SIMULATION OF SECURE AODV IN GRAY HOLE ATTACK FOR MOBILE AD-HOC NETWORK

Onkar V. Chandure[1], Aditya P. Bakshi[2], Saudamini P. Tidke[3], Priyanka M. Lokhande[4]
[1&2]Asst. Prof. Department of I.T., J.D. Institute of Engg. & Technology,Yavatmal, India
[3]MTech –IT (Scholar) TIT Engg, Bhopal, India
[4]ME –CSE (Scholar) Sipna COET, Amravati, India

ABSTRACT

A MANET is an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways and interface with a fixed network. Its nodes are equipped with wireless transmitters/receivers using antennas which may be omni directional (broadcast), highly-directional (point-to-point), or some combination thereof. At a given time, the system can be viewed as a random graph due to the movement of the nodes, their transmitter/receiver coverage patterns, the transmission power levels, and the co-channel interference levels. In this, paper, we are focusing on the concept of gray hole attack in adhoc network & impact of gray hole attack on network. 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. Because of the gray hole attack on the network there is an impact on the different performance metrics of the network such as PDR, e2edelay, throughput etc. Our mechanism helps to protect the network by detecting and reacting to malicious activities of any node. 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: *Mobile ad hoc network, Routing Protocol, Security in MANET, Gray Hole node.*

I. INTRODUCTION

A Mobile ad-hoc network is a network [1] formed without any central administration which consists of mobile nodes that use a wireless interface to send packet data. These attacks can be classified into two categories, attacks on Internet connectivity and attacks on mobile ad hoc networks. Ad-Hoc network [2] is a wireless network without having any fixed infrastructure. Each mobile node in an ad-hoc network moves arbitrarily and acts as both a router and a host. A wireless ad-hoc network consists of a collection of "peer" mobile nodes that are capable of communicating with each other without help from a fixed infrastructure. The interconnections between nodes are capable of changing on a continual and arbitrary basis. Nodes within each other's radio range communicate directly via wireless links, while those that are far apart use other nodes as relays. Nodes usually share the same physical media; they transmit and acquire signals at the same frequency band. However, due to their inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks. Ad-hoc networks are more vulnerable than wired.
Wireless networks are typically much easier to snoop on, as signals go through the air and only physical
Proximity is required to gain access to the medium. Mobile ad hoc network (MANET) is a class of wireless networks with no fixed infrastructure (or base stations) and is formed on ad hoc basis. Peer-

to-peer routing is done in these networks; the absence of any central authority makes MANETs more vulnerable to various forms of attacks than a typical wireless network. The impromptu nature of the MANETs formation makes it hard to distinguish between trusted and untrusted nodes. The dynamic nature of MANETs makes the trust relationship between nodes also change. Routing is one of the most basic networking functions in mobile ad hoc networks. Hence, an adversary can easily paralyze the operation of the network by attacking the routing protocol. This has been realized by many researchers and several "secure "routing protocols have been proposed for ad hoc networks. However, the security of those protocols has mainly been analyzed by informal means only.

In this, we are focusing on the concept of gray hole attack in adhoc network .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.

The MANET security can be classified in to 5 layers, as Application layer, Transport layer, Network layer, Link layer, and Physical layer. However, the focus is on the network layer, which considers mainly the security issues to protect the ad hoc routing and forwarding protocols. When the security design perspective in MANETs is considered it has not got a clear line defense. Unlike wired networks that have dedicated routers, each mobile node in an ad hoc network may function as a router and forward packets for other peer nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. In order to achieve this goal, the security approach should provide overall protection that spans the entire protocol stack. But sometimes the security protocol may not be able to meet the requirements as said above and results in a packet forwarding misbehavior.

