IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 9, Issue 1, Ver. III (Jan. 2014), PP 28-35
www.iosrjournals.org

Intrusion Detection Enabled Mobile Ad hoc Networks to Counter Blackhole and Grayhole Attacks

B. Prabhakara Reddy[1], Dr. M.N. Giri Prasad[2]

Associate Professor, Dept of ECE[1]

Professor and HOD, Dept of ECE[2]

Bheema Institute of Technology & Science, Adoni[1]

JNTUA College of Engineering, Anantapur[2]

Andhra Pradesh, India[1, 2]

***Abstract**: Mobile ad hoc network (MANET) is a temporary multi-hop wireless network that consists of mobile nodes which have the ability to communicate with each other without having fixed network infrastructure or central base station. The open access nature of wireless links in MANETs makes them susceptible to the Denial of service attacks such as Blackhole, Grayhole and etc. The disadvantage of the most ratified routing protocols like Ad hoc On-demand Distance vector(AODV) routing protocol is the fact that they have been developed without considering security mechanisms in advance hence resulting in the vulnerability of MANETs to such malicious attacks. In this work we propose an ad hoc routing protocol called SEA (Security Enabled AODV) to defend MANET against the Blackhole and Grayhole attacks. The simulations were implemented using popular discrete event network simulator NS-2.35 in the latest version ubuntu-12.04 environment. Network Simulations have been performed on the basis of performance parameters and effect has been analyzed after adding Blackhole and grayhole nodes. The simulation analysis proved that the proposed SEA outperforms the conventional AODV routing protocol in the attack scenarios in terms of different Quality of Service (QOS) parameters such as PDR, Average end to end Delay, Throughput, Normalized Routing Overhead and etc.*

***Keywords:** Blackhole; Grayhole; Wormhole; AODV; PDR; Throughput;*

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is a new paradigm of mobile wireless networks, offering unrestricted mobility with zero centralized infrastructure support [1]. The network nodes play the dual role as hosts and routers in MANET on the basis of mutual cooperation so as to enable communication between them. But few of the unreceptive nodes deny cooperating with other nodes leading such type of misbehavior to the dropping of data packets. More over the limited bandwidth, open nature of wireless medium, memory constraints and processing capabilities of MANET also makes them more vulnerable to the security threats. So secure routing is the major concern in MANETs. The traditional security measures are not applicable in MANETs due to the following reasons: (i) MANETs do not have infrastructure nature due to the absence of centralized authority (ii) MANETs do not have grounds for a priori classification due to the fact that all nodes are required to cooperate in supporting the network operation (iii) wireless attacks may come from all directions within a MANET (iv) wireless data transmission does not provide clear line of defense, gateways and firewalls and (v) MANETs have constantly changing topology owing to the movement of nodes in and out of the network.

The MANET is susceptible to various attacks viz. Denial-of-service (DoS) attacks such as Blackhole, Wormhole, and Sinkhole, eavesdropping, spoofing the packets transacted and the malicious modification of the packet contents [2]. The most ratified routing protocols for MANETs were designed based on the fact that they have been developed without considering security mechanisms in advance which is going to be the major drawback and becomes even more critical when extreme emergency communications must be deployed at the ground of a rescue. In these circumstances nodes with malicious intent could launch different kind of attacks damaging the communication quality. In regards to this, we attempt to analyze and improve the security of the conventional routing protocol AODV [3] against the Black hole and Grayhole attacks. In black hole attack a malicious node called blackhole replies to every route request by falsely claiming that it has a fresh enough routes to the destination without looking into the available resources. This malicious approach of the blackhole node attracts all the traffic of the network to that malicious node which then drops or modifies them all. A Grayhole attack is a variation of Blackhole attack, where an adversary first behaves as an honest node during the route

discovery process, and then silently dumps the received data packets without forwarding to the next hop towards the destination even in congestion less scenario. Detection of Grayhole attack is harder because nodes can drop packets partially not only due to its malicious nature but also due to shortage of resources, selfish nature or network congestion.

Network security is usually based on encryption and authentication frameworks. On the other hand, such schemes are not always enough to counter the insider attacks launched by compromised nodes. There comes a need for intrusion detection systems (IDS) [4]. IDS can constitute a second wall of defence and their role is critical since the majority of MANETs will be deployed in unreceptive environments in which legitimate nodes can be captured and operated by the attackers. Nodes that are equipped with IDS's operate in promiscuous mode and monitor the traffic sent or received by their neighbours in order to detect malicious activities. There exist two Intrusion detection systems which are popularly being used. One among them is Host-based intrusion detection system (HIDS) which run on each host by focusing on collecting data through operating system audit logs and the other one is Network-based based intrusion detection system (NIDS) [5] which do not run on each host but on cluster heads of regions within the MANET.

