An Innovative Approach to Detect the Gray-Hole Attack in AODV based MANET

Madhuri Gupta
Maharana Pratap College of Technology, Gwalior (M.P)
India

Krishna Kumar Joshi
Maharana Pratap College of Technology, Gwalior (M.P)
India

ABSTRACT
The wireless arena has been experiencing exponential growth in nowadays. Wireless devices are now playing an ever-increasingly important role in our lives. an ad hoc network might consist of several home-computing devices, including notebooks, handheld PCs, and so on. Each node will be able to communicate directly with other nodes that reside within range of transmission. For communicating with nodes that reside besides this range, the node needs to use intermediate nodes to relay messages hop by hop. Gray hole is a node that can switch from behaving correctly to behaving like a black hole that is it is actually an attacker and it will act as a normal node. So we can't identify easily the attacker since it behaves as a normal node. Every node maintains a routing table that stores the next hop node information which is a route packet to destination node In this paper we proposed an innovative approach for the detection of the dangerous grayhole attack. The proposed algorithm is implemented on a very popular on demand routing protocol known as AODV (Ad hoc On demand Distance Vector) routing protocol. The beauty of this proposed algorithm is that it not only identifies the grayhole attacker node but also confirm it as well. The algorithm is divided into two phases: Noting Phase and the Confirmation phase. To simulate the effect of the proposed work the popular NS 2(Network Simulator 2) is used.

General Terms
Mobile Adhoc Networks, Routing protocols, Active attacks, Passive attacks, Reactive Routing protocol, Algorithm.

Keywords
MANET; AODV; RREP; RREQ; Grayhole

1. INTRODUCTION
The wireless communication landscape has been changing greatly, driven by the fast advances in wireless technologies and the greater selection of new wireless services and applications. The developing third-generation cellular networks have greatly improved the speed of data transmission, which enables a variety of higher-speed mobile data services. Meanwhile, new standards for short-range radio such as 802.11, Hiperlan, infrared transmission and Bluetooth are helping to create a wide range of new applications for home networking and enterprise, enabling wireless broadband multimedia and data communication in the office and home. An ad hoc network might consist of several home-computing devices, including notebooks, handheld PCs, and so on. Each node will be able to communicate directly with other nodes that reside within range of transmission. For communicating with nodes that reside besides this range, the node needs to use intermediate nodes to relay messages hop by hop.

Fig 1: Mobile Ad hoc Networks

Gray hole is a node which can switch from behaving correctly to behaving like a black hole that is it is actually an attacker and it will act as a normal node. So we can't identify easily the attacker since it behaves as a normal node. Every node maintains a routing table that stores the next hop node information which is a route packet to destination node.

2. AODV PROTOCOL
As a routing protocol for mobile ad hoc networks, AODV is intended to accommodate networks that are as large as several thousand nodes. It is one of several *demand-driven* (or *on-demand*) protocols that are in existence today. Hence, the protocol is invoked only when a node (host) has data to transmit. It is a *reactive* protocol. The AODV RFC indicates that the transport layer protocol is UDP, which of course only offers best effort delivery of packets, and does not support either error recovery or flow control. Addressing is handled using IP addressing. Since each node acts as both a host and routing node, each must maintain a routing table that contains information about known destination nodes. Entries are keyed to destinations. Each entry in the routing table contains nine fields. In addition to the destination node IP address, the fields contain routing information and information that relates to the qualitative state of the route for maintenance purposes. AODV only maintains information on the next destination (hop) in the route, not the entire routing list. This saves memory and lowers computational overhead for route maintenance. It also contains information enabling the host to share information with other nodes when link states change. The sequence number, unique to each destination route, is the key to maintaining up to date routing information. Protocol messages that contain routing information also include a sequence number. By observing the value of the sequence number, an intermediate node can determine the "freshness" of the routing information.

The basic message set consists of RREQ (Route Request), RREP (Route reply), RERR (Route error) and HELLO message.