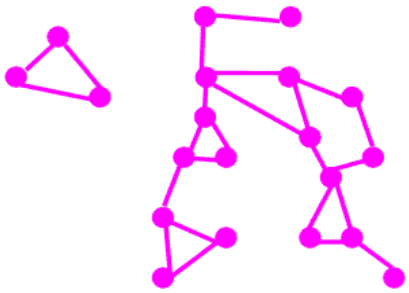

Figure 1: Basic Idea about the MANET Structure

II. LITERATURE REVIEW & RELATED WORK

Extensive research has been done in the MANET area. Reliable network connectivity in wireless networks is achieved if some counter measures are taken to avoid data packet forwarding against malicious attacks in MANET. A lot of research has taken place to avoid malicious attackers. In this section we mainly focus on the analyzing & defend the system from malicious impact of different attacks on MANET. Secure ad hoc routing protocol has been proposed as a technique to enhance the security in MANET.

S.Ramaswamy *et. al*. [3] presented an algorithm to prevent the co-operative black hole attacks in ad hoc network. This algorithm is based on a trust relationship between the nodes, and hence it cannot tackle gray hole attacks. According to their algorithm instead of sending the total data traffic at once, they divide it into small sized blocks, in the hope that the malicious nodes can be detected& removed in between transmission.

Marti *et al* [4] proposed to trace malicious nodes by using watchdog/pathrater. In watchdog when a node forwards a packet, the node's watchdog verifies that the next node in the path also forwards the packet by promiscuously listening to the next node's transmissions.

Gonzalez *et al* [5] presents a methodology, for detecting packet forwarding misbehavior, which is based on the principle of flow conservation in a network. The problem of security and cooperation enforcement has received considerable attention by researchers in the ad hoc network community.

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 [6],

Papadimitratos and Hass [7], Snazgiri [8]. Buttyan and Hubaux [9] have presents a self organized PGP-based mechanism to authenticate nodes using chains of certificates and transitivity of trust.
Zeshan [10] proposed a two-fold approach for detection and isolation of nodes that drops data packets. Usha and Radha [11] proposed extension to the TWOACK scheme, in which each node must send back a normal Ack to its immediate source node after receipt of any kind of packet. This scheme requires an end to end Ack packet (i.e. Nack) to be sent between the source and the destination.
S.Banerjee *et al* [12] has also proposed an algorithm for *detection & removal of Black/Gray Holes*. According to their algorithm instead of sending the total data traffic at once, they divide it into small sized blocks, in the hope that the malicious nodes can be detected& removed in between transmission. Flow of traffic is monitored by the neighbors of each node. Source node uses the acknowledgement sent by the destination to check for data loss & in turn evaluates the possibility of a black hole. However in this mechanism false positives may occur and the algorithm may report that a node is misbehaving, when in fact it is not.

III. ROUTING PROTOCOLS

The primary goal of routing protocols in ad-hoc network is to establish optimal path (min hops) between source and destination with minimum overhead and minimum bandwidth consumption so that packets are delivered in a timely manner. A MANET protocol should function effectively over a wide range of networking context from small ad-hoc group to larger mobile Multihop networks. As fig shows the categorization of these routing protocols. Routing protocols can be divided into proactive, reactive and hybrid protocols, depending on the routing topology.

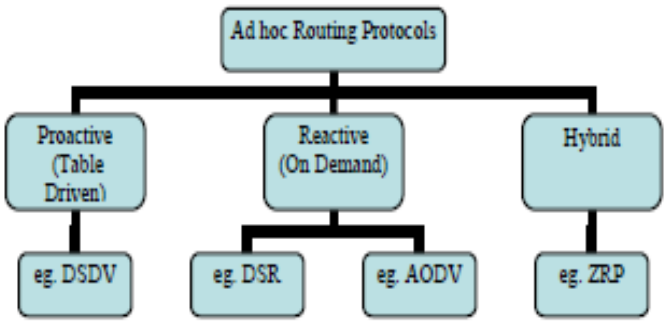

Figure 2: Hierarchy of Routing Protocols

3.1 Reacting Routing Protocol

Reactive routing protocols [13] are on-demand protocols. These protocols do not attempt to maintain correct routing information on all nodes at all times. Routing information is collected only when it is needed, and route determination depends on sending route queries throughout the network. The primary advantage of reactive routing is that the wireless channel is not subject to the routing overhead data for routes that may never be used. While reactive protocols do not have the fixed overhead required by maintaining continuous routing tables, they may have considerable route discovery delay. Reactive search procedures can also add a significant amount of control traffic to the network due to query flooding. Because of these weaknesses, reactive routing is less suitable for real-time traffic or in scenarios with a high volume of traffic between a large numbers of nodes.