In our work, we propose an innovative approach to detect Blackhole and Grayhole attacks using HIDS approach by maintaining memory caching mechanism at each node. In order to detect the malicious activities HIDS sensors analyze the received data. Thereafter, actions will be initiated automatically in order to stop the attack. While the mechanism presented in this paper applies to almost all ad hoc protocols, but we have designed the proposed approach keeping in mind the AODV protocol [6].

The organization of the rest of this paper is as follows. The related work of the proposed approach is briefed in section 2. We present AODV protocol in section 3. In section 4 the blackhole and grayhole attack scenarios are briefly discussed. In section 5 the proposed method is discussed. The simulation environment is presented in section 6. The results analysis, conclusion for the present work is discussed in sections 7, 8 respectively. Finally the future scope of this proposed approach is presented in section 9.

II. RELATED WORK

The proposed method SEA aims to find the secured routes by preventing the MANET from the two popular Denial of service attacks called black hole and grayhole attacks by using memory caching mechanism to inspect the large differences among the sequence numbers of nodes who have sent back the Route Reply (RREP) packets. The authors proposed a technique for detecting the group of adversary nodes i.e. blackhole node and grayhole nodes in ad hoc networks in reference paper [7]. In [8], the authors proposed an innovative approach that requires a source node to wait until three or more RREP packets to arrive from the neighboring nodes. The authors analyzed the impact of blackhole attack on MANET and proved that a blackhole node is randomly assigning huge destination sequence number without looking into the available to convince the source node in [9]. In [10], an algorithm based on course based scheme has been proposed by Disha et al to observe every node in a selected route path to counter the malicious attacks.

III. AODV ROUTING PROTOCOL

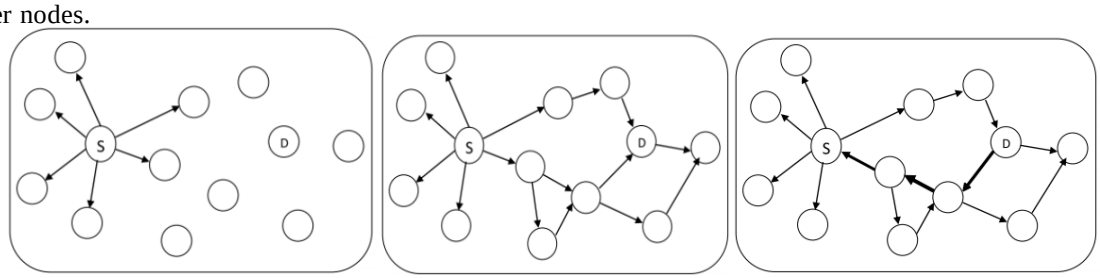
AODV is an on demand driven protocol whose route discovery process is also reactive on an as needed basis. It works in two phases i.e. Route discovery phase and Route maintenance phase. It uses Route Request (RREQ), Route Reply (RREP) control messages in Route Discovery phase and Route Error (RERR) control message in Route Maintenance phase. The header information of this control messages can be seen in detail in [11]. The example to describe the route discovery process is illustrated in Fig 1. Fig 1(a) depicts that node S sends out a route request packet to find a path to node D. Fig 1(b) shows that the route request is forwarded throughout the network, each node adding its address to the packet. Fig 1(c) presents how the node D then sends back a route reply to S using the path contained in one of the route request packet that reached it. The thick lines represent the path the route reply takes back to the sender.

Source node sends RREQ packets to all its immediate neighbors. If any of the next-hop neighbors itself is the destination node then it sends control RREP packet to the sender node. If it is not the case then the nodes check their routing tables whether it has route entry for the destination. If yes, they send the control message RREQ to their next hop neighbors. The same process will continue until the destination node is reached or an intermediate node having an entry in its routing table database for a fresh route to the destination. If not, it forwards the RREQ packet by broadcasting it to its neighbors.