2.1 RREQ Messages

- When communication routes between nodes are valid, AODV does not play any role.
- When a node wants to discover a route to a destination, a RREQ message is broadcasted.
- Intermediate nodes use RREQ to update their routing tables (in the direction of the source node), as it propagates through the network.
- The RREQ also consists of the most recent sequence number for the destination.
- A sequence number is must to the valid destination route at least as great as that contained in the RREQ.

Type	J	R	G	D	U	Reserved	Hop count
RREQ ID							
Destination IP Address							
Destination Sequence Number							
Originator IP Address							
Originator Sequence Number							

Fig 2: RREQ Packet

2.2 RREP Messages

- When a destination node has a RREQ message, the destination route is made available by unicasting a RREP back to the source route.
- Intermediate nodes update RREP routing tables (in the direction of the destination node), as the RREP propagates back to the source node.

Type	R	A	Reserved	Prefix size	Hop Count
Destination IP Address					
Destination Sequence Number					
Originator IP Address					
Life Time					

Fig 3: RREP Packet

2.3 RERR Messages

- For broken links, RERR message is broadcasted.
- Directly generated by a node or passed on when received from another node

Type	N	Reserved	Destination Count
Unreachable Destination IP Address (1)			
Unreachable Destination Sequence Number (1)			
Additional Unreachable Destination IP Addresses (if needed)			
Additional Unreachable Destination Sequence Numbers (if needed)			

Fig 4: RERR Packet

2.4 Hello Messages

- Hello Message = RREP with TTL = 1
- For broadcasting connectivity information, this message is used.
- A node should use Hello messages only if it is part of an active route.

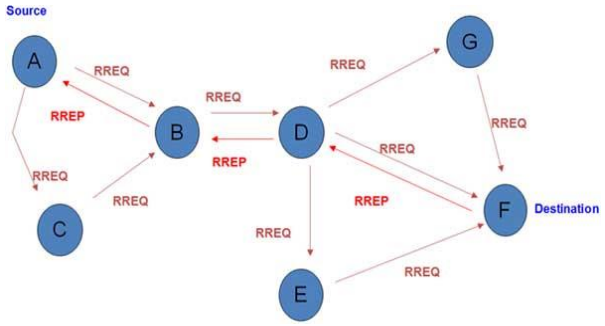

Fig 5: Routing a Packet by AODV

3. GRAY HOLE ATTACK

In computer networking, a **packet drop attack** or **black hole attack** is a type of denial-of-service attack in which a router that is supposed to relay packets instead removes them. This usually occurs from a router becoming compromised from a number of different reasons. One reason mentioned in research is through a denial-of-service attack on the router using a Distributed Denial of Service tool. Because packets are routinely dropped from a flossy network, the packet drop attack is very hard to detect and prevent.

The malicious router can also attain this attack selectively, for example, by dropping packets for a particular network destination, at a specific time of the day, a packet every *n* packets or every *t* seconds, or a randomly selected part of the packets. This is known as a **gray hole attack**. If the malicious router drops all the coming packets, the attack can actually be discovered fairly quickly through common networking tools such as trace route. Also, when other routers observe that the negotiated router is dropping all traffic, they will generally start to remove that router from their forwarding tables and finally no traffic will flow to the attack. But if the malicious router starts dropping packets on a specific time period or over every *n* packet, it is generally harder to detect because some traffic still flows across the network

Gray hole is a node that can switch from behaving correctly to behaving like a black hole that is it is actually an attacker and it will act as a normal node. So we can't identify easily the attacker since it behaves as a normal node. Every node maintains a routing table that stores the next hop node information which is a route packet to destination node
The gray hole attack has two phases:
Phase 1:
A malicious node performs the AODV Protocol to promote itself as having a valid route to destination node, with the intention of interrupting packets of spurious route.
Phase 2:
In this phase, the nodes has been dropped the interrupted packets with a certain probability and the detection of gray hole attack is a difficult process. Normally in the gray hole attacks the attacker behaves maliciously for the time whenever the packets are not dropped and then switch to their normal behavior. Both normal node and attacker are same.

Due to this behavior, it is very hard to find out in the network to figure out such kind of attack. The other name for Gray hole attack is node misbehaving attack.