3.2 Proactive Routing Protocol

In a network utilizing a proactive routing protocol, every node maintains one or more tables representing the entire topology of the network. These tables are updated regularly in order to maintain up-to-date routing information from each node to every other node. To maintain the up-to-date routing information, topology information needs to be exchanged between the nodes on a regular basis, leading to relatively high overhead on the network. On the other hand, routes will always be available on request. Many proactive protocols stem from conventional link state routing, including the Optimized Link State Routing protocol (OLSR).

3.3 Hybrid Routing Protocol

Wireless hybrid routing is based on the idea of organizing nodes in groups and then assigning nodes different functionalities inside and outside a group [13]. Both routing table size and update packet size are reduced by including in them only part of the network (instead of the whole); thus, control overhead is reduced. The most popular way of building hierarchy is to group nodes geographically close to each other into explicit clusters. Each cluster has a leading node (*cluster head*) to communicate to other nodes on behalf of the cluster. An alternate way is to have implicit hierarchy. In this way, each node has a local scope. Different routing strategies are used inside and outside the scope. Communications pass across overlapping scopes. More efficient overall routing performance can be achieved through this flexibility. Since mobile nodes have only a single Omni directional radio for wireless communications, this type of hierarchical organization will be referred to as logical hierarchy to distinguish it from the physically hierarchical network structure.

IV. GRAY HOLE ATTACK

Gray Hole attack [14] may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface. A Gray hole attack is a variation of the black hole attack, where the malicious node is not initially malicious, it turns malicious sometime later. The gray hole attack has two phases. In the first phase, 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. In the second phase, 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 certainly. A gray hole may exhibit its malicious behavior in different ways. It may drop 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 node may behave maliciously for some time duration by dropping packets but may switch to normal behavior later.

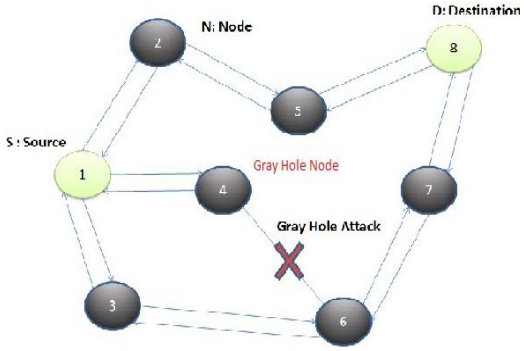

Figure 3: Example of Gray Hole Attack

Fig 3, shows the example of gray hole attack on the adhoc network. In this figure node 1 is act as a source node, node 8 act as a destination node. Node 4 represents the gray hole node in above diagram .Node 4 takes the packets from the neighboring node and drop the certain packets during the packet transmission.

4.1 Impact of Gray Hole Attack on Adhoc Network

When there is a gray hole attack occur in the adhoc network, performance of adhoc network gets decreases. Gray hole attack decreases certain performance metrics of the network such as packet delivery ratio, end to end delay & packet loss ratio.

- Packet delivery ratio (PDR): is nothing packet send at the source to the packet receive at the destination.
  PDR =Ps/Pr
- End to end delay (e2e): it refers to the time taken for a packet to be transmitted across a network from source to destination.
  End to end delay D =Td-Ts
  Where Td is the packet receive at the destination
  Ts –Packet send at the source node

- Packet loss ratio: is where the network traffic fails to reach at the destination in a timely manner.
  Packet dropped/loss, Pd= Ps-Pa

4.2 Method for Gray Hole Node or Suspected node

This method is useful to find out the suspected or malicious behavior of any node during the adhoc network. This method helps us in recognizing as well as prevent from the suspected node.
DSN-Destination Sequence Number, NID- Node –Id, MN-ID – Malicious Node ID.

