IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 4, June 2014.

www.ijiset.com

ISSN 2348 - 7968

Mitigation of Black Hole and Grey Hole Attack In Mobile Ad hoc Networks

Amanpreet Kaur[1],ManjotKaur Sidhu[2]

[1]M.Tech Scholar,CSE, Chandigarh Group of College, Gharuan, Mohali, Punjab, India

2Associate Professor,CSE, Chandigarh Group of College, Gharuan, Mohali, Punjab, India

Abstract

Wireless networks are gaining popularity to its peak today. Mobile Ad hoc Networks called MANETs are self-configuring wireless networks and it is without any centralized control made by mobile nodes. Nodes can act as both routers and hosts. The dynamic topology of MANETs allows nodes to join and leave the network at any point of time. So, it is vulnerable to various kinds of attacks like Active attack, Passive attack, Internal attack, External attack, Black hole and grey hole attack. Previouswork is done on security issues in MANET were based on reactive routing protocol example: Ad-Hoc On Demand Distance Vector (AODV). Various kinds of attacks were studied earlier, and their effects were elaborated by stating how these attacks disrupt the performance of MANET. In this paper, we present a review on number of techniques that helps to mitigate black hole and grey hole attack that effect the performance of MANET.

Keywords— Black hole attack; Grey hole attack;MANETs; AODV.

1. INTRODUCTION

Mobile Ad-Hoc Networks are autonomous and decentralized, infrastructure less wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices like mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network.MANETs have become increasingly important in increasingly wide range of applications, such as battlefields and other military environments, disaster areas, and outdoor activities[1]. The MANET differs fromother wireless networks because of its dynamic topology. It is a set of mobile nodes where every node communicates with each other without any predefinedinfrastructureand centralized administration. Due to the openness of its nature it is vulnerable to various kinds of threats but security is very essential. The wireless mobile ad hoc nature of MANETs brings new security challenges to the network design. As the wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation, mobile ad hoc networks are intrinsically exposed to numerous security attacks. Black hole and gray hole are the imminent attacks that are launched on Ad hoc on demand distance vector routing protocol. Both the attacks claim the shortest route to the destination and exploit this later by dropping the packets. Following are the advantages of MANET:

- They provide access to information and services regardless of geographic position.
- Independence from central network administration. Self-configuring network, nodes are also act as routers.
- Less expensive as compared to wired network.
- Scalable—accommodates the addition of more nodes.
- Improved Flexibility

ISSN 2348 - 7968

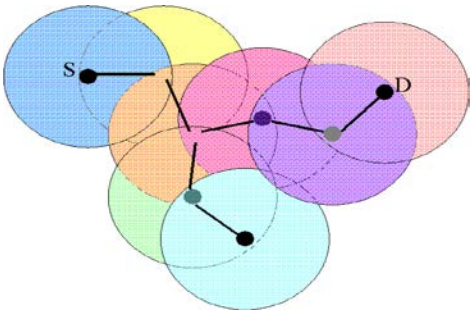


Figure1 MANET Environment

1.1 Ad hoc on demand distance vector (AODV) is a routing protocol being used for wireless ad hoc network. AODV routing protocol is a pure reactive protocol. In AODV protocol, the route is established between the source and destination when the route is required. Route discovery and route maintenance are the two phases with which routing is carried out. Ad-Hoc network routing protocols are commonly divided into three main classes; Proactive, reactive and hybrid protocols.

1.1.1 *Proactive Protocols*: Proactive or table-driven routing protocols. In proactive routing, each node has to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view.

1.1.2 *Reactive Protocols:* Reactive routing is also known as on-demand routing protocol since they do not maintain routing information or routing activity at the network nodes if there is no communication

1.1.3 *Hybrid Protocols*: They introduce a hybrid model that combines reactive and proactive routing protocols. The Zone Routing Protocol (ZRP) is a hybrid routing protocol that divides the network into zones. ZRP provides a hierarchical architecture where each node has to maintain additional topological information requiring extra memory.

2. SECURITY GOALS/REQUIREMENTS IN MANET

There are mainly four mechanism- Availability, Confidentiality, Integrity and Authenticationthat are used to provide the security. A brief explanation about these terms given below:

2.1 *Availability:*The network should only be available for the authenticated users and this mechanism is used to protect against the attacks like Gray hole attack, black hole attack, Information disclosure and Message altering
.