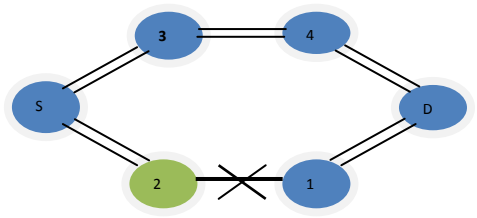

Fig. 6 Grayhole attack in MANET

In above figure

- S- Source
- D- Destination
- 1- Node, 3- Node, 4-Node
- 2-Malicious Node

4. RELATED WORK

Mr. C.S. Dhamande et al [1] has proposed a technique which is summarized as: 1. to study the effects of Gray Hole attack in the light of packet delivery ratio (PDR), network load and End to End delay in MANET. 2. Simulating Grayhole attack using Ad- hoc On Demand Vector (AODV) Routing protocol. 3. Comparing the results of AODV protocol with and without Gray Hole attack. 4. Proposed new efficient security technique in AODV protocol as a counter measure of gray hole attack & also minimize the impact of gray hole attack

Ashok Desai et al [3] proposed a mechanism which is based on the mobile agent. In this method, each mobile agent has two parameters, one is expiry time and other is RTT time. In a fixed time interval mobile agent is generated from source node and move to the network. In a fixed time period, it should calculate the overhear rate of its next hop and compare it with the threshold value. In this algorithm, mobile agent does not visit each neighbour node but only observes the next node in current route. This algorithm detects the gray hole and minimizes the packet drop and congestion

Avnesh Kumar et al [4] proposed a methodology which detect and prevent the group gray hole attack in the network. In this method, to detect the malicious node, the previous neighbour node and suspected node checks the two hop distance node for each possible path which goes towards the destination. So, firstly it stores the RREP packet at previous node and adds one hop distance of suspected node. This algorithm is based on destination based routing method. The major factor of this algorithm is to maximize the overall network throughput

Sarita Chaudhary et al [5] proposed a technique for detection and removal of black holes and gray holes from the network. In this methodology, the concept of core maintenance of the allocation table is used in which when a new node adds in the network, it broadcasts a message as a request for IP address. Then backbone node randomly selects an IP address which is free in the network. The new IP address is allotted to the new node and sends an acknowledgement to the backbone node.

Onkar V. Chandure et al [6] proposed an algorithm that is based on security based technique which is used to recognize and eradicate the problem of gray hole attack. It works in two phases, firstly it develops a method which is used to handle the malicious node in the network and then routing protocol is used to recognize the gray hole attack.

5. PROPOSED WORK

In this research work we proposed an innovative approach for the detection of the dangerous grayhole attack. The proposed algorithm is implemented on a very popular on demand routing protocol known as AODV (Ad hoc On demand Distance Vector) routing protocol. To simulate the effect of the proposed work the popular NS 2(Network Simulator 2) is used. The beauty of this proposed algorithm is that it not only identifies the grayhole attacker node but also confirm it as well. The algorithm is divided into two phases: Noticing Phase and the Confirmation phase.

In the noticing phase, for communicating with the destination node Source node (S) firstly want to find the route for the destination node. For this purpose it prepare a RREQ (Route REQuest) packet, in which it fills the address of the destination node (called as DSTO) and this packet is broadcasted to the neighboring nodes. Now, the source node waits for all the replies send by the replying nodes in terms of the RREP (Route REPly) packets and after getting all the replies from the replying nodes, it sorts these replies in terms of the Decreasing order of the destination sequence numbers (DSN) into its own Route Record (RR). Means, a RREP contains highest DSN stored in the top of the RR table.

Now, the source node compares the DSN of the first entry from the R-R table with the Threshold value (TV), which is average of the all the DSNs of the replying nodes. Now, If DSN of the first node is much greater than TV the source node note this node as attacker node and called the second phase.

In the Confirmation phase, Source node sends a new RREQ packet for a new destination, known as Virtual Destination (DSTV) and waits for the reply coming from the replying nodes containing the paths from the source node to this virtual node. And stores the replies in terms of their DSNs, and picks the first entry from the RR table and compare it with the TV and if it is much greater than the TV and also that node which is already considered as the noticing node in the previous phase then confirm it as Grayhole attacker node. And after confirming the grayhole attacker node it broadcast the information about this node to all other nodes and then they remove the entry of this grayhole node from their route cache.