Level 1: Initialization Phase of Process or starting phase of process
Retrieve the current time
Add the current time with BCAST_ID_SAVE
Level 2: Storing Process
Store all the Route Replies DSN and NID in RR-Table
Repeat the above process until the time exceeds
Level 3: Identify and Remove Malicious /Suspected / Gray Hole Node
Retrieve the first entry from RR-Table
"rrep_lookup" function is for looking any RREP message up if it is exist
"rrep_remove" function is for removing any record for RREP message that arrived from defined node
"rrep_purge" function is to delete periodically from the list if it has expired.
Discard or remove the entry from RR-Table and store its NID and Update table
Level 4: Proper selection of node process
Select the NID having highest DSN among RR-table entries
Level 5: Continue default process
Call Receive Reply method of default AODV Protocol
The above algorithm starts from the initialization process, first set the waiting time for the source node to receive the RREQ coming from other nodes and then add the current time with the waiting time. Then in storing process, store all the RREQ Destination Sequence Number (DSN) and its Node Id in RR-Table until the computed time exceeds. Generally the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely that node is the malicious node, immediately remove that entry from the RR-Table. This is how malicious node is identified and removed. Final process is selecting the next node id that has the higher destination sequence number, is obtained by sorting the RR-Table according to the DSEQ-NO column, whose packet is sent to Receive Reply method in order to continue the default operations of AODV protocol.

V. EXPERIMENTAL RESULTS & DISCUSSION

We are mainly focusing on the issue of gray hole attack detection & prevention or malicious node behavior .Result is analyzed by the comparing the performance metrics of the normal AODV, gray hole attack & SAODV.

5.1 Simulation Parameters for AODV, Gray Hole & SAODV

Evaluation is done by keeping total Simulation time constant and varies the number of mobiles nodes used in the network. For e.g. if total simulation time is 200 ms then this time is constant only there is a variation in the nodes value.

Table I: Simulation Parameters for Ad-Hoc Network

Simulator	Ns-2 (Version 2.32)
Simulation Time	200 (s)
Number of mobile nodes	10,20,30,40,50
Topology	700 * 700 (m)
Routing Protocol	AODV
Traffic	CBR (constant bit rate)
Transport Protocol	TCP & UDP
Packet Size	512 bytes

5.1.1 Evaluation of Packet Delivery Ratio for Normal AODV

In this, the packet delivery ratio is calculated for normal aodv protocol with different mobile nodes. (Simulation time 200 s)

Table II: Number of Nodes & PDR for AODV

Nodes	10	20	30	40
PDR	91.60	95.89	97.03	95.20

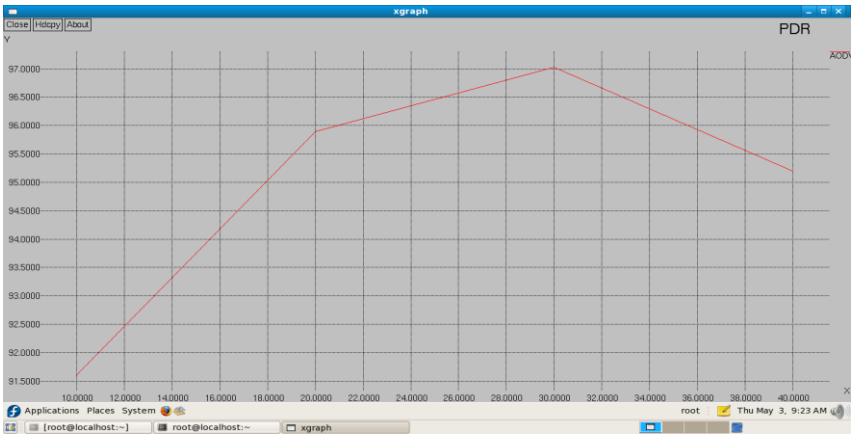

Figure. 4: Number of Nodes & PDR for AODV

5.1.2 Evaluation of Packet Delivery Ratio for Gray Hole Node

In this, the packet delivery ratio is calculated for gray hole node with different mobile nodes. (Simulation time 200 s)