2.2 *Integrity*: Integrity means if source node sends A(message) then destination receives A(message). No modification done by any other node. The transmission of information should be protected against any message modification.

2.3 *Confidentiality:*There is difficult to attain the confidentiality in MANET due to intermediate nodes routing, which can easily retrieve the information from the routing nodes.

2.4 *Authentication:* Authentication is very essential so the network should be accessed only by the authenticated nodes such as Digital signature and Non repudiation.

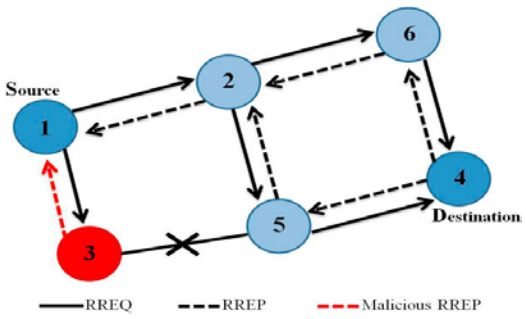
3. BLACK HOLE AND GREY HOLE ATTACK

Black hole and Grey hole attack are distinguish attack in MANET. In black hole attack, source node sends or broadcast the route request message to the nodes. But request is listened by the attackeror malicious node and then malicious node claim itself that it has a shortest path to the destination minimum hop count and maximum sequence number.Thus the source node believes and the source node ignores the RREP packet from the other nodes including the correct nodes and it will start sending the packets towards the malicious nodes. Then the malicious node takes all the routes towards itself and it doesn't allow forwarding the packets to the others nodes. Black hole is one of the active type of attack. There are three types of black hole attack:

3.1 *Single Black hole attack*: In this type of attackonly one malicious node uses routing protocol to claim itself of being shortest path to destination node but drops routing packets and doesn't forward packets to its neighbors.

3.2 *Cooperative Black hole attack*: Black hole is a malicious node that incorrectly replies the route requests that it has a fresh route and minimum hop count and then it drops all packets which received. Serious damage arises if the malicious nodes work together as a group then this is called cooperative black hole attack.In Black hole attack a malicious node may advertise a fresh path to a destination during routing process. The intention of the node may be to disturb the path finding process or interpret the packet being sent to destination. Example, In AODV, the attacker or malicious node can send a fake RREP to the initialize node called source node, claiming that it has a sufficiently fresh route to the destination node. It causes the source node to select the route that passes through the attacker node. Therefore, all traffic will be routed through the attacker node, and hence, the attacker can misuse or discard the traffic. The method how malicious node fits in the data routes varies.

3.3 *Multiple Black Hole Attack:*The black hole attack is worse if the multiple Black hole nodes exist in the network.When multiple black hole nodes exist in the network and all the malicious nodes are responsible for performing the Black hole attack. In this attack multiple malicious nodes advertises itself having the shortest path to the destination and falsely replies to the route requests and drop all the receiving packets. This type of attack in which multiple nodes are malicious is called Multiple Black Hole Attack.



[8] Figure 2 Black hole Attack

In figure 2, Single Black hole Attack occurs. In this figure node 1 is a source node and node 4 is a destination node. Node 3 is a malicious node and falsely reply to the source node and does not send the packet to the destination node and drop all the packets and spurious node 3 also effect the MANET network. Grey hole attack is more dangerous and difficult to detect then the black hole attack.

Gray-hole attack is a kind of black hole attack. In gray hole attack packets are dropped with some probability. It drop packet coming from (source) and going to certain specific node in a network while forwarding all packet from and to other nodes. In another behavior, gray-hole node drops packets for some duration and switches from malicious behavior to normal behavior. Thus the behavior of the gray hole attacker is varies from normal to malicious and vice versa. Hence it is difficult to detect.

The gray hole attack has two phases:
First phase: A malicious node exploits the AODV protocol to advertise itself that it has a true route to destination node, with the intention of interrupting packets of spurious or wrong route.

Second phase: In second phase, the nodes has been dropped the interrupted packets with a certain probability. Normally in the gray hole attacks the attacker behaves maliciously for the time until the packets are dropped and then switch to their normal behavior [2]. Both normal node and attacker node is same. Due to this behavior it is very difficult to find out in the network to figure out such kind of attack. Gray hole attack is also known by the name node misbehaving attack.

