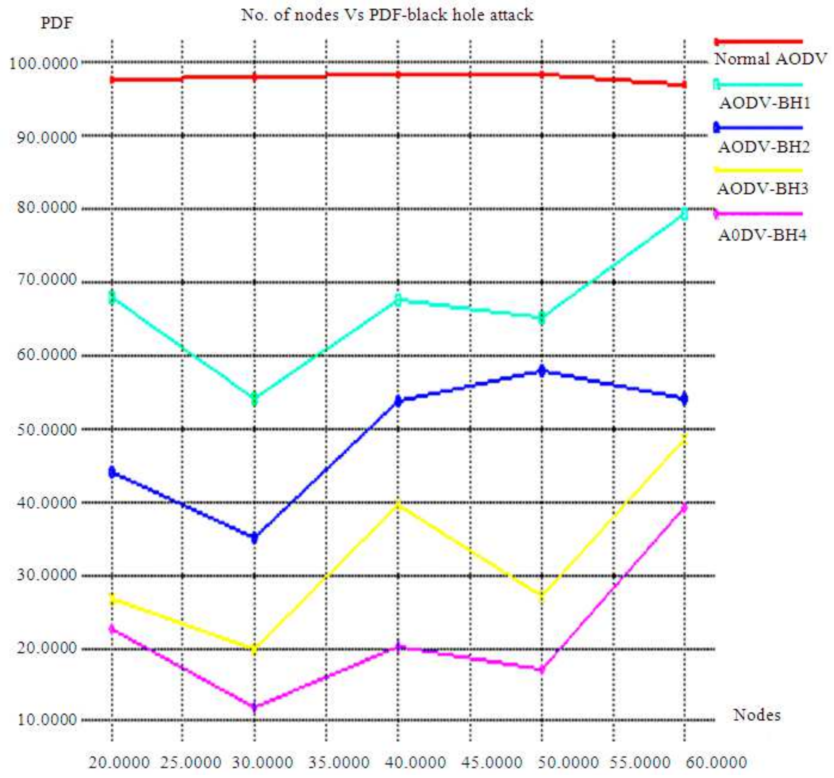


Fig. 9. Number of Nodes Vs. packet delivery fraction

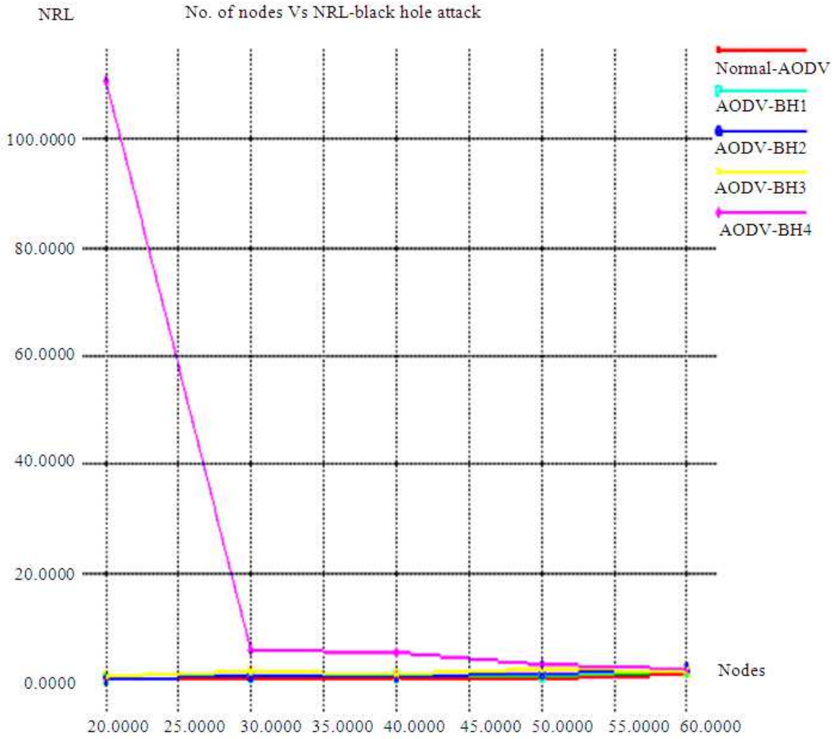


Fig. 10. Number of nodes Vs. normalized routing load

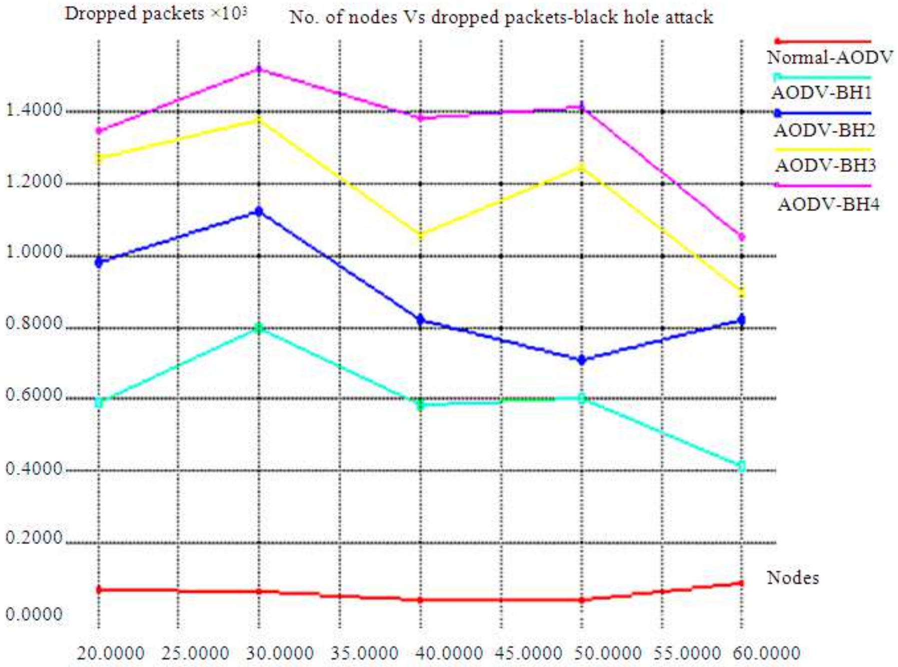