Table III: Number of Nodes & PDR For Gray Hole Node

Nodes	10	20	30	40
PDR	86.41	80.70	94.00	95.20

From the table, we can clearly identified the packet delivery ratio is degrade after the gray hole attack in the adhoc network. Because the gray hole attacks drop the data packets during the transmission but with no fixed probability of losing the data packets. if we change the simulation time then again there is a change in the PDR values. If the values of nodes are increases then it required more time for simulating the network.

5.1.3 Evaluation of Packet Delivery Ratio for SAODV

In this, the packet delivery ratio is calculated with different mobile nodes. (Simulation time 200 s). In this, we are improving the packet delivery ratio of the network as well as secure the network from the gray hole attack. Result shows the improvement in PDR when compared with gray hole attack.

Table IV: Number of Nodes & PDR For SAODV

Nodes	10	20	30	40
PDR	95.66	81.39	94.46	98.40

5.1.4 Comparison of Packet Delivery Ratio for AODV, Gray Hole & SAODV (200 S)

Table V: Number of Nodes & PDR for AODV, Gray Hole & SAODV

Nodes	AODV	Gray Hole	SAODV
10	91.60	86.41	95.66
20	95.89	80.70	81.39

30	97.03	94.00	94.46
40	95.20	95.20	98.40

From the table V, we can clearly identified that there is a much more increase in the PDR values, after the gray hole attack there is drop of packets but because of the SAODV procedure there is a increment in the PDR values as well as improvement in the performance of the network.

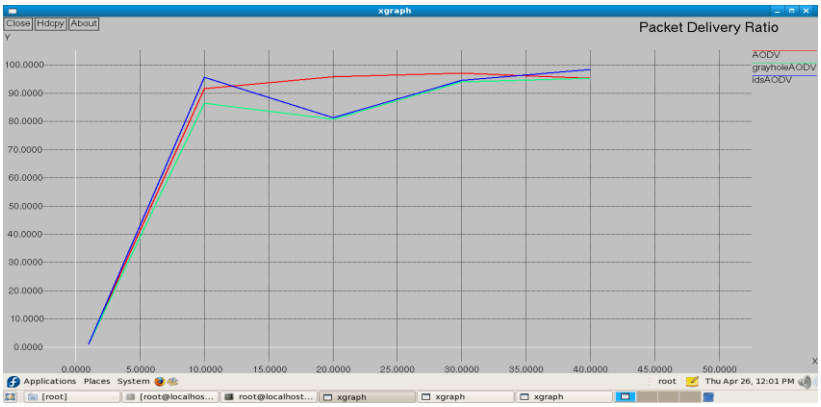

Figure 5: Number of Nodes & PDR for AODV, Gray Hole & SAODV

5.1.5 Evaluation of End to End Delay for AODV, Gray Hole & SAODV

e2e delay is calculated for normal aodv protocol with different mobile nodes(simulation time 200 s).

Table VI: E2e Delay for Normal AODV, Gray Hole & SAODV

Nodes	AODV	Gray Hole	SAODV
10	0.00724547	0.00763422	0.0111809
20	0.00315586	0.00801343	0.0121467
30	0.0315781	0.0139475	0.0173508
40	0.0166477	0.0166477	0.0200695

