Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol

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

V.T.Gaikwad
Associate Professor, Dept of CSE, Sipna's College of Engg & Tech, Amravati (MS) INDIA

ABSTRACT
In this paper, we describe the basic idea related with the implementation of AODV protocol & impact of gray hole attack on adhoc network. Information exchange in a network of mobile and wireless nodes without any infrastructure support such networks are called as adhoc networks. A Mobile adhoc network is mobile, multihop wireless network which is capable of autonomous operation. A Gray hole is a 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. Our mechanism helps to protect the network by detecting and reacting to malicious activities of any node. The results enable us to minimize the attacks on integrated MANET-Internet communication efficiently. Simulation will be carried out by using network simulator tool so as to address the problem of detection & prevention of gray hole attack in mobile ad-hoc network.

Keywords
Ns-2, adhoc network, AODV, Gray Hole Attack. Security threats, Packet forwarding misbehavior.

1. INTRODUCTION
Security is an essential service for wireless network communications. Wireless mobile ad hoc nature of MANET brings new security challenges to network design. Mobile ad hoc networks, due to their unique characteristics, are generally more vulnerable to information and physical security threats than wired networks Securing network protocols requires detailed analysis of normal protocol operations and vulnerabilities. Network protocol design and implementation have become increasingly complex. Mobile ad hoc network has been a challenging research area for the last few years because of its dynamic topology, power constraints, limited range of each mobile host's wireless transmissions and security issues etc. However, the characteristics of MANETS pose both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, access control, and no repudiation. A mobile ad-hoc network (MANET) is a network [1, 2] formed without any central administration which consists of mobile nodes that use a wireless interface to send packet data. In this work, we discuss one such attack known as Gray Hole Attack on the widely used AODV (Ad -hoc On-demand Distance Vector) routing protocol in MANETs. A mechanism presented shows the method to detect & prevent from gray hole attack in Mobile ad hoc network. Routing protocols are generally necessary for maintaining effective communication between distinct nodes. Routing protocol not only discovers network topology but also built the route for forwarding data packets and dynamically maintains routes between any pair of communicating nodes. Routing protocols are designed to adapt frequent changes in the network due to mobility of nodes. Several ad hoc routing protocols have been proposed in literature and can be classified [3] into proactive, reactive and hybrids protocols. Routing protocols basically performs two important functions: Routing function and Data-Forwarding function. Routing function performs routes discovery and routes maintenance activity. Data-Forwarding function is concerned with forwarding data packets toward the destination through the established route.

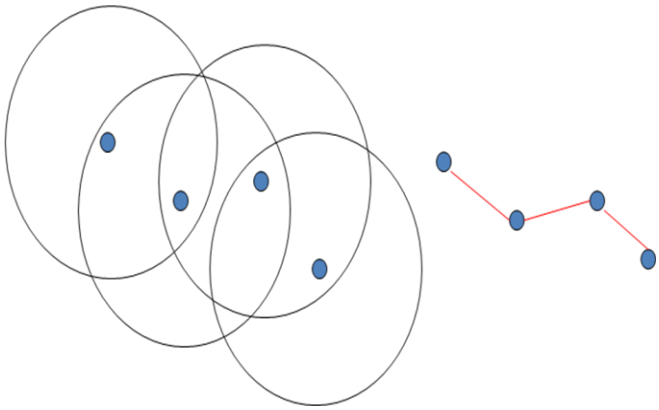

Figure 1.1.Representation of Multihop Wireless network

1.1 Attacks on Mobile Adhoc Network
Attacks on mobile ad hoc networks can be classified into following two categories: passive attacks and active attacks. [4,5]

1.1.1 Passive attacks:
A passive attack does not disrupt proper operation of the network. The attacker snoops the data exchanged in the network without altering it. Here, the requirement of confidentiality can be violated if an attacker is also able to interpret the data gathered through snooping. Detection of passive attacks is very difficult since the operation of the network itself does not get affected. they can reduced by using powerful encryption techniques.

