A Survey on Modified approach to detect and prevent Grayhole attack in MANET

Ankita Prajapati[1], Prof. Krunal Panchal[2].

[1]*Student (Master of Engineering), Information Technology, L.J. Institute of Engineering and Technology , Gujarat, India.*
[2]*Assistant Professor(PG dept.), Computer Engineering, L.J. Institute of Engineering and Technology , Gujarat, India.*

ABSTRACT

Mobile Ad hoc Network (MANET) has distributed mobile wireless nodes, which do not have pre-determine topology and pre-existing infrastructure mobile nodes that can arbitrarily change their geographic locations and random mobility with constrained resources, ad hoc networks are vulnerable due to their structure less property. During the Grayhole attack, a Grayhole 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. In these proposed detection mechanisms for In this paper we represent a mechanism which is helpful for prevention of gray hole attack, through observing the delay of different path to receiver and verification using authentication approach. 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.

Keyword:-*MANET, AODV, Black-hole-attack, Gray-hole Attack.*

1.INTRODUCTION

Mobile ad hoc network (MANET)[7] is an emerging area of research which is infrastructure less network that enables the user to communicate without any fixed infrastructure. MANET[8] is a wireless network that can transfer the information from source to destination wirelessly.The nodes are movable which communicate and coordinate with the other nodes[7].Now days this network is widely used all around the world because it does not require any fixed wired network to establish communication between the source and the destination. The entire network can be established by using transmitter, receiver, processor and the battery[8]. In today's scenario the mobile ad hoc network used in many real time applications like military surveillance, disaster management, air pollution monitoring etc[8].There are many issues in MANET like Security, Routing, Medium access scheme,Self Organization, Multicasting, Energy Management etc[6].

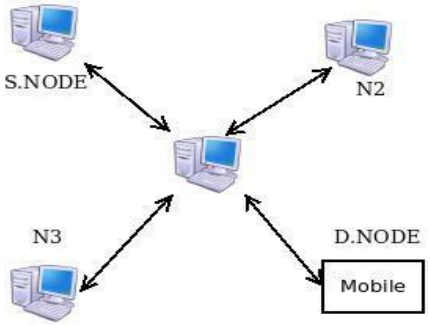

Fig. 1. Mobile Ad-hoc Network [7].

ATTACKS IN MANET

Taking into consideration the constraints of MANETs, most routing protocols are fairly simple, and therefore quite vulnerable to attacks.Some of these attacks are:Eavesdropping, Rushing attack ,Byzantine attack ,Location disclosure attack, Sleep deprivation attack, Routing table overflow attack ,Black hole attack ,Grayhole attack ,Wormhole attack,Denial of service, Impersonation attacks, Man-in-the-Middle attacks etc[13].

Security is the prime issue in the MANET among all the research issues. There are two common kinds of denial of server attack (DOS); one of them is Black Hole Attack and the other one is Gray Hole attack which has major class of threat today[7].It is the variation of Black hole attack. Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network and that node drops the entire packet. But in Gray-Hole attack, nodes will drop the packets selectively[8].

GRAYHOLE ATTACK:

In Grayhole attack, the attackers uses selective data packet dropping method to behave as genuine node and try to participate into full communication[8].Gray Hole attack execute malicious activity by dropping the packet selectivity by launching a single malicious layer[7]. They mislead the source node by pretending for shortest path.Gray-hole malicious node participate into route discovery process and update the source route cache/ routing table as shortest path[7]. Afterwards, source always consider malicious node as next hop node and forward packet to same. Malicious node captures all the incoming packets but drop on random basis.Gray-hole attack [9] may apply through two ways which are listed below:

1. Dropping all incoming UDP packets.
2. Partial dropping of UDP packets with random selection process.

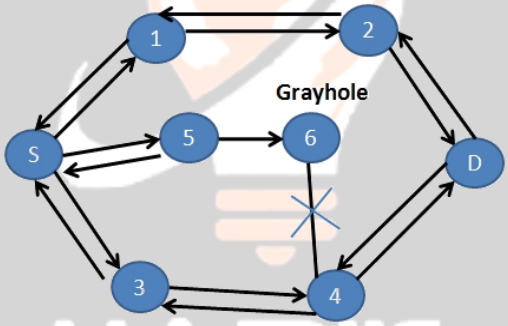

Fig. 2: Gray Hole Attack in MANET[10].