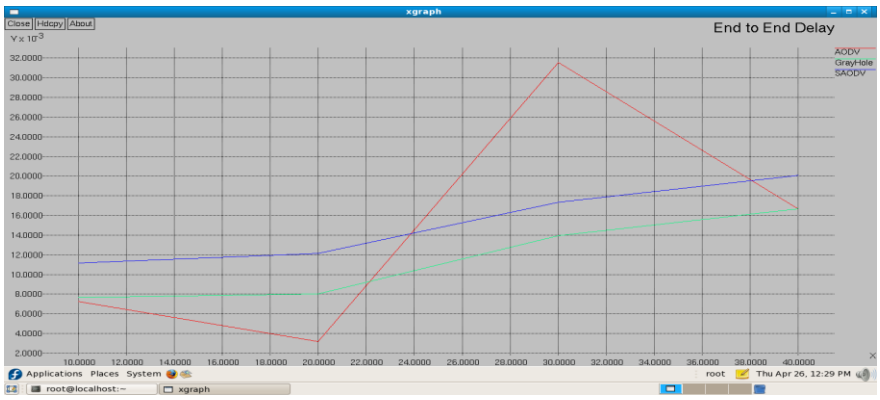

Figure 6: Number of Nodes & E2e for AODV, Gray Hole & SAODV

5.1.6 Evaluation of Throughput for AODV, Gray Hole & SAODV (Kbps)

Table VII: Throughput for Normal AODV, Gray Hole & SAODV

Nodes	10	20	30	40
AODV	36.72	38.43	38.89	38.16
Gray Hole	34.64	32.35	37.68	38.16
SAODV	38.33	32.60	37.86	39.44

5.1.7 Basic Parameters for adhoc network & graphical representation of gray hole attack with different mobile nodes

Basic parameters of ad-hoc network consist of:

- Simulator used
- Topology Area
- Simulation Time
- Number of nodes
- Routing Protocol
- Traffic
- Pause time
- Transport Protocol
- Packet size