Abbreviations used in the Algorithm
DSN – Destination Sequence Number
SSN- Source Sequence Number
DSTO - Original Destination
DSTV- New Virtual Destination
R-R Table- Route Reply Table
RREQ- Route Request

Algorithm
Phase 1: Noticing Phase

Step 1: Root Discovery Process
Source S starts the route discovery process for the DSTO by broadcasting the RREQ packet to the neighboring node.

Step 2: Collecting All the Replies
S stores all the replies sent by the Replying nodes after sorting in terms of the Highest DSN in RR Table.

Step 3: Identification of Noticing Node
Pick topmost entry from RR-Table.
If (DSN>>TV)

{
S [Nid] =1;
//Noticing Node
}
Go to step 4

Phase 2: Confirmation phase
Step 4: Confirmation of the Noticing node as the Grayhole Node
S sends a new RREQ packet for a new destination, known as Virtual Destination (DSTV) and waits for the reply coming from the replying nodes containing the paths from the source node to this virtual node. And stores the replies in terms of their DSNs, and picks the first entry from the RR table and compare it with the TV and if it is much greater than the TV and also that node which is already considered as the noticing node in the previous phase then confirm it as Grayhole attacker node.
Step 5: Removal of Grayhole Node
Remove the Entry of the Grayhole node from the R-R table.
Step 6: Broadcasting the Information of the Grayhole Node
S broadcast the information about the Grayhole node to all other nodes.

Step 7: Continue Default Routing Process
Continue with the normal procedure of AODV Protocol.

6. IMPLEMENTATION AND RESULTS
The proposed work is implemented in NS-2 simulator and executed on a Pentium (Core i3) processor with 3 GB of RAM, running at 2.40 GHz under Red Hat Enterprise Linux (RHEL) 5.0.

6.1 Parameters
The effectiveness of our work to detect the Grayhole attack is evaluated in this subsection using the simulations performed in a very popular simulator, called Network Simulator (NS)-2 with the 10, 20, upto 100 nodes mobile nodes. The graphical representation of this simulation is shown in the popular animator, called Network Animator (NAM).The traffic type is Continuous Bit Rate (CBR), the channel used is a wireless channel, the Ad hoc routing protocol used is Dynamic Source routing (DSR) and the network interface is wireless physical. The parameters are defined below:

TABLE 1 SIMULATION PARAMETERS

Parameter	Value
Number of Nodes	Variable (10,20, and 50)
Topography Dimension	750 m x 750 m
Traffic Type	CBR
Signal Propagation Model	Two Ray Ground model
MAC Type	802.11 MAC Layer
Packet Size	512 bytes
Mobility Model	Random Way Point
Antenna Type	Omni directional
Mobile Ad Hoc Routing Protocol	AODV
Interface Queue	Drop Tail/Priority Queue
Maximum packets in Interface Queue	100
Channel	Wireless Channel
Link Layer Type	LL
Network Interface Type	Wireless Phy
Number of Grayhole attackers	1

6.2 Simulation Results
The simulation scenario of the 50 mobile wireless nodes. This figure is used to show the initial position of these nodes