Table 1: Difference between Black hole and Grey hole Attack

Black hole Attack	**Grey hole Attack**
In Black hole attack malicious node drops all the packets.	In Grey hole attack malicious node drop the packets with certain probability.
Malicious node does not forward the packets to the other nodes.	Malicious nodes forward the 50% packet to the other node.
Easy to detect then the Grey hole attack.	More difficult to detect

ISSN 2348 - 7968

4. RELATEDWORK/MITIGATION TECHNIQUES

Huirong Fu et.al.[3] proposedDRI Table and Cross Checking Scheme to identify the cooperative black hole nodes. Each node maintains the extra DRI table with two entries "From" and "Through", where 1 represents true and 0 represent false. These entries stand for the information on routing data packet from and through the nodes. In this solution, the Intermediate node replies the next hop information and DRI entry about next hop node along with RREP packet. The source node then checks the reliability of intermediate nodes by using cross checking scheme via alternate paths by using DRI table information. It provides 50 % throughput but failed because it increases end to end delay and routing overhead.

NaveenaGarg[4] proposed a method to detect and isolate both black hole ad grey hole attack. In black hole, malicious node falsely replies for any Route Requests (RREQ) without having true route to specified destination and drops all the receiving packets. The damage will become more serious if these malicious nodes work together as a group. When malicious nodes work together in a group then it comes under one type of black hole attack i.e. cooperative black hole attack. A, when the malicious node works as a true node initially then it turns malicious sometime later then it is called grey hole attack. In this paper a mechanism to detect and remove both cooperative and grey hole attack using the concept of restricted IP's along with the construction of backbone of trusted nodes and Core maintenance table.

Rajiv Ranjan[5] proposed a method to mitigate an attack which can bring great damage to the network is known as black hole attack. This attack disturbs the router. In this paper an algorithm is design which has capability to detect this type of attack. Based on cross layer design, authors demonstrate a technique to point out wormhole attacks in MANET and proposed a pathbased method to overhear the next hop's action in Network layer. This scheme does not send extra controlpackets and saves the system resources ofthe detecting node. A collision rate reporting system is established toestimate dynamic detecting threshold so as to lower the false positive rate under high network overload.

Jiwen CAI et.al. [6] Proposed an approach/ algorithm to detect Black and gray hole attack. These attacks can bring great damage to the network and they are routing disturbing. In this paper author's proposed efficient algorithm or adaptive approach to detect black and gray attack in ad-hoc network based on cross layer design. A path-based method to overhear the next hop's action proposed in the network layer but scheme does not send out extra control packets and saves the system resources of the detecting node. In MAC layer, a collision rate reporting system is establishedto estimate dynamic detecting threshold so as to lower the false positive rate under high network overload. In this paper DSR protocol used to test the algorithm and ns-2 simulator. The average detection rate is above 90% and the false positive rate is below 10% and the adaptive threshold strategy contributes to decreasing the false positive rate.

Dr. Debika Bhattacharyya et.al [7] classifies several common attacks against the ad hoc networks routing protocols in this paper which is based upon the techniques that could be used by attackers to exploit routing messages. In this paper author's designed a new security mechanism for mobile ad hoc networks, one must consider the attacksvariations as well as the characteristics of the attacks that could be launched against the ad hoc networks and existingdetection and mitigation schemes.

Fan-HsunTseng, Li-Der Chou and Han-ChiehChao[8] survey the existing techniques and discuss the state of the art routing methods. The black hole attack issecurity threats in wireless mobile ad hoc networks. The intruders utilize the loophole to carry out their malicious behaviors because the route discovery process is necessary and inevitable. In this paper authors don't only classify these proposals into single and cooperative black hole attack but also categories the solutions and give the comparison table. Comparison of Single Black Hole Attack Detection Schemes is given in this paper. Comparison between protocol like AODV, secure AODV and DSR are done.

ISSN 2348 - 7968

KundanMunjalat.el. [9] proposed an algorithm to detect and remove multiple black hole attack. The attack becomes worse when multiple black hole nodes present in the network. In single black hole attack only one malicious node present in the network but in multiple black hole attack more than one or multiple malicious nodes present in the network and all are responsible to do attack. In this paper enhancement in the AODV protocol by proving more security after detecting the single or multiple black hole nodes in MANET. The multiple black hole nodes are detected at the initial stage before the route discovery process of AODV, by using fake RREQ(route request) packet and modified RREP(route reply) packet, which leads to less routing overhead and high Packet Delivery Ratio.