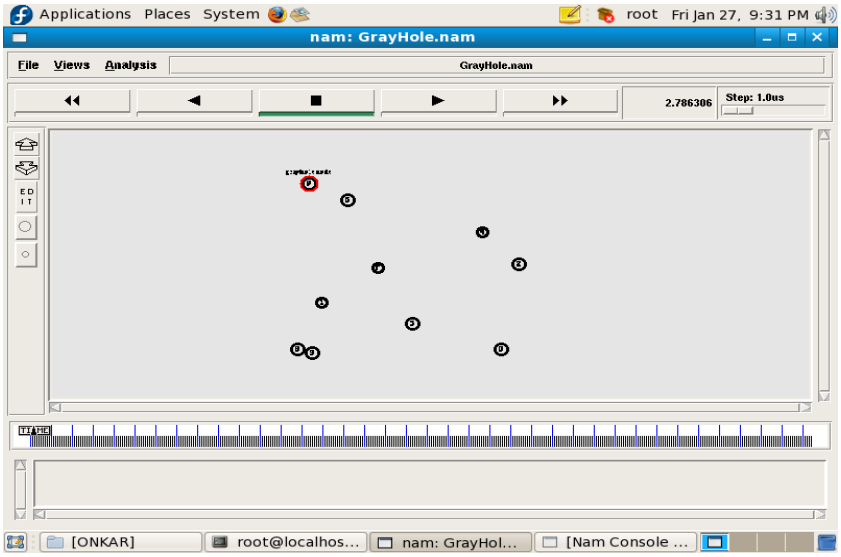

Figure 7: Gray Hole attack with 10 mobile nodes

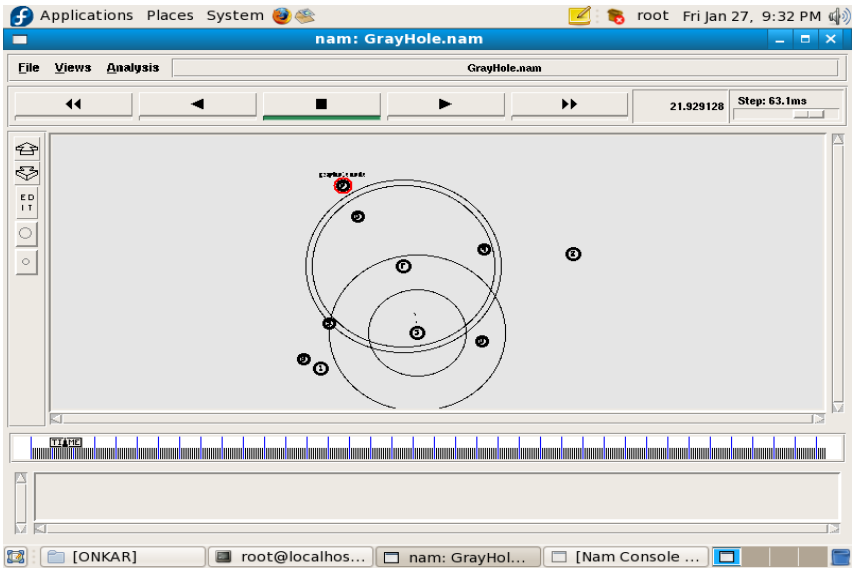

Figure 8: Gray Hole with 10 Mobiles Nodes with Drop of Certain Packets

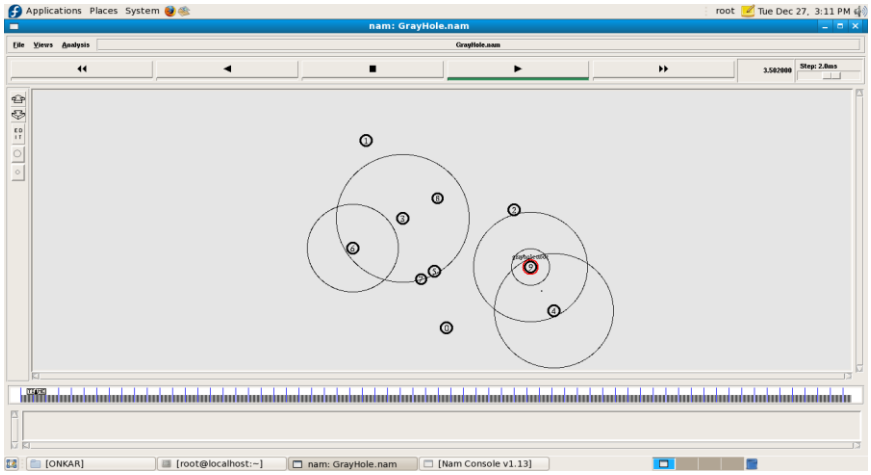

Figure 9: Single Gray Hole Node with Circle Represents RREQ & RREP

VI. CONCLUSION

Mobile ad-hoc network has been active research based area over the past few years, due to their application in military and civilian communication. But it is vulnerable to various types of attacks. Misbehavior of nodes causes the damage to the nodes & packet also. Gray hole attack cause damage to the network & also it is difficult to detect.

In this paper, we proposed a method algorithm for the detection & prevention of the gray hole attack as well as malicious node behavior. From the experimental result, Algorithm is well efficient in improving the performance metrics of the adhoc network. As the gray hole node or attack is detect & prevent then there is much more increase in the packet delivery ratio as well as end to end delay. By implementing a secure technique (SAODV) in the algorithm the performance of the network gets increases and also we can secure our network from the gray hole attack. In order to further improve accuracy in the adhoc network, we can go for the some additional features in the simulations parameters of the adhoc network. So that we can achieve the reliability and accuracy in the network & that will be the further direction.

VII. FUTURE WORK

Many Problems in ad-hoc network remain to be investigated. Method for the detection & prevention of gray hole or malicious node is very efficient for detecting & preventing from the gray hole attack or behavior of malicious node. Because of the different attacks on the ad-hoc network, the performance of the network gets decreases. Future work will involved some new additional features or parameters using which there is a much more increment in the performance metrics of the network as well as try to avoid the different attacks which occur on the network, with the use of different routing protocols available in MANET. As future work, we intend to develop simulations to analyze the performance of the proposed solution based on the performance metrics and mainly concentrate on one thing that there is a minimum amount of packets loss during the transmission.