If its routing table contains an entry to the destination, then node compares the Destination Sequence Number (DNN) in its routing table to that present in the control message RREQ packet as a next

step. This DNN is the sequence number of the last sent packet from the destination to the source. If the DNN present in the routing table is higher than the one contained in the RREQ packet, then it denotes that the route is a fresh route and packets can be sent through this route. This intermediate node then sends a control RREP packet to the node through which it received the RREQ packet. The RREP packet gets forwarded back to the source through the reverse route. The source node then modifies its routing table and sends its packets through this new identified route. If it is not the case the node relays the request further to its neighbours in the process of finding destination.

During the operation, in route maintenance phase, if any node identifies a link failure it sends a Route ERROR (RERR) packet to all other nodes that uses this link for the purpose of making communication to other nodes.



1(a) 1(b) 1(c)

Fig 1. Example Route request and Route reply scenario in Mobile ad hoc networks

Every mobile node in AODV would send Ciao messages periodically to facilitate each node to know about its one-hop neighboring nodes. If anyone of the node fails to receive a Ciao message from a neighbor node within a timeout time then it sends Route Error control message to all the nodes recorded in its routing table. After receiving the Route Error control message the received nodes updates their database indicating that particular node as the disappeared node and would remove the compromised route from their routing tables.

Despite its excellent packet delivery of more than 99% the AODV routing protocol has a limitation to fight the threat of black hole and grayhole attacks. This is due to the fact that AODV protocol has been developed without considering security mechanisms in advance hence allowing the malicious nodes to forge a sequence number and hop count in the routing message during the route searching phase there by winning a chance to get hold of the route, eavesdropping or sinking all data packets as they go by.

IV. BLACKHOLE AND GRAYHOLE ATTACKS IN MANET

Blackhole attack is one of the most active DoS attack since it disrupts routing services in the network [12]. The blackhole attacker go ahead with an approach by aerating itself having a valid shortest path to attract all traffic in the network towards it with a malicious intent of blocking data packets. In Fig 1, the source node **S** initiates a route by spreading the RREQ message for the destination D. If a black hole node receives this RREQ packet then it responds in no time with a fake RREP packet by inserting high sequence number without looking into available resources. The source node S perceives this message as if it comes from a node which has a shortest as well as fresh route to the destination or from the destination itself. Then blackhole node may get the opportunity to deceive the source node by initiating it to send the data packets on that route. Then black hole node simply drops the data packets instead of relaying. This type of attack is creating a blackhole that absorbs everything but giving nothing.

Another significant DoS attack which also may disrupt the network routing services is the grayhole attack [13]. Grayhole attack is just a continuation of blackhole attack in which adversary activities and behaviours are remarkably volatile in nature. In this, grayhole node aerate as if as a honest node during route discovery phase and silently may drop some of the received packets even in the congestion less scenario or forward packets according to the convenience. This grayhole node disrupts the route discovery process and degrades the performance of network. The grayhole attack is more difficult to detect than blackhole attack as it is not exhibiting the malicious behavior all the times. A gray hole may exhibits its malicious behavior on only some specific nodes or on timely basis that is with various techniques. Broadly grayhole attacks may be categorized into three types as follows.

from certain specific nodes in network, while forwarding all packets for other nodes.

2. Grayhole attack on time basis: In this type of grayhole attack a grayhole node behave maliciously for some time duration with the intention of dropping packets and all other times it behaves like a normal node.

3. Grayhole attack on node and time basis: This attack may exhibit a behavior which is a combination of above two, making detection of attack more difficult.

V. PROPOSED METHODOLOGY

In this proposed work, every mobile node in MANET is enabled with Intrusion Detection System (IDS), which is mainly used to estimate the apprehensive value of a node according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. When an apprehensive value exceeds a threshold, a chunk message is broadcasted by nearby IDS, giving notice to all nodes on the network to cooperatively isolate the malicious node. The chunk message contains the Identification Number (IN) of issuing node IDS, the IN of identified malicious node, and the time instant of identification. Upon receipt of a chunk message issued by IDS, normal nodes will place the malicious node on their blacklists, thus, the AODV routing protocol for normal nodes must be slightly revised.

If IDS detects a malicious node, it will broadcast the identification number of malicious node, through a chunk message, to all nodes within its radio transmission range. When a normal node receives a chunk message, the identification number of the malicious node is added to the chunk table labeled as Table 1. The table 1 lists malicious Node 2 identity, as issued by IDS_1; and malicious Node 5 identity, as issued by IDS_2, as well as their timestamps. Every normal node must verify the chunk messages from IDSs before updating its own chunk table.