Fig. 11. Number of nodes Vs. dropped packets

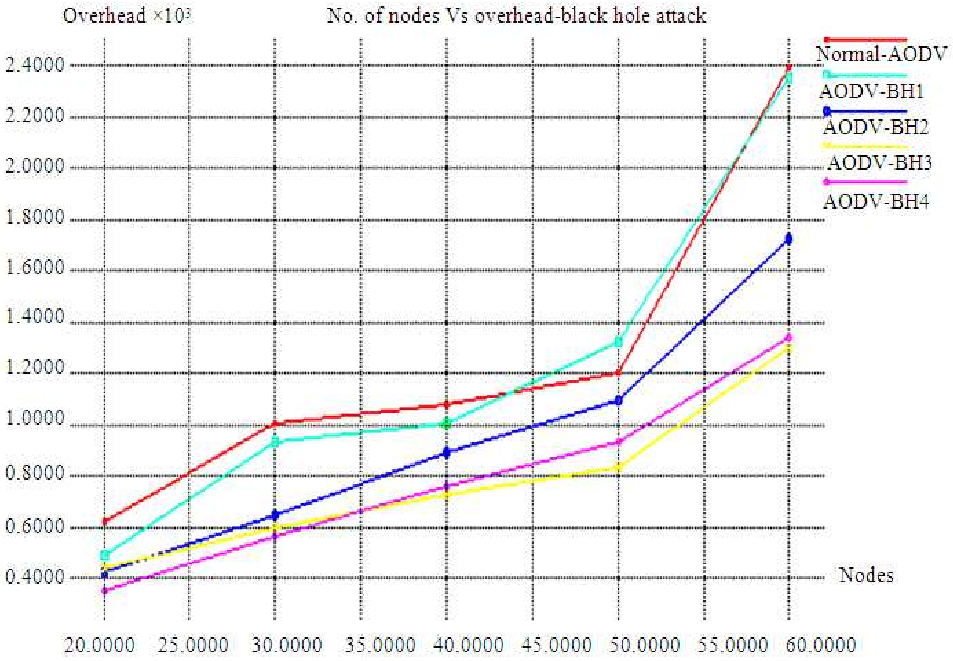


Fig. 12. Number of nodes Vs. overhead

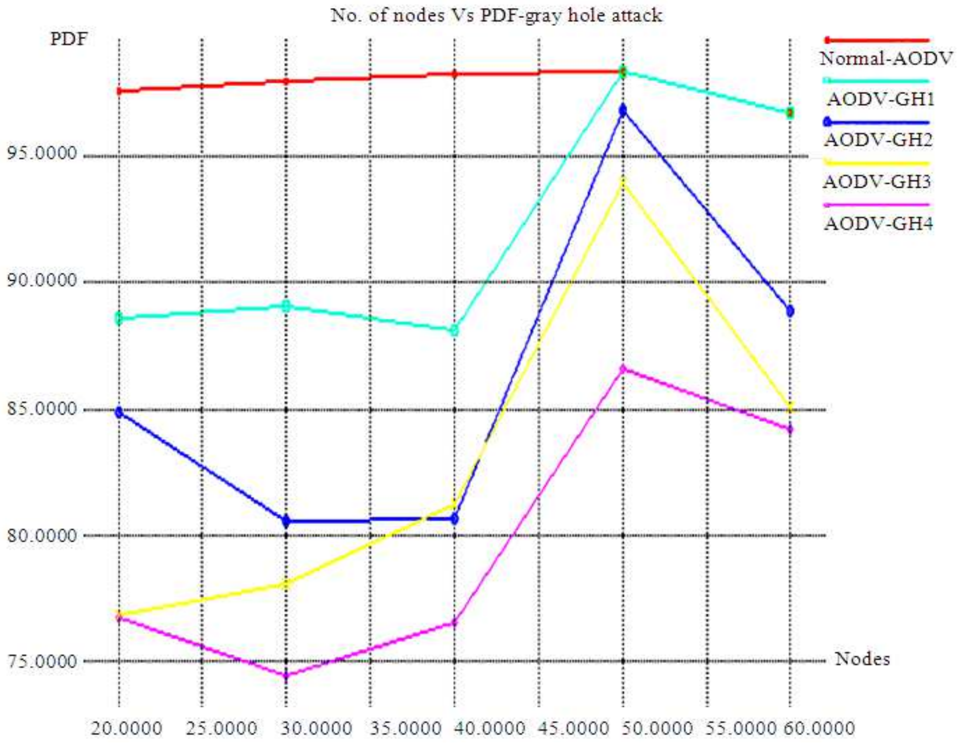


Fig. 13. Number of Nodes vs. Packet delivery fraction

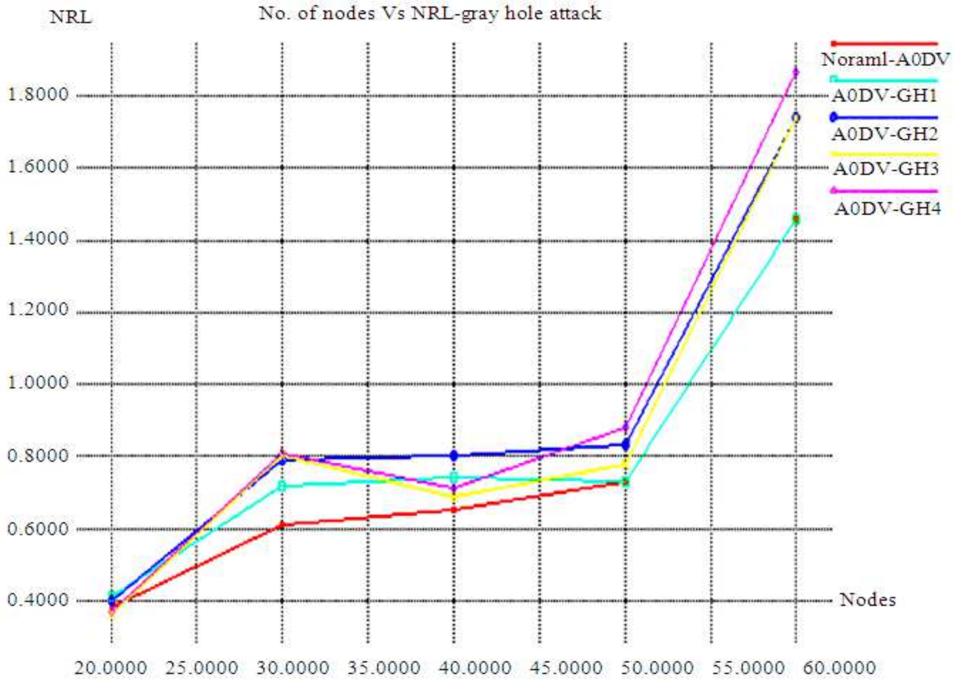