REFERENCES

[1] 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.

[2] Poongothai T. and Jayarajan K., *"A non-cooperative game approach for intrusion detection in Mobile Adhoc networks"*, International Conference of Computing, Communication and Networking (ICCC), 18-20 Dec 2008, St. Thomas, VI,pp 1-4.

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

[4] S. Marti, T. J. Giuli, K. Lai, and M. Baker, *"Mitigating Routing Misbehavior in Mobile Ad Hoc Networks"*, Proceedings of the 6th annual international conference on Mobile Computing and Networking *(MOBICOM)*, Boston, Massachusetts, United States, 2000, 255-265.

[5] Oscar F. Gonzalez, Michael Howarth, and George Pavlou, *"Detection of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks",* Center for Communications Systems Research, University of Surrey,Guildford, UK. Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium on May 21, 2007.
[6] 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.
[7] P. Papadimitratos, and Z. Haas, "*Secure routing for mobile ad hoc network*s", In Proceedings of SCS Communications Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 2002.
[8] 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.
[9] L. Buttyan, and J. Hubaux, "*Enforcing cooperation in self organizing mobile as hoc networks*", In Proceedings of IEEE/ACM Workshop on Mobile Ads Hoc Networks, Technical report DSC/2001/046, EPFL-DIICA, August 2002.
[10] Muhammad Zeshan, Shoab A. Khan, Ahmad Raza Cheema and Attique Ahmed, "*Adding Security against Packet Dropping Attack in Mobile Ad Hoc Networks",* in 2008.International Seminar on Future Information Technology and Management Engineering, November 2008, pp. 568-572.
[11] S. Usha, S. Radha, *"Co-operative Approach to Detect Misbehaving Nodes in MANET Using Multi-hop Acknowledgement Scheme", i*n 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies, December 2009, pp.576-578.
[12] 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.
[13] Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu *"Mobile ad hoc networking: imperatives and challenges"*, School of Engineering, University of Texas at Dallas, Dallas, TX, USA, 2003.
[14] J. Sen, M.G. Chandra, S.G. Harihara, H. Reddy, and P.Balamuralidhar, *"A mechanism for detection of gray hole attack in mobile Ad Hoc networks",* in Proc. of the 6th International Conference on Information, Communications & Signal Processing, December 2007, pp. 1-5.

AUTHORS

Onkar V. Chandure received his Bachelor Degree in Information Technology With distinction from Amravati University Amravati, INDIA in 2008.He has also received Master Degree in Information Technology in 2012 From Sant Gadge Baba Amravati University, Amravati, INDIA. He recently towards his PhD. He is currently working as an Assistant Professor in Information Technology Department J.D. Institute of Engineering & Technology,Yavatmal, India. His fields of interest include mobile adhoc network.

Aditya P. Bakshi received his Bachelor Degree in Computer Science & Engg from Amravati University Amravati, INDIA in 2008.He has also received Master Degree in Computer Engg in 2012 From Sant Gadge Baba Amravati University, Amravati, INDIA. He recently towards his PhD. He is currently working as an Assistant Professor in Information Technology Department J.D. Institute of Engineering & Technology,Yavatmal, India. His fields of interest include Image Processing.

Saudamini P. Tidke received her Bachelor Degree in Information Technology from Amravati University Amravati, INDIA in 2010. She is also pursuing a Master Degree in Information Technology From TIT Engg, Bhopal, RGPV University Bhopal. INDIA. His fields of interest include mobile adhoc network.

Priyanka M. Lokhande received her Bachelor Degree in Information Technology from Amravati University Amravati,INDIA in 2010.She is also pursuing a Master Degree in Computer Science & Engg From Sipna COET, Amravati, INDIA. From Sant Gadge Baba Amravati University, Amravati, INDIA. His fields of interest include mobile adhoc network.