1.1.2 Active attacks:
An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network. It can be classified into two categories external attacks and internal attacks. External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls. Both passive and active attacks can be made on any layer of the network protocol stack.

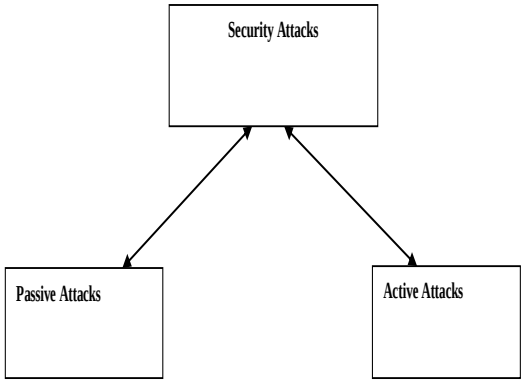

Figure 1.2 Attacks on Mobile Adhoc Network

Passive Attacks	Active Attacks
Snooping,eavesdropping,traffic analysis ,monitoring	Wormhole, black hole, gray hole, information disclosure, resource consumption, routing attacks

Table 1.1 Network Security Attacks against MANETS

1.1.3 Gray Hole Attack:

Gray Hole attack is the attack on the adhoc network .Gray Hole attack can be act as a slow poison in the network side means we can't said that probability of losing the data. In Gray Hole Attack [6] a malicious node refuses to forward certain packets and simply drops them. The attacker selectively drops the packets originating from a single IP address or a range of IP addresses and forwards the remaining packets. Gray Hole nodes in MANETs are very effective. Every node maintain a routing table that stores the next hop node information for a route a packet to destination node ,When a source node want to route a packet to the destination node , it uses a specific route if such a route is available in it's routing table. Otherwise, nodes initiates a route discovery process by broadcasting *Route Request* (RREQ) message to it's neighbors. On receiving RREQ message, the intermediate nodes update their routing tables for a reverse route to source node. A *Route Reply* (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other node that has a current route to destination. We now describe the gray hole attack[7] on MANET'S .The gray hole attack has two important stages , In first stage, a malicious node exploits the AODV protocol to advertise itself as having a valid route to destination node, with the intension of interrupting or corrupting packets, event though route is spurious. In second stage, nodes drop the interrupted packets with a certation probability. Detection of gray hole is difficult process. In some other gray hole attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior. Due this behavior it's very difficult for the network to figure out such kind of attack. Gray hole attack is also termed as node misbehaving attack. A variation of black hole attack s is the gray hole attack, in which nodes either drop packets selectively (e.g. dropping all UDP packets while forwarding TCP packets) or drop packets in a statistical manner (e.g. dropping 50% of the packets or dropping them with a probabilistic distribution). Both types of gray hole attacks seek to disrupt the network without being detected by the security measures in place [8].

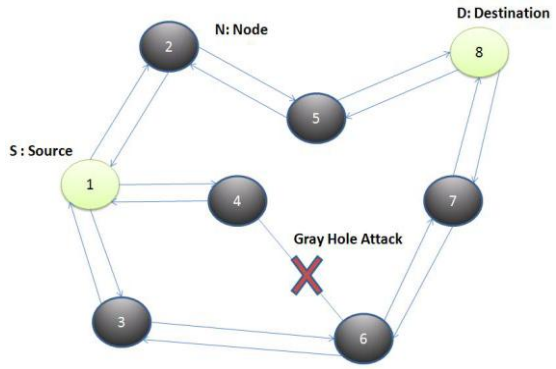

Figure 1.3 Gray Hole Attack in Mobile Adhoc Network

1.2 FEATURES OF MANET

MANET is advantageous with its several significant features [9] of which some of them are listed below:

Autonomous Terminal: In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. Besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.

Distributed Operation: One of the features of MANET is nothing but distribution operation since there is no background network for the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate among themselves and each node acts as a relay as needed, to implement functions security and routing etc.