Fig. 14. Number of Nodes Vs. normalized routing load

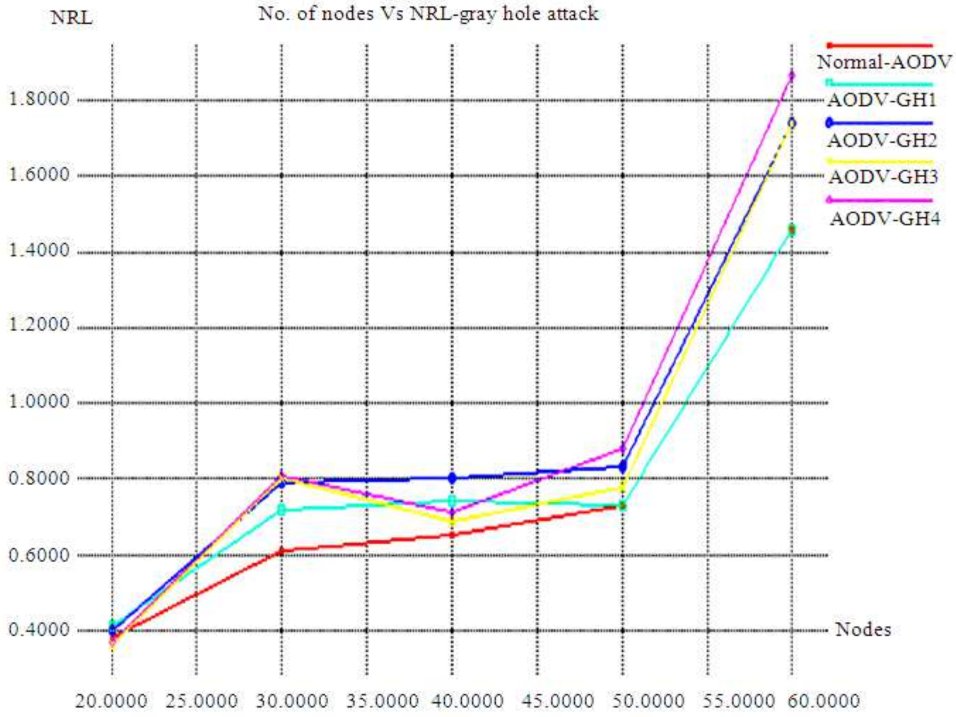


Fig. 15. Number of Nodes Vs. dropped packets

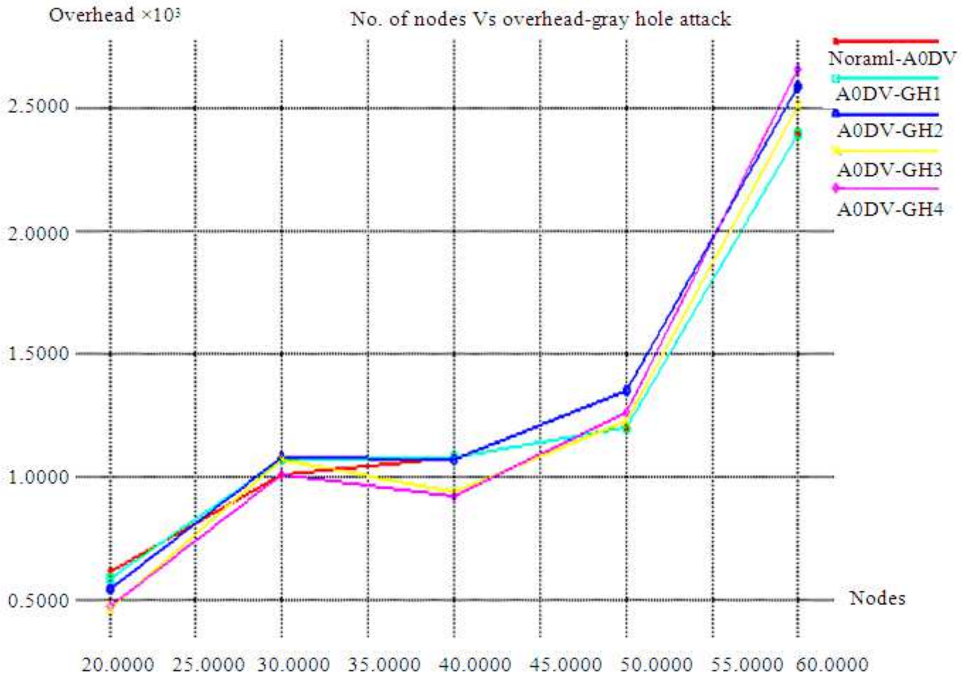


Fig. 16. Number of Nodes vs. Overhead