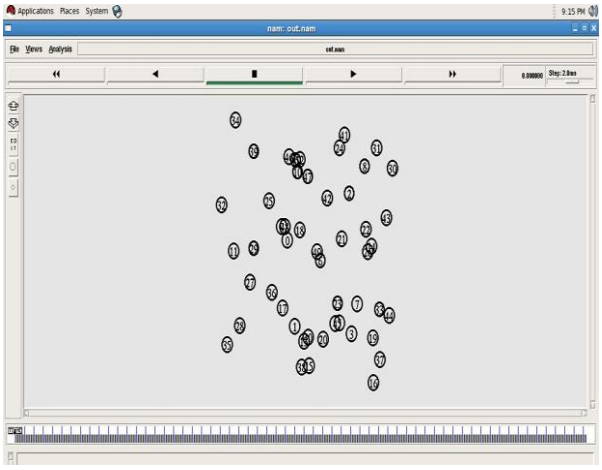

Fig 7: Initial Simulation of 30 Mobile Nodes Implementing AODV Protocol

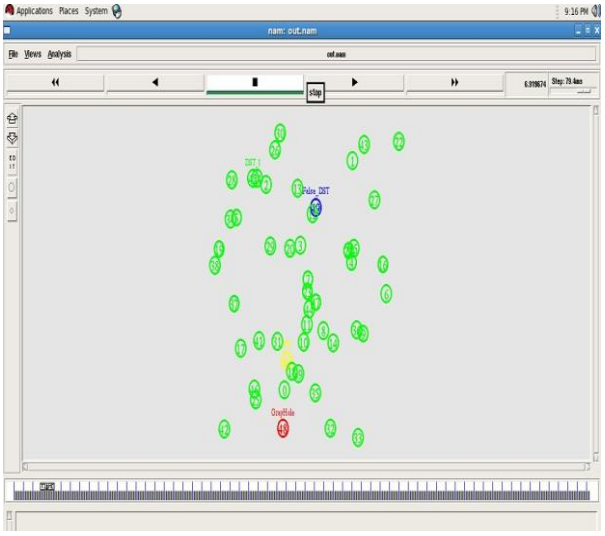

Fig 8: Final Simulation of 30 Mobile Nodes Implementing AODV Protocol

6.3 Simulation Graphs

We have shown three graphs, End to End Delay, Throughput, and Packet Delivery Ratio for showing the simulation results.

6.3.1 Average End to End Delay Graph

It gives the average time to send a packet from source to the destination. his Graph is drawn between Number of Black hole Nodes in X Axis and Avg. End to end Delay (in milliseconds) in Y-Axis.