Multihop Routing: The IEEE 802.11 technology is a good platform to implement single-hop adhoc networks. Single-hop is that stations must be within the same transmission area (100-200 meters) to communicate. This limitation can be overcome by multi-hop adhoc networking which forwards packets via one or more intermediate nodes [10].

Dynamic Network Topology: In adhoc network nodes are mobile, the network topology may change rapidly and unpredictably and the connectivity among the terminals may vary with time. MANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes [11]. The nodes in MANET dynamically establish routing among themselves as they move about, forming their own network on the fly.

Fluctuating Link Capacity: The nature of high bit-error rates of wireless connection might be more profound in a MANET. One end-to-end path can be shared by several sessions. The channel over which the terminals communicate is subject to noise, fading, and interference, and has less bandwidth than a wired network. In some scenarios, the path between any pair of users can traverse multiple wireless links and the link themselves can be heterogeneous.

Lightweight Terminals: Nodes in MANET are with less CPU processing capability, small memory size and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.

2. RELATED WORK

In this section we explore related work on security challenges in MANETS.Banerjee et. al. [7] has also proposed an algorithm for detection & removal of Black/Gray Holes. S.Ramaswamy et.al. [12] Presented an algorithm to prevent the co-operative black hole attacks in ad hoc network. In this section we mainly focus on the analyzing & defend the system from malicious impact of different attacks on MANET. Mechanisms or technique to prevent the routing layer from malicious attacks for securing the system of a MANET by cryptographic techniques are proposed by Y. Hu, Perrig and Johnson [13], Papadimitratos and Hass [14], Snazgiri [15]. In this section we mainly focus on the analyzing & defend the system from malicious impact of different attacks on MANET.

3. AODV PROTOCOL IN MANET

AODV stands for Ad-hoc on-demand Distance Vector Routing protocol The AODV protocol builds on the DSDV algorithm .it is an on demand routing algorithm. Operation of the protocol is divided into two functions, route discovery &route maintenance. At first all the nodes send hello message on its interface and receive hello message from its neighbors. This process repeats periodically to determine neighbor connectivity when a route is needed is to some destination, the protocols start route discovery .It uses two term route request & router reply.

A node has to update its own sequence number in two cases:

3.1 Control Messages in AODV

• Sequence Number and Routing Table Management.

• Before starting a route discovery process, the node has to Increment its own sequence number.

• A destination node has to update its own sequence number to the maximum of its current sequence number and the destination sequence number in RREQ packet immediately before transmitting the RREP packet. The sequence numbers in the routing table entries may be changed by the node only in the following circumstances.

• Offer of a new route to itself, if it is the destination node.

• Reception of an AODV message with new information about the sequence number for a destination.

• Expiration of path or path breaks.

When a node receives an AODV control message, either to create or to update a route for a particular destination, it searches its routing table for an entry to the destination. If there is no route entry, it creates a new one with the sequence number contained in the control packet, or else the sequence number is set invalid. Otherwise, the node compares the existing entry with the new information and updates it if either.

• The new sequence number is higher than in the routing table entry.

• The sequence numbers are equal and the new hop count plus one is smaller than in the existing route.

• The sequence number is unknown.

Besides the destination sequence numbers, the routing entry for each valid route contains a precursor list.

4. PERFORMANCE METRICS

The performance of the network is analyze according to the following performance metrics:

4.1 Packet Delivery Ratio (PDR)

The packet delivery ratio is nothing but the ratio of data or packets send at the source to the data or packets receive at the destination. To improve the performance of the network system the packet delivery ratio must be high as possible. if the packet delivery ratio is 100 % then we can say that the network is more reliable.

4.2 End to End Delay (e2e)

End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination. To get the reliable transmission in the network, this end to end delay should be minimum as possible.