In Grayhole attack, the nature of the malicious node is highly unpredictable. It behaves as genuine legitimate node for a short duration and behaves as a malicious node for other duration. Thus we can say that the Grayhole attack is the extension of the Blackhole attack. Grayhole a ttack acts as a slow poison because the probability of the packet loss cannot be determined perfectly [12].

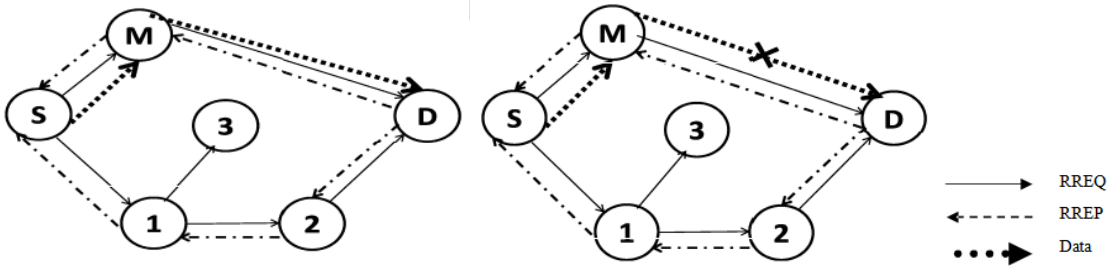

Fig 3: Operation of Grayhole Attack[12].

2. WORKING OF GRAYHOLE ATTACK:

Gray-hole is an attack that can switch from behaving genuine to sinkhole. Because it can act as normal node switch over to malicious node it becomes too typical to identify the state whether it us normal node or malicious node[8].Firstly during the route discovery processes, it drops the packets and secondly, by changing its state to mischievous state or vice versa, where false node pretends to act like the true node[7].

When the source node broadcast the RREQ packet the AODV approach executed the request packet.If did it match afterwards the route establishment occurs from source to destination.Then the threshold value calculated. If the threshold value is higher then common node then the grayhole node would be present in the network.

The grayhole node selectively drops the packets.Furthermore, in the state of malicious node it also forwards some packet to create illusion of genuine nodes. Due to this behavior it is very hard to find out in the network to figure out such kind of attack[8].

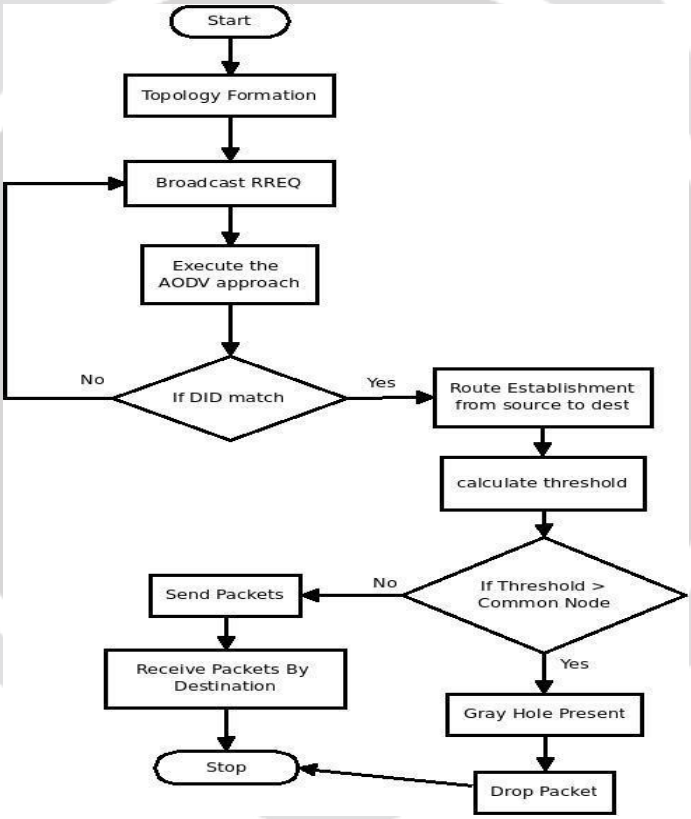

Fig. 4. Flow Chart depicting the working of Gray Hole Attack [7].