6.3.1.1 Number of mobile nodes =10

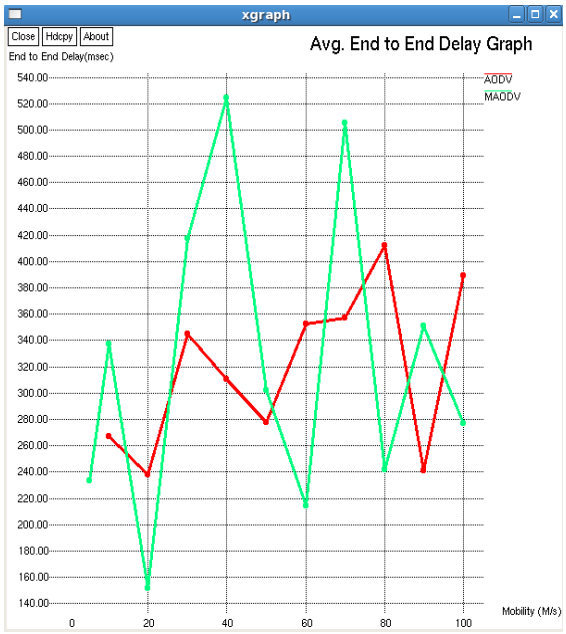

Fig 9: Average End to End Delay (in msec.) for 10 mobile nodes

6.3.1.2 Number of mobile nodes =20

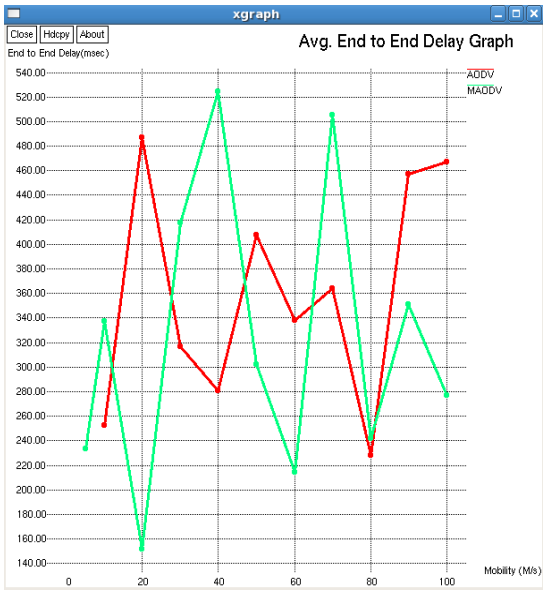

Fig 10: Average End to End Delay (in msec.) for 20 mobile nodes

6.3.1.3 Number of mobile nodes =50

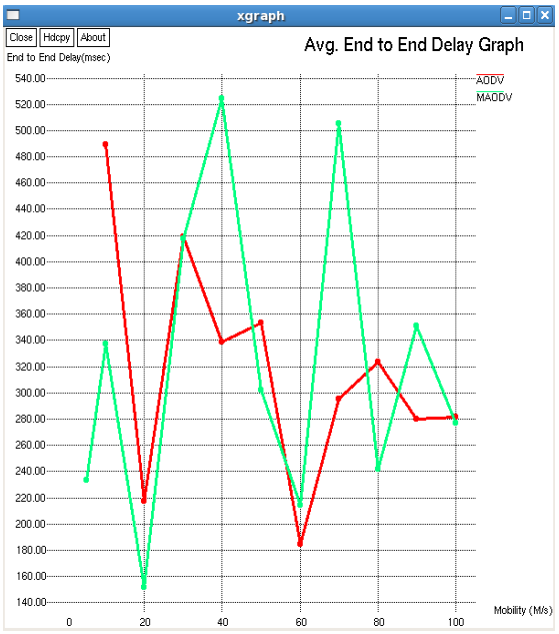

Fig 11: Average End to End Delay (in msec.) for 50 mobile nodes

6.3.2 Throughput Graph

It gives the total number of bits send to the physical layer per second. This Graph is drawn between Mobility (in m/sec) in X Axis and Throughput (in Kbps) in Y-Axis.