Table 1.Table to spread the chunk messages

IDS	Malicious Node	Time stamp	
IDS-1	2	09-12-2013	22:26:00
IDS-2	5	09-12-2013	22:29:00

The implemented routing algorithm SEA for normal nodes is basically the same as AODV, with the exception that, intermediate nodes may not reply to RREQs; the difference lies in that: 1) one chunk table is added in addition to a routing table, and is used to record a list of malicious nodes. 2) When receiving a chunk message broadcasted by IDS, a normal node will add the malicious node stored in the chunk message into the chunk table 3) when forwarding a RREP packet, a normal node will drop a RREP if its neighboring node that forwards the RREP is found in the chunk table.

Table 2. RRR Table

Route			Maximum hop count	Broadcasting nodes	Expiration Time
Source	Destination	Source sequence			
3	7	7004	4	4,10,13	11:10:22
8	9	2015	7	3,11,15,14	11:11:34.

Apart from Chunk and Routing tables the proposed Implementation SEA employs two more tables, which are RRR and RAN tables, as shown in Table 2 and 3. The RRR table records RREQ messages of a watched IDS node within its radio transmission range, for instance, the first row in Table **2** indicates RREQ for (source node, destination node, source sequence) = (3, 7, 7004), wherein, the IDS has observed that nodes 4, 10, and 13 broadcasted this RREQ with a maximal hop count of 4. The RAN table is used for an IDS node to record the apprehensive values of nodes within its radio transmission range. The apprehensive value of a node is an important benchmark to judge a malicious node. In principle, if an intermediate node is not the destination node, and it never broadcasts a RREQ for a specific route, but forwards a RREP for the route, then its apprehensive of node 6 in Table 3 is 2, which does not exceed the threshold thus it is considered as in an inactive state. On the other hand the apprehensive value of node 4 is 4, which is assumed as having reached the threshold thus it is in an active state and blocked.

Table 3. RAN Table

Node ID	Apprehensive Value	Status
14	1	inactive
4	4	active
6	2	inactive

VI. SIMULATION ENVIRONMENT

We introduced a new routing protocol called SEA (Security Enabled AODV) as an enhancement to

the conventional routing protocol Ad hoc On-demand Distance Vector (AODV) protocol to counter the blackhole and grayhole attacks in Mobile Ad hoc Networks. The problem is investigated by means of collecting data available resources and simulation which gives some results. Further these simulation results are properly analyzed for making decisions on their basis. The simulations are carried out using the popular discrete event network simulator NS2 (V 2.35) in Ubuntu-12.04 [14, 15] operating environment. The NS2 facilitates the users to create their own routing protocols according to the requirement and compare its performance with the existing protocols. To evaluate the performance of a protocol for an ad hoc network, it is necessary to analyze it under practical conditions, especially including the movement of mobile nodes. Simulation requires setting up traffic and mobility model for performance evaluation. Table 4 shows the parameters that have been used in performing simulation.

Table 4: Simulation Parameters

Parameters	Value
Simulator	Ns-2.35
Data packet size	512 byte
Simulation time	200 sec
Environment size	500 x 500
Number of nodes	Ranging between 20 to 100
Transmission range	250m
Pause time	0 s
Observation parameters	Packet Delivery Ratio, End-to-end delay, Throughput, Normalized overhead
No. of malicious node	4 (2 black hole nodes and 2 grayhole nodes)
Traffic Type	CBR Traffic
Mobility	10 m/s
Routing Protocols	AODV and SEA

6.1 Mobility Model

There exists a variety of mobility models proposed by Sanchez and Manzoni [16], what we have implemented in our simulation is the random waypoint mobility model. A mobility model is used to describe the movement of a mobile node its location and speed variation over time while the simulation of a routing protocol. The random waypoint mobility model proposed by Maltz and Johnson [17] is the popular model that is widely implemented & analyzed in simulation of routing protocols because of its availability and simplicity. At the start of the simulation each mobile node waits for a specified time called pause time, **p** and randomly selects one location. A mobile node chooses a new random destination after staying at its previous position for a time period of **p** till its expiry. A node travels across the area at a random speed distributed uniformly from v0 to vmax where v0 and vmax represent the minimum and maximum node speeds. This process of choosing random destination at random speed is repeated again and again until the simulation is finished. That is we are free to select the direction, destination and speed of a node irrespective of the one-hop nodes.