3. RELATED WORKS

3.1 LITERATURE REVIEW

3.1.1 Gray Hole Attack Detection using False Reply Count and TrueLink based Path Authentication in MANET

- In [1] Yugandhara S. Patiland and Dr. Ashok M. Kanthe proposes False reply count and TrueLink based Path Authentication scheme, False reply count is very help full to detect gray hole without increasing routing overhead. The algorithm is executed on every node in the network at the local level, due to this it takes minimum time and faster than existing technique. This technique never exchanges black list and never send ALARM packets to inform other nodes about malicious node. This property reduces network traffic. TrueLink is facilitated for path authentication. As false reply count technique executes during route discovery process, any honest node can switch in the black hole after route establishment between source and destination. Hence it is important to detect gray hole and verify link.

3.1.2 A Modified Approach for Recognition and Eradication of Extenuation of Gray-Hole Attack in MANET using AODV Routing Protocol

- In [2] Sudheer Kumar and Nitika Vats Doohan proposes IDS-agent approach to detect highest sequence number node. When it detects the suspicious node, it adds it into blacklist of source node to avoid further transmission. Simulation of proposed solution observes that prevention technique not only detect malicious node but also help to prevent it.

3.1.3 A novel approach for mitigating gray hole attack in MANET

- In [3] Shashi Gurung and Siddhartha Chauhan proposes MGAM (Mitigating Gray hole Attack Mechanism), that mitigates the impact of the smart gray hole attack. which is mainly used to compute the number of packets dropped by the particular node.When any anomaly is detected by the G-IDS nodes, an ALERT message is broadcasted by it, alerting all nodes in the network for blocking the malicious node. All normal nodes upon receiving the ALERT message issued by G-IDS nodes will include the malicious node in their blacklist table, The simulation results show that our proposed mechanism improves the network performance in terms of PDR, PLR and average throughput.

3.1.4 A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks

- In [4] Rutvij H. Jhaveri and Narendra M. Patel proposes bait detection scheme (called SNBDS) for AODV protocol which is based on the destination sequence number. The scheme attempts to counter grayhole attack during route discovery phase without introducing additional control packets to propagate information about malicious nodes to other nodes in the network..

3.1.5 Hindrance and Riddance of Gray Hole Attack In MANETs Multipath Approach

- In [5] Jyoti Prabha Singh, Savita Shiwani, Dinesh Goyal, Vishal Gaur,proposed a packet update scheme and even advise the elimination scheme by discovering all the malicious nodes.The overall simulation performance is demonstrate that the Gray Hole attack scenario provides good result and even normalize the Gray Hole effect network which results in normalizing effects, of Gray Hole.Concept has shown improved result after elimination of the Gray Hole attack in the simulation result.

3.2 COMPARATIVE TABLE

Table : Comparative Table

Sr. No.	Paper Title	Method Used	Advantages	Disadvantages
1	Gray Hole Attack Detection using False Reply Count and TrueLink based Path Authentication in MANET	False Reply Count and TrueLink Path Authentication	Doesn't increase routing overhead.It takes minimum time and faster than existing technique. Also reduces network traffic.	Complex Architecture, Network congestion issue

2	A Modified Approach for Recognition and Eradication of Extenuation of Gray-Hole Attack in MANET using AODV Routing Protocol	IDS-agent approach	The technique not only detect malicious node but also help to prevent it.Also it performs better then grayhole attack in case of 30 & 40 scenarios.	Work on only 30-40 nodes Idenfiy and analsysis on only one malacious node.
3	A novel approach for mitigating gray hole attack in MANET	GIDS,MGAM	Deal with smart gray hole attack and sequence number based Attack and it doesn't use any additional control packet to detect the malicious node in the network.	The gray hole attacker will not be detected and blocked if it is outside the range of GIDS.GIDS nodes are fixed in the network and therefore cannot move.
4	A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks	SNBDS	Doesn't use additional control packets. Improvement in PDR NRO under the first two adversary models (Attack1 and Attack2) as compared to DSAODV.	The third adversary model (Attack3) drops data packets to bring down the network performance.
5	Hindrance and Riddance of Gray Hole Attack In MANETs Multipath Approach	Packet update scheme	Gray Hole attack scenario provides good result and even normalize the Gray Hole effect.	To find out the entire malicious node , repeat the whole process which can take more time and resources too.