4.3 Packet Loss Ratio

Packet loss ratio is again one of the metrics deal with the performance side. Packet loss occurs when one or more packets of data traveling across a computer network fail to reach their destination. Packet loss is distinguished as one of the three main error types encountered in digital communications. The other two being bit error and spurious packets caused due to noise. Packet loss can be caused by a number of factors including signal degradation over the network medium due to multi-path fading, packet drop because of channel congestion corrupted packets rejected in-transit, faulty networking hardware, faulty network drivers or normal routing routines (such as DSR in ad-hoc networks).In addition to this, packet loss probability is also affected by signal-to-noise ratio and distance between the transmitter and receiver.

5. PROCESS FOR FINDING OUT SUSPECTED NODE OR MALICIOUS NODE IN ADHOC NETWORK

Malicious node or suspected node indirectly affect on the adhoc network. It damages the data or packets during the network data transmission process, due to which the network gets disturb and ultimately performance of the network get reduced. This method focus on both suspected behavior of the node in the network. Once a node is recognize to be really malicious or suspected, the scheme has a notification mechanism for sending messages to all the nodes that are not yet suspected to be malicious, so that the spiteful node can be separated and not allowed to use any network resources. The mechanism consists of suspected node finding way which is invoked sequentially. This security procedure is invoked by a node when it identifies a suspicious node by examining its DRI table. We call the node that initiates the suspected node recognition procedure as the *Initiator Node* (IN). The IN first chooses a *Cooperative Node* (CN) in its neighborhood based on its DRI records and broadcasts a RREQ message to its 1-hop neighbors requesting for a route to the CN. In reply to this RREQ message the IN will receive a number of RREP messages from its neighboring nodes. It will certainly receive a RREP message from the *Suspected Node* (SN) if the latter is really a gray hole (since the gray holes always send RREP messages but drop data packets probabilistically). After receiving the RREP from the SN, the IN sends a probe packet to the CN through the SN. After the *time to live* (TTL) value of the probe packet is over, the IN enquires the CN whether it has received the probe packet. If the reply to this query is affirmative, (i.e., the probe packet is really received by the CN) then the IN updates its DRI table by making an entry „1" under the column „*Check Bit* against the node ID of the SN.

However, if the probe packet is found to have not reached the CN, the IN increases its level of suspicion about the SN and activates the suspected node recognition procedure, as discussed later in this Section.

SN-Suspected node CN-Cooperative node IN- Initiator node Nodes used in the network- N1 To N9

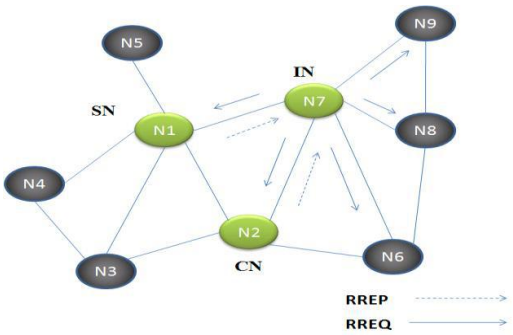

Figure 5.1 Basic Idea about the malicious node or suspected node finding process

NID (NODE ID)	PROBE STATUS
2	0
6	1
8	1
9	1

Table 5.1: Probe status for node 7

In Fig. 5 [16] node 7 acts as the IN and initiates the suspected node recognition method for the SN (node 1) and chooses node 2 as the CN. Node 2 is the most reliable node for node 7 as both the entries under columns „From and „Through for node 2 are „1". Node 7 broadcasts a RREQ message to all its neighbor nodes 1, 2, 6, 8 and 9 requesting them for a route to the CN, i.e., node 2 in the example.
After receiving a RREP from the SN (node 1), node 7 sends a probe packet to node 2 via node 1. Node 7 then enquires node 2 whether it has received the probe packet. If node 2 has received the probe packet, node 7 makes an entry „1" under the column „*CheckBit*" in its DRI table corresponding to the row of node 1. If node 2 has not received the probe packet, then node 7 invokes the suspected node recognition procedure. The elucidation that we propose here is basically only update the working of the source node without altering intermediate and destination nodes by using a method called Malicious node detection procedure. In this method three things are added, a new table RR-Table (Request Reply), a timer WT (Waiting Time) and a variable MN-ID (Malicious Node ID) to the data structures in the default AODV Protocol.