6.2 Performance Analysis

The two protocols AODV and SEA are compared by evaluating the following QOS performance parameters.

- **Packet Delivery Ratio** - It is the ratio of number of packet received by destination to the number packet originated from source.

$$PDF = (P_r / P_s)$$

Where P_r is total Packet received and P_s is the total Packet sent.

- **Throughput or Network throughput** - It is the average rate of successful packet delivery over a communication network.
- **Average end-to end delay-** It is defined as the time taken for a data packet to be transmitted across MANET from source to destination.

$D = (T_r - T_s)$

- **Normalized Routing Overhead -** It can also be defined as the ratio of routed packets to data transmissions in a single simulation. It is the routing overload per unit data delivered successfully to the destination node.

6.3.***Experimental Setup***

The simulation scenario and parameters used for performing the detailed analysis of Black hole attacks on MANET routing protocols is mentioned below. This section describes the how the performance parameters have been evaluated to simulate the routing protocols.
Following files have been used for simulation.

- **Input to Simulator**: Connection and Traffic pattern files, Simulation TCL files
- **Output File from Simulator**: Trace file, Network Animator file
- **Output from Trace Analyzer**: Gnuplot file

To generate the connection pattern scenario and traffic movement file the following example command is used.

Generation of connection pattern scenario file:

Ns cbrgen.tcl [-type cbr / tcp] [-nn nodes] [-seed seed] [-mc connections] [-rate rate] > scenario file

Here type - traffic type (cbr /tcp), nn – no. of nodes, seed - 1.0 for cbr traffic and 0.0 for tcp traffic, mc – number of mobile connections, rate – packet input rate, simulation time, and x, y – grid size.

Generation of Traffic pattern Scenario File:

./setdest -n <num_of_nodes> -p <pause time> -s <Maxspeed> -t <simtime> -x <maxx> -y <maxy> Scenario file
Here n – no. of nodes, p – pause time, s – speed, t -simulation time, and x, y – grid size.

6.4. Analysis using Trace Analyzer

After performing simulation, trace files are generated. Trace file contains the information of Send/Receive Packet, Time, Traffic Pattern, Size of Packet, Source Node, Destination Node and etc. Gawk script trace analyzer is used to analyze trace output from simulation. When files are analyzed using this trace analyzer an output Gnuplot is used to generate the graphs.

VII. RESULTS & DISCUSSIONS

Using outputs from Gawk script the following graphs and results are generated using Gnuplot.

7.1. Packet Delivery Ratio

Simulation results of Fig. 2 show that under malicious attack the packet delivery ratio of SEA is approximately doubled (40%) as compared to AODV (20%) under black hole attack.

7.2. End To End Delay

Simulation results in Fig. 3 show that SEA has less end to end delay than AODV routing protocol under black hole attack.

7.3. Normalized Routing Overhead

Simulation results in Fig.4 show that SEA has a lower normalized routing overhead as compared to AODV routing protocol under black hole attack.

7.4. Throughput

Simulation results in Fig. 5 show that under malicious attack the throughput of SEA is increased by 60% of as compared to AODV under malicious attack.

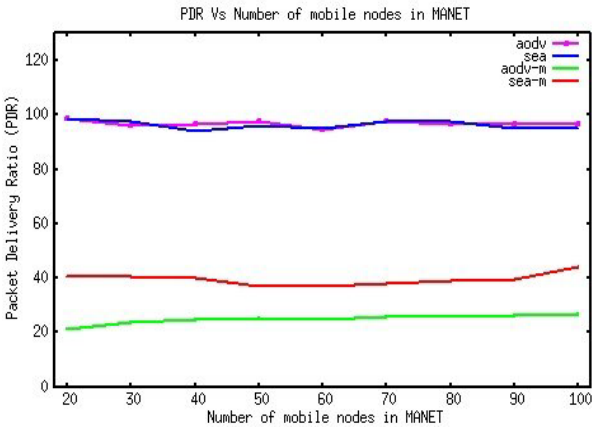


Fig.2. PDR versus number of nodes

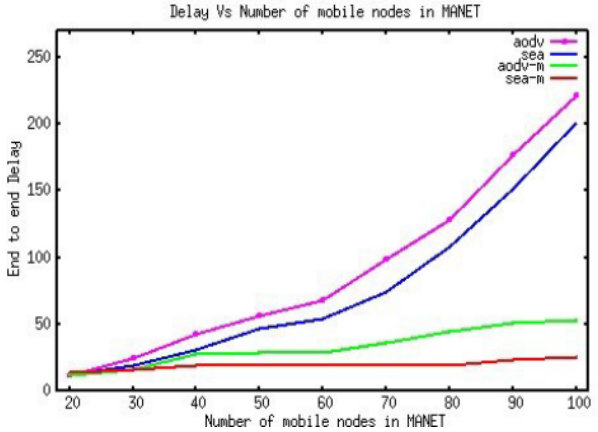


Fig.3 Delay versus number of nodes.