6.3.2.1 Number of mobile nodes =10

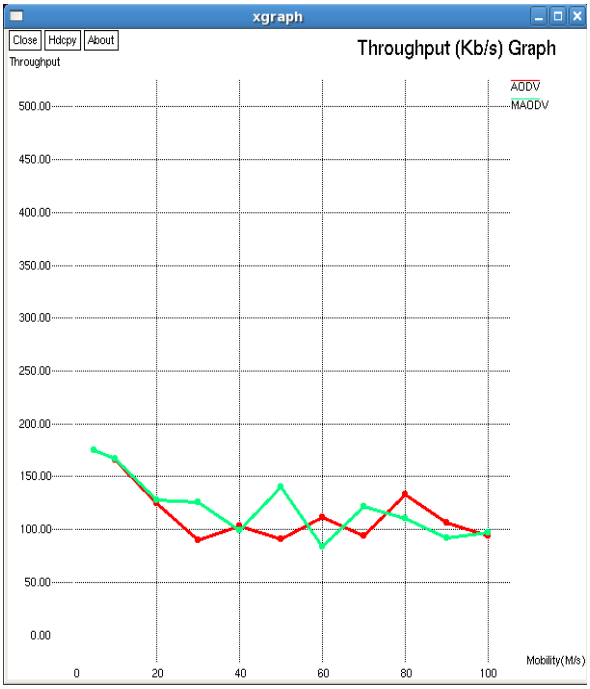

Fig 12: Throughput Graph with 10 mobile node

6.3.2.2 Number of mobile nodes =20

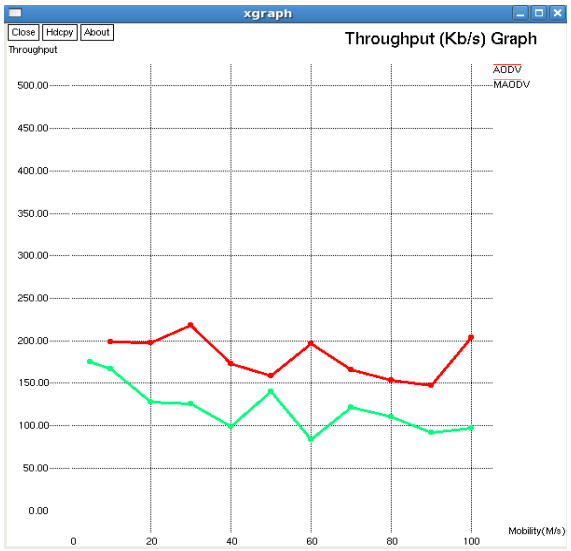

Fig 13: Throughput Graph with 20 mobile node

6.3.2.3 Number of mobile nodes =50

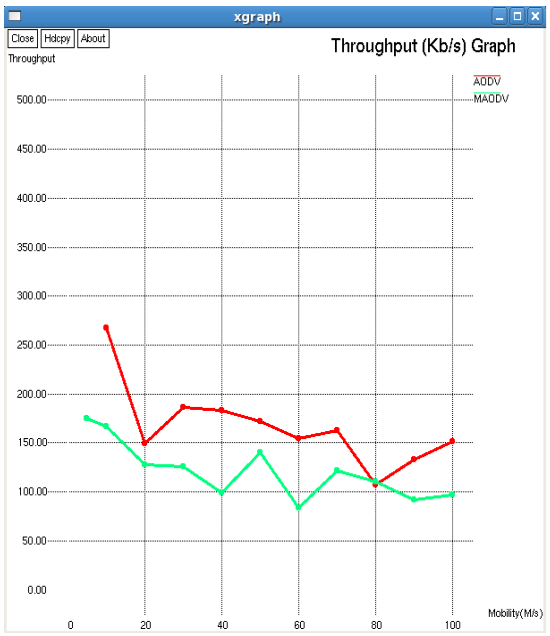

Fig 14: Throughput Graph with 50 mobile node

6.3.3 Packet Delivery Ratio Graph

It gives the ratio of the total incoming packets and the actual received packets by the destination. This Graph is drawn between Number of Black hole Nodes in X Axis and PDR in Y-Axis.