6. EXPERIMENTAL RESULT

6.1 Implementation of AODV Routing Protocol

Nodes(nn)	10	20	30	40	50
Packet Delivery Ratio (PDR)	81.88	98.88	98.88	98.75	98.93

Table 6.1 AODV Implementation with nn & PDR value

In the implementation of AODV protocol the performance of the AODV protocol is carried according to the performance metrics like packet delivery ratio, packet loss ratio, throughput & end to end delay term. During the implementation of the protocol different nodes are taken into consideration & on the basis of different nodes, the packet delivery ratio is calculated for every selected node. for node 10 the packet delivery ratio is 81.88 ,for node 20 packet delivery ratio is 98.88,for node 30 it is 98.88,for node 40 it is 98.75 & for node 50 it is 98.93.

Simulator	Ns-2(version 2.32)
Simulation time	500 (s)
Number of mobile nodes	10,20,30,40,50
Topology	700 * 700 (m)
Routing protocol	AODV
Traffic	Constant Bit Rate (CBR)

Table 6.2 Simulation Parameters for AODV & Gray Hole node

From table 6.1 the packet delivery ratio is different for different nodes. The packet delivery ratio must be so that paket sends at sender side is same as packet receive at destination side. in this we can achieve 100 % performance.

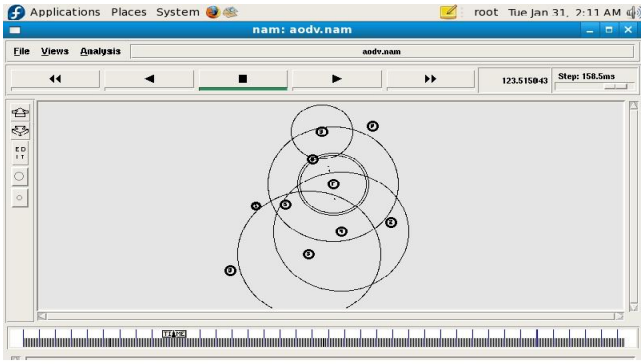

Figure 6.1 Mobile Nodes broadcasting the request for the packets

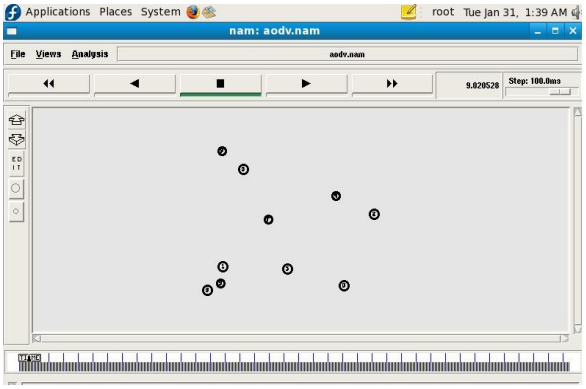

Figure 6.2 Dynamic Topology of nodes

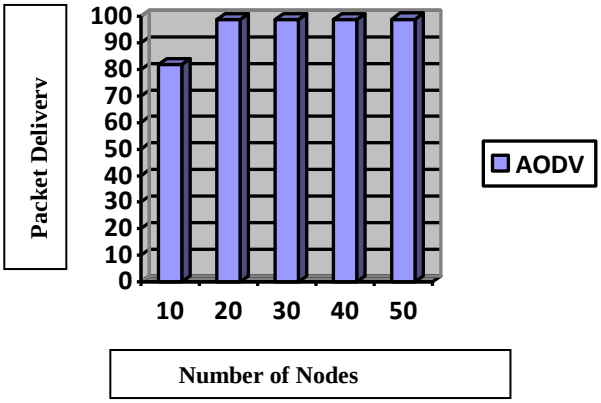

Figure 6.3 AODV with PDR & Nodes

6.2 Implementation of Gray Hole Attack in Adhoc network using simulator