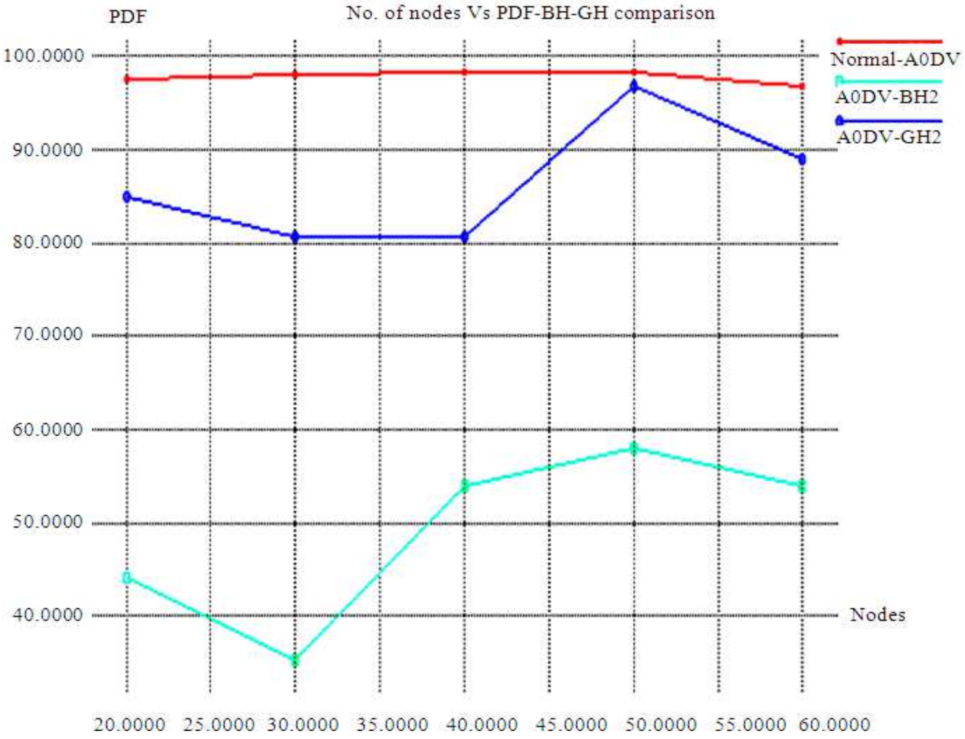


Fig. 17. PDF Comparision graph

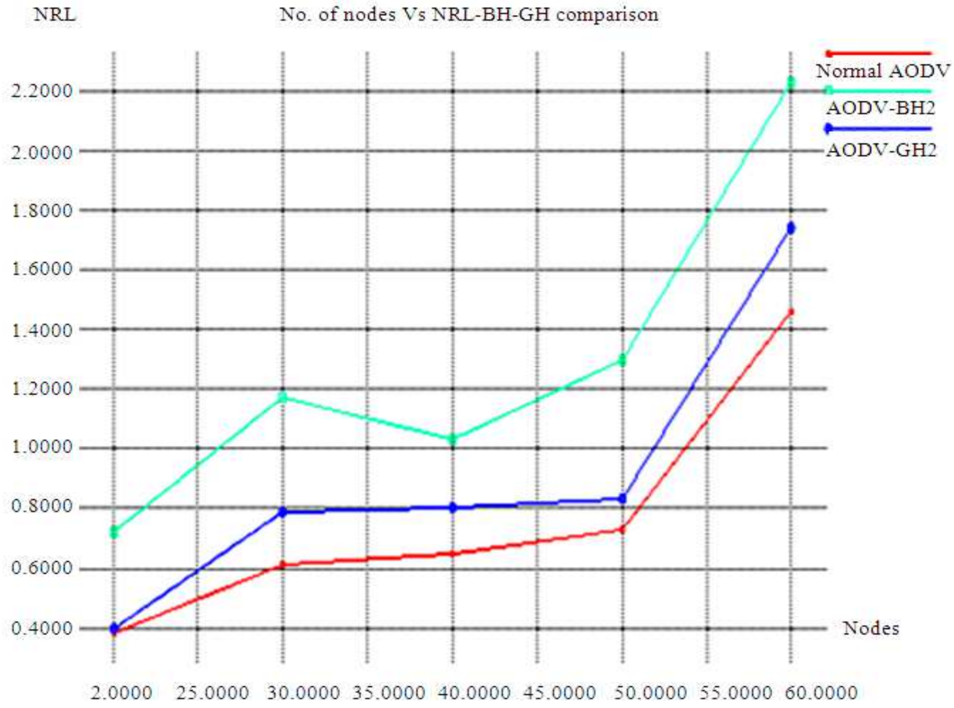


Fig. 18. Routing Load Comparision Graph

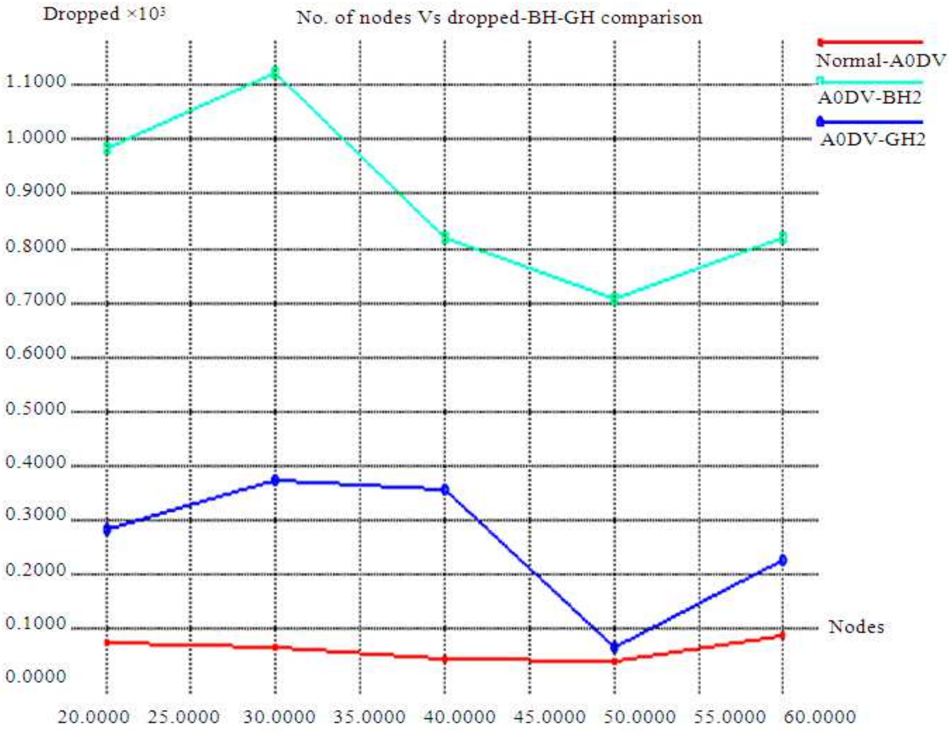


Fig. 19. Total dropped packets comparision graph

The above **Fig. 19** shows the comparison table between Black hole attacks and Gray Hole attacks. Packet delivery ratio decreases when we increase the attacking nodes for both Black Hole and Gray Hole attacks. Normalized routing load decreases when we increase the nodes. Overhead also increases when we increase the attacking nodes. Dropped packets also get increased in the presence of more vulnerable nodes for both the cases of Black Hole attack and Gray Hole attack.