6.3.3.1 Number of mobile nodes =10

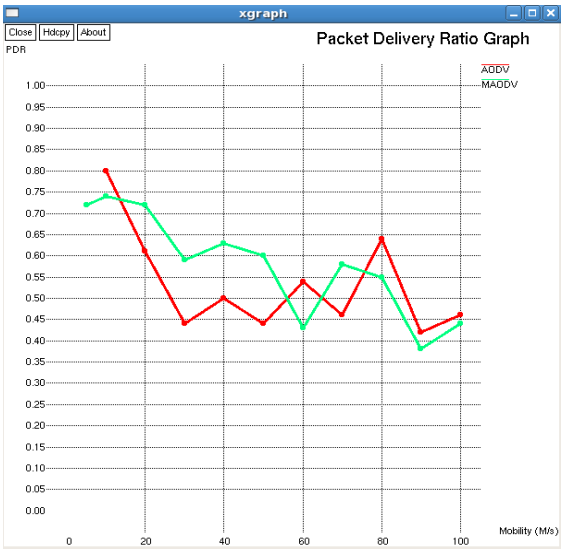

Fig 15: Packet Delivery Ratio Graph with10 mobile node

6.3.3.2 Number of mobile nodes =20

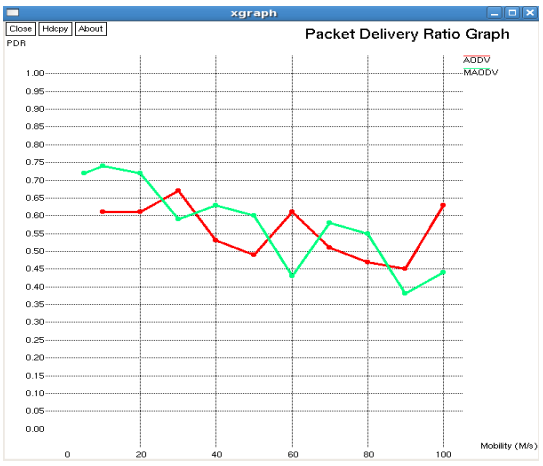

Fig 16: Packet Delivery Ratio Graph with 20 mobile node

6.3.3.3 Number of mobile nodes =50

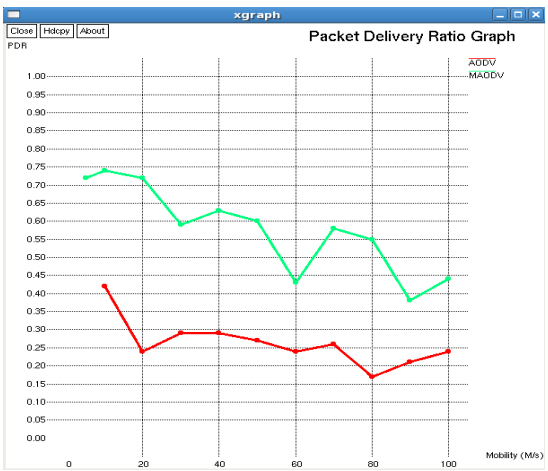

Fig 17: Packet Delivery Ratio Graph with 50 mobile node

6. CONCLUSION

In this paper, we proposed an algorithm to detect the gray hole attack in AODV based MANET. In the proposed solution, there are two phases. One is noticing phase in which the source node compares the DSN of the first entry from the R-R table with the Threshold value (TV), which is average of the all the DSNs of the replying nodes. Now, if DSN of the first node is much greater than TV the source node note this node as attacker node. Other is confirmation phase in which source node sends a new packet for a new destination, if again DSN is greater then confirm it as a gray hole attacker node. Compare the performance as a throughput, packet delivery ratio and end to and delay

7. REFERENCES

[1] Banerjee S, "Detection/removal of cooperative black and grayhole attack in mobile ad hoc networks" In Proceedings of the World Congress on Engineering and Computer Science,2008.

[2] Sen J., Chandra M., HarishaS.G. Reddy H., Balmuralidhar P., "A Mechanism for Detection of Gray Hole Attack in Mobile AdHoc Networks", Information, Communications and Signal Processing, 2007, 6thInternational IEEE Conference.

[3] Gao Xiaopang, Chen Wei,"A novel Gray Hole Attack DetectionSchemeforMobileAd-HocNetworks"NetworkandParallelComputingWorkshops ,2007,NPCWorkshops,2007,IFIPInternational IEEE Coference.

[4] Kurosawa S.,Nakayama H.,KatoN ,Jamalipura A., and Nemoto Y. ,"Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning method," International Journal of Network Security,Vol.5,No.3,P.P338-346,Nov.2007.

[5] Jiwan CAI ,Ping YI, Jialin CHEN, Zhiyang WANG ,Ning LIU, "An Adaptive Approch to Detecting Black and Gray Hole Attacks in Ad Hoc Networks", Advanced Information Networking and Applications (AINA),2010th IEEE International Conference.

[6] Shivani Sharma, Tanupreet Singh, "Sequenced queue based routing algorithm (SQRA) for detection and correction of gray hole attack by implementing IDS", Proc. of the Intl. Conf. on Recent Trends In Computing and Communication Engineering -- RTCCE 2013.

[7] Ashok M. Kanthe, Dina Simunic, Ramjee Prasad, "A mechanism for grayhole attack detection in Mobile adhoc networks", International journal of computer applications(0975-8887) volume 53- No. 16, September 2012.

[8] Mr.Chetan S. Dhamande, Prof. H.R. Deshmukh ," A efficient way to minimize the impact of gray hole attack in adhoc network", International journal of emerging technology and advanced engineering, (ISSN 2250-2459, volume 2, issue 2,feb 2012).

[9] Dhamande C.S., Deshmukh H.R., "A competent way to diminish the brunt of gray hole attack in MANET ", International Journal of Wireless Communication (ISSN: 2231-3559 & E-ISSN: 2231-3567, VOLUME 2, ISSUE 1, 2012).

[10] Shivani Sharma, Tanupreet Singh, "An effective intrusion detection system for detection and correction of gray hole attack in MANETs", International journal of computer applications (0975-8887, volume 68- No. 12, April 2013).