In the implementation of Gray hole attack on adhoc network there is a impact on the performance of network. The performance of the system gets degrade due to the loss of packets & it is because of gray hole attack on the network. The Gray hole attack drops the packet during the transmission Gray hole, nodes drops the interrupted packets with a certation probability. Compare the table 6.1& 6.3, we can clearly observed that for normal implementation of AODV with nodes 10 the packet delivery ratio is 81.88 but after the gray hole attack on the AODV the packet delivery ratio with same node value 10 becomes 78.33.means there is a loss of packets & the loss of packet is due to the gray hole attack problem. normal implementation of AODV with nodes 20 the packet delivery ratio is 98.88 but after the gray hole attack on the AODV the packet delivery ratio with same node value 20 becomes 88.17. normal implementation of AODV with nodes 30 the packet delivery ratio is 98.88 but after the gray hole attack on the AODV the packet delivery ratio with same node value 30 becomes 90.77, normal implementation of AODV with nodes 40 the packet delivery ratio is 98.75 but after the gray hole attack on the AODV the packet delivery ratio with same node value 40 becomes 97.29, normal implementation of AODV with nodes 50 the packet delivery ratio is 98.93 but after the gray hole attack on the AODV the packet delivery ratio with same node value 50 becomes 87.40.

Nodes(nn)	10	20	30	40	50
Gray hole	78.33	88.17	90.77	97.29	87.40

Table 6.3 Gray Hole Implementation

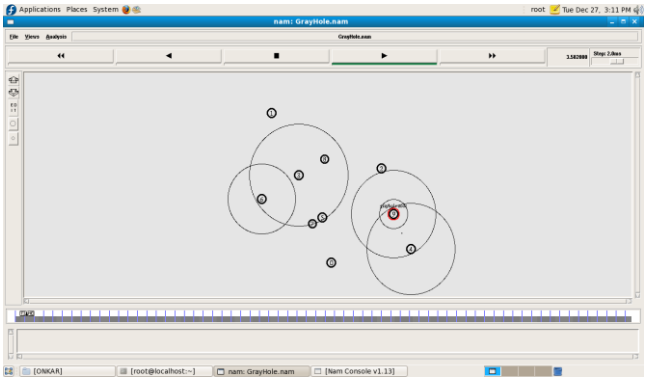

Figure 6.4 Gray Hole node on the AODV protocol Indicated by Red circle

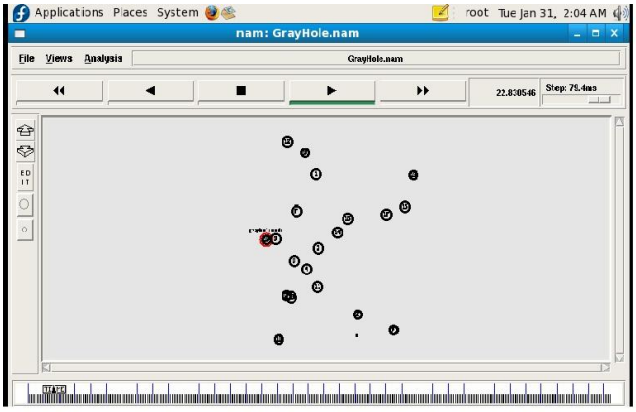

Figure 6.5 Gray Hole Attack with different nodes in the network

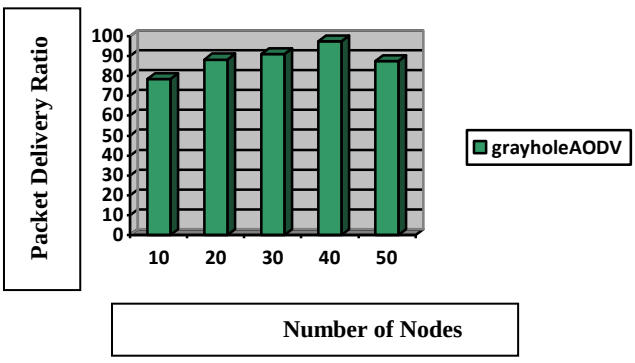

Figure 6.6 Gray hole AODV with PDR

Number of nodes (nn)	End to end delay for AODV(e2e)	End to end delay for Gray Hole AODV(e2e)
10	0.00336421	0.0034471
20	0.00943334	0.00898087
30	0.00264237	0.0145479
40	0.0147734	0.00536673
50	0.00538735	0.00302071