4. DISCUSSION

The results obtained explain that while comparing the two attacks, the impact of black Hole is higher than that of Gray Hole in all the cases. As shown in the graphs, the performance in terms of normalized routing load in the case of black Hole is little bit high and almost constant. But in the case of Gray Hole it is increasing with the network density. The performance in terms of overhead is increasing with the increase of network density in both cases and almost equal for different black/Gray Holes. The performance in terms of dropped packet is increasing with the increase of number of black/Gray Holes. Further, if we compare the graphs then we can find that the impact of black Hole is very much higher than that of the Gray Hole attack.

5. CONCLUSION

In this study we have studied and analyzed the performance of two types of attacks known as Black Hole and Gray Hole attacks. As shown in tables and graphs the impacts of these two attacks are considered under various network attributes and we have also compared the impact of these two attacks. As shown in the graphs and tables the Black Hole attacks are more vulnerable than Gray Hole attacks because the packet drop ratio is high for Black Hole attacks compared to Gray Hole attacks, not only that the normalized routing load also increases in the presence of Black Hole attacks compared to Gray Hole attacks. When compared to packet delivery fraction Black Hole attacks delivery rate decreases compared to Gray Hole attacks, the routing packets also decreased in the presence of Black Hole attacks to that of Gray Hole attacks. Thus from the simulation results one can observe that Black Hole attacks causes more damage to MANET compared to Gray Hole attacks. In our work we have considered the fake message "send fake RREP" from the source to destination. In our future work we try to analyze other such types of malicious behavior in AODV protocol. Furthur, while studying the AODV protocol we understand about its drawback, so we will provide a solution to secure AODV protocol.

6. REFERENCES

Aad, I., J.P. Hubaux, E.W. Knightly, 2008. Impact of denial of service attacks on ad hoc networks. IEEE/ACM Trans. Network., 16: 791-802. DOI: 10.1109/TNET.2007.904002

Gao, X. and C. Wei, 2007. A novel gray hole attack detection scheme for mobile ad-hoc networks. Proceedings of the International Conference on IFIP Network and Parallel Computing Workshops, Sep. 18-21, IEEE Xplore Press, Liaoning, pp: 209-2014. DOI: 10.1109/NPC.2007.88

Hu, Y.C., A. Perrig and D.B. Johnson, 2002. Ariadne: A secure on-demand routing protocol for ad hoc networks. J. Wireless Netw., 11: 21-38. DOI: 10.1007/s11276-004-4744-y

Issariyakul, T. and E. Hossain, 2008. Introduction to Network Simulator NS2. 1st Edn., Springer, New York, ISBN-10: 0387717595, pp: 400.

Liu, C. and J. Kaiser, 2003. A survey of mobile ad hoc network routing protocols. University of Ulm Technology.

Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehavior in mobile ad hoc networks. Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, (MobiCom' 00), IEEE Xplore Press, New York, pp: 255-265. DOI: 10.1145/345910.345955

Nguyen, H.L. and U.T. Nguyen, 2008. A study of different types of attacks on multicast in mobile ad hoc networks. Ad Hoc Netw., 6: 32-46. DOI: 10.1016/j.adhoc.2006.07.005

Ning, P. and K. Sun, 2005. How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols. Ad Hoc Netw., 3: 795-819. DOI: 10.1016/j.adhoc.2004.04.001

Panagiotis, P. and Z.J. Haas, 2002. Secure routing for mobile ad hoc networks. Proceeding of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, Jan. 27-31, IEEE Xplore Press, San Antonio, TX., pp: 1-13.

Perkins, C., E. Belding-Royer and S. Das, 2003. Ad hoc On-demand Distance Vector (AODV) routing. RFC.

Royer, E.M. and T. Chai-Keong, 1999. A review of current routing protocols for ad hoc mobile wireless networks. IEEE Personal Commun., 6: 46-55. DOI: 10.1109/98.760423

Sen, J., M.G. Chandra, S.G. Harihara, H. Reddy and P. Balamuralidhar, 2007. A mechanism for detection of gray hole attack in mobile ad hoc networks. Proceedings of the 6th International Conference on Information, Communications and Signal Processing, Dec. 10-13, IEEE Xplore Press, Singapore, pp: 1-5. DOI: 10.1109/ICICS.2007.4449664