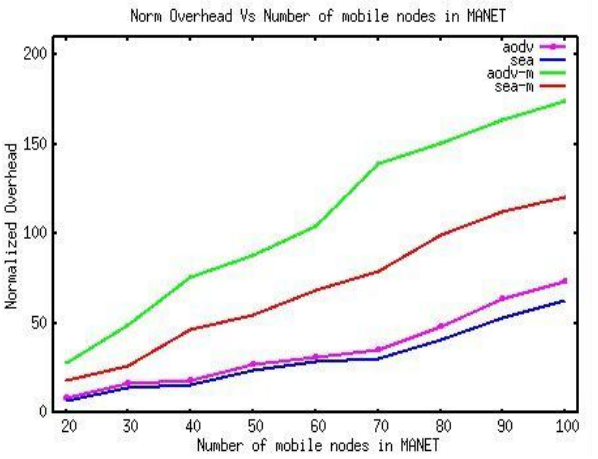


Fig.4. Norm overhead versus number of nodes

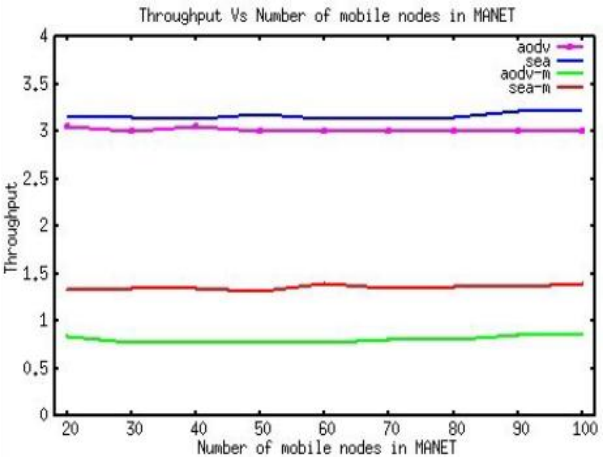


Fig.5 Throuput versus Number of nodes

Simulation results show the average values for each QOS parameter as discussed above with respect to number of mobile nodes in MANET. It has been observed from the simulation results that when the protocols are under attack of blackhole nodes and grayhole nodes, SEA is less affected than AODV. We analyzed that under the attack scenario the proposed implementation outperforms the conventional AODV in terms of packet delivery ratio. The simulation results also proved that the proposed protocol also producing better throughput as compared to AODV in the attack scenarios. Further the values for average end-to-end delay are also reduced to a greater extent in SEA in the attack scenario when compared to AODV. Whereas there is a slight increase in the routing overhead this is quite negligible. But there is a positive aspect for SEA even with regards to control overhead. The SEA consumes less overhead per received packet which is called Normalized overhead than AODV.

VIII. CONCLUSION

In this paper, we have analyzed the Black hole and grayhole attack on AODV routing protocol and the proposed routing protocol SEA with respect to different performance parameters such as Packet Delivery Ratio, End-to- end delay, Throughput and Normalized overhead. The SEA is proposed with an objective to detect and defend against the blackhole and grayhole nodes by deploying Intrusion Detection Systems in MANETs. When the apprehensive value of a node exceeds a predefined threshold, a chunk message is broadcasted by the detected IDS to all nodes on the network in order to cooperatively isolate the malicious node. We have analyzed the vulnerability of two protocols AODV and SEA under different network scenarios and traffic patterns against Blackhole and grayhole attacks. The Simulation results showed that SEA performs better than AODV against all QOS parameters. For detailed report one can go through the results analysis part in section 6.

IX. FUTURE SCOPE

Simulation can be performed by using other existing parameters. This work contains simulation based on random mobility model only. Other mobility models can also be studied and behavior of protocols can be analyzed. Black hole and grayhole attacks are needed to be analyzed on other existing MANET routing protocols such as DSDV, ZRP, and DSR etc. Also attacks other than Blackhole and grayhole such as Wormhole shall be considered for further research. Mobile Ad hoc Networks are open to both the external and internal attacks due to lack of any centralized security system. In this paper attempt is made only to counter the internal attacks so further research can be carried out as an extension to the present work by considering some cryptography security framework to defend the external attacks.