Table 6.4 E2e delay for AODV & Gray Hole AODV With different nodes value

7. CONCLUSION

Performance is the main term for any network but because of some attacks such as gray hole attack as main in this paper the network performance gets degrade. 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. To show the effectiveness and results of proposed approach, implementation work on Network Simulator 2 tool is still in progress phase. Future works will includes some method to secure the adhoc network from the gray hole attack & also improve the performance of the network & make the network well efficient.

REFERENCES

[1] K. Snazgiri, B. Dahill, B. Levine, C. Shields, and E.A. Belding-Royer, "*Secure routing protocol for ad hoc networks*,"In Proceedings of International Conference on Network Protocols (ICNP), Paris, France, November 2002.

[2] L. Zhou, and Z. Haas, "*Securing ad hoc network*," IEEE Network Magazine, Special issue on network security, Vol. 13,No. 6, November/December 1999, pp. 24-30.

[3] C. Mbarushimana, and A. Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad Hoc Networks," in Proc. of the 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW '07),May 2007, pp. 679–684.

[4] S. Yi and R. Kravets, Composite Key Management for AdHoc Networks.Proc. of the 1st Annual International Conference on Mobile and Ubiquitous Systems: Networkingand Services(MobiQuitous'04), pp. 52-61, 2004.

[5] R. Oppliger, Internet and Intranet Security, Artech House, 1998.

[6] Vishnu K, and Amos J .Paul," Detection & Removal of cooperative Black/Gray hole attack in Mobile ADHOC Networks." International Journal of Computer Applications 2010, Volume 1-No.22, pp.38-42.

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

[8] Oscar F. Gonzalez, God win Ansa, Michael Howarth andGeorge Pavlou. "Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc networks", Journal of Internet Engineering, 2:1, 2008.

[9] K. Weniger, M. Zitterbart, "Mobile adhoc networks – current approaches and future directions," Network, IEEE, vol 18, Issue 4, pp 6–11, July-Aug 2004.

[10] Rappaport, T.S.; Annamalai, A.; Buehrer, R.M.; Tranter, W.H.,"Wireless communications: past events and a future perspective",IEEE Communications Magazine, Vol. 40, Issue 5, PP 148 – 161, May 2002.

[11] Conti M, Giordano S, "Multihop Adhoc Networking: The Theory",IEEE Communications Magazine, Volume 45, Issue 4, pp 78 - 86,April 2007

[12]Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya,John Dixon, and Kendall Nygard,"Prevention of Cooperative Black Hole Attack in Wireless AdHoc Networks". In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA, pp. 570-575.

[13] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on demand routing protocol for ad-hoc networks," *In Proceedings of the 8th Annual International Conference on Mobile Computing and Networking* (MobiCom 2002), pp. 12-23,ACM Atlanta, GA, September 2002

[14] P. Papadimitratos, and Z. Haas, "Secure routing for mobile ad hoc networks," In Proceedings of SCS Communications Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 2002.

[15] K. Snazgiri, B. Dahill, B. Levine, C. Shields, and E.A. Belding-Royer, "Secure routing protocol for ad hoc networks," In Proceedings of International Conference on Network Protocols (ICNP), Paris, France, November 2002.

[16] Jaydip Sen, M.Girish Chandra Harihara S.G ,H.ReddyP.Balamuralidhar,"A Mechanism for Detection of Gray Hole Attack in Mobile AdHoc Networks," Information, Communications & Signal Processing, 2007 6th International Conference on.ICICS 2007,pp.1-5.