4. CURRENT ISSUES IN MANET

The problems that arise in the network layer of an ad hoc network can be broadly classified into the following three categories: Topology control, Data communication, Service access. Topology control problems are discovering neighbors, determining the transmission radii, location identification, link establishment to neighbors, scheduling the node-awake and sleep time, cluster formation, maintenance, and so on.Data communication problems are Routing, Location updating, Broadcasting, Multicasting.Service access problems typically deal with cellular network access, Internet access, IP addressing in merge or split network scenarios, data or service replication upon detection, or expectation of network partition.There are some major technical issues that the research community has to resolve. Security,Reliability ,Scalability, Quality of service, Power management, Interoperability,Mobility[11].

5. CONCLUSION

The overall study concludes that the Gray Hole is severe threat in the ad hoc mobile network security which occurs due to vulnerabilities of AODV routing protocol. There is need to identify the vulnerabilities and increase its growth. The complete work observes Grayhole attack as crucial threat and will propose a solution to overcome its problem.Gray hole attack ultimately decrease the concert of the network. The main goal of the gay hole attack should be the improvement of security and as well as the performance of the network.

6. REFERENCES

[1] Yugandhara S. Patil, Dr. Ashok M. Kanthe." Gray Hole Attack Detection using False Reply Count and TrueLink based Path Authentication in MANET" Computer Engineering Department, Sinhgad Institute of Technology, Lonavala.Pune, India.IEEE-2016.

[2] Sudheer Kumar, Nitika Vats Doohan " A Modified Approach for Recognition and Eradication of Extenuation of Gray-Hole Attack in MANET using AODV Routing Protocol". Medi-Caps Group of Institution Indore,India.IEEE-2016.

[3] Shashi Gurung, Siddhartha Chauhan." A novel approach for mitigating gray hole attack in MANET". Department of Computer Science and Engineering, National Institute of Technology, Hamirpur, Hamirpur, HP, India.Springer-2016.

[4] Rutvij H. Jhaveri,Narendra M. Patel." A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks". Department of Computer Engineering, CSPIT, Charotar University of Science & Technology, Changa 388 421, India, Department of Computer Engineering, Birla Vishvakarma Mahavidyalaya, Vallabh Vidyanagar 388 120, India.Springer-2015.

[5] Nadav Schweitzer, Ariel Stulman, Member, IEEE, Asaf Shabtai and Roy David Margalit." Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks".IEEE-2016.

[6] AD HOC WIRELESS NETWORKS by C.Siva Ram Murthy and B.S.Manoj-Pearson publication.

[7] Jyoti Prabha Singh,Savita Shiwani,Dinesh Goyal,Vishal Gaur"Hindrance and Riddance of Gray Hole Attack In MANETs Multipath Approach" 2017,3rd IEEE International Conference on Computational Intelligence and Communication Technology (IEEE-CICT) 978-1-5090-6218-8/17/$31.00 ©2017 IEEE.

[8] Rupali Sharma "Gray-hole Attack in Mobile Ad-hoc Networks:A Survey" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (3) , 2016, 1457-1460.

[9] V. SHANMUGANATHAN, Mr.T.ANAND "A Survey on Gray Hole Attack in MANET" IRACST International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.2, No6, December 2012.

[10] Ruchi Tiwari, Jyoti Jain "Exposure and Mitigation of the Gray Hole Attack from AODV in Mobile Ad hoc Network: An Approach" International Journal of Computer Applications (0975 – 8887)Volume 165 – No.5, May 2017.

[11] Subhankar Dhar "MANET:Applications, Issues, and Challenges for the Future"Int'l J. of Business Data Communications and Networking, 1(2), 66-92, April-June 2005.

[12] Mr. Ankit D. Patel,Mr. Kartik Chawda,"Blackhole and Grayhole Attacks in MANET" 2014,ISBN No.978-1-4799-3834-6/14/$31.00©2014 IEEE.

[13] Nabil Nissar, Najib Naja,Abdellah Jamali,"Lightweight Authentication-based Scheme for AODV in Ad-hoc Networks" 2017,978-1-5090-6681-0/17/$31.00 ©2017 IEEE.