REFERENCES

[1]. Tanu, Satinder and Das "Security Threats in Mobile Adhoc Network: A Review" in IJCNWC, Vol. 2, No. 1, 2012
[2]. Supriya and Manju "Manet Security Breaches: Threat to a Secure Comm. Platform" IJANS, Vol. 2, No. 2, April 2012.
[3]. Nisha, Simranjeet Kaur, Sandeep AroraJose "Analysis Of Black Hole and Gray Hole attack On RP- AODV In MANET", IJERT, ISSN:2278-0181, Vol. 2 Issue 8, Aug - 13.
[4]. Sharmila, Muruga, "A recent secure intrusion detection system for Manets", ICISC-2013, Vol 3, Special Issue 1.
[5]. F Richard, Helen, Bu and, Du "Security and quality of service (QoS) co-design in cooperative mobile ad hoc networks", JWCN (Springer journal), 2013.
[6]. Nisha P John "A New Approach for the Detection of Black hole Nodes in AODV Based Mobile Ad-Hoc Networks", IJERT, Vol. 2 Issue 1, January- 2013, ISSN: 2278-0181.
[7]. H.Deng; W.Li; D.Agarwal, "Routing security in wireless ad hoc networks", [J]. Communication Magazine, IEEE, (2002), 70-75. [8]. Lakshmi, Priya, Jeeva, Rama, Thilagam "Modified AODV Protocol against Blackhole Attacks in MANET", IJET, Vol.2, 2010.
[9]. Satoshi, Nakayama,Yoshiaki "Detecting Blackhole Attack on AODV-based MANETs by Dynamic Learning Method", IJNS, Vol.5, No.3, PP.338–346, Nov. 2007.
[10] Disha G.Karriya, Atul B. Kathole, Sapna R.Heda, "Detecting black and gray hole attacks in mobile ad hoc network using an Adaptive method", IJTAE, 2012.
[11]. C. Perkins. "Request for Comments (RFC) -3561", Category: Experimental, Network, Working Group, July 2003.
[12]. J. Luo, M. Fan, D. Ye, "Black hole attack prevention based on authentication mechanism," 11th IEEE Singapore ICCS, pp. 173-177, Guangzhou, 19-21 Nov. 2008.+++
[13]. Nisha, Simranjeet Kaur, Sandeep "Analysis Of Black Hole And Gray Hole Attack On RP- AODV In MANET", IJERT, ISSN: 2278- 0181, Vol. 2 Issue 8, August – 2013.
[14] www.isi.edu/nsnam/ns/tutorial Marc Greis tutorial on ns2 [15] Matthias Transier "Ns2 tutorial running simulations"
[16]. Tracy Camp, Jeff Boleng and Vanessa Davies, "A survey of Mobility Models for Ad hoc Network Research", WCMC-special issue, vol 2, No5, 2002.
[17]. Tracy Camp, Jeff Boleng and V Davies, "A survey of Mobility Models for Ad Hoc Network Research", Feb 15, 2007.

Prabhakara Reddy Baggidi received B.Tech degree in Electronics and Communication Engineering in the year 1997 from SV University, Tirupathi, India. He is awarded with M-Tech degree in Digital Systems & Computer Electronics in the year 2002 and currently carrying out Ph.D work in association with Jawaharlal Nehru Technological University, Anantapur, India. He guided many academic projects for the last 15 years of teaching experience. His research interests are in the field of Mobile Ad hoc Networks and Optical Networks.

Dr. M. N. Giri Prasad is currently working as Professor and HOD, Dept. of ECE, JNTUA, Andhra Pradesh, India. He received B.Tech degree from JNTU College of Engineering, Anantapur, Andhra Pradesh, India in 1982, M.Tech degree from Sri Venkateshwara University, Tirupathi, and Andhra Pradesh, India in 1994 and Ph.D. degree from J.N.T University, Hyderabad, and Andhra Pradesh, India in 2003. He is having 85 National and International publications to his credit. He is the member of IE (India), Member of ISTE, and NAFEN. His areas of research are Signal & Image Processing, Microcontroller Applications, and Embedded Systems.