JunhaiLuo et.al.[10] proposed a solution to the black hole attack which is one of the security threat that can occur in MANETs. In black hole attack, a malicious node exploits the routing protocol to advertise itself as having the shortest path to the destination and minimum hop count but it intercept and drop all the data packets. The black hole problem is addressed in this paper. In this paper, an authentication mechanism based on the hash function, the Message Authentication Code (MAC), and the Pseudo Random Function (PRF) is proposed for black hole attack. The simulation results show by using ns2 (network simulator) the scheme provides fast message verification identifies black hole and discovers the safe routing avoiding the black hole attack.

5. CONCLUSION

Mobile Ad hoc Networks is a self-configuring & infrastructure less network that consists of independent mobile nodes and can communicate via wireless medium.In MANET, each mobile node can move freely in any direction, and changes their links to other devices frequently. Security is an important part of ad hoc networks. Due to the dynamic topology of MANET, resource constraints, no centralized infrastructure and limited security, it is vulnerable to various attacks like black hole attack and grey hole attack. In black hole attack, the malicious node advertises itself as having the shortest path to the destination, maximum sequence number and falsely replies to the route request(RREQ), and drops all receiving packets. Grey hole attack is more difficult to detect because it drop the packet with the certain probability and behaves like malicious node after some time. In this paper various mechanisms has been studied to detect the black hole attacks &Grey hole node and concluded that lots of work done on the black hole attack and grey hole attack. The detection of Grey Holes in ad hoc networks is still considered to be more a challenging task. So, Future work is intended to an efficient Grey hole attack detection and elimination algorithm with minimum delay & overhead.

REFERENCES

[1] Kartik Kumar Srivastava, AvinashTripathiand Kumar Tiwari, " Secure Data Transmission in MANET Routing Protocol" IJCTA , Int.J.Computer Technology &Applications,Vol 3 (6), 1915-1921 Nov-Dec 2012. Available online@www.ijcta.com

[2]OnkarV.Chandure, Prof V.T.Gaikwad " A Mechanismfor recognition & Eradication of Gray Hole attack usingAODV Routing Protocol in MANET" IJCSIT , Vol.2,No.6, Jul 2011.

[3] Sanjay Ramaswamy, Huirong Fu, ManoharSreekantaradhya, John Dixon and Kendall Nygard, "Prevention of Cooperative Black Hole Attackin Wireless Ad Hoc Networks" International Journal of Computer Science.

[4] Vikram verma1and Naveenagarg, "Enhanced AODV Protocol to Mitigate Black Hole Attack in MANETS" Proc. of Int. Conf. on Emerging Trends in Engineering and Technology, ACEEE.

[5] Rajiv Ranjan, NareshTrivedi and AnoopSrivastava "Mitigating of Black Hole Attack in Manets",VSRD-IJCSIT, Vol. 1 (2), 2011, 53-57, ISSN no. 2231-2471.

[6] Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network", 2010 24th IEEE International Conference on Advanced Information Networking and Applications.

[7] HimadriNathSaha , Dr. Debika Bhattacharyya , Dr. P. K.Banerjee,Aniruddha Bhattacharyya ,Arnab Banerjee , Dipayan Bose , "Study of Different Attacks in Manet with its Detection & Mitigation Schemes", International Journal of Advanced Engineering Technology E-ISSN 0976-3945

[8] Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh Chao, "A Survey of Black Hole Attacks in Wireless Mobile Ad Hoc Networks", Tseng et al. Human-centric Computing and Information Sciences 2011, 1:4 http://www.hcis-journal.com/content/1/1/4

[9] NishuKalia, KundanMunjal, "Multiple Black Hole Node Attack Detection Scheme in MANET by Modifying AODV Protocol" , International Journal of Engineering and Advanced Technology (IJEAT), Volume-2, Issue-3, February 2013.

[10]JunhaiLuo,,Mingyu Fan, Danxia Ye, "Black Hole Attack Prevention Based on Authentication Mechanism" , Communication Systems, 2008.ICCS 2008.11th IEEE Singapore International Conference.

[11] Mohammad Al-Shurman, Seong-Moo Yoon and Seungjin park, "Black Hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, Proceedings of the 42nd annual southeast regional conference , 2004, pp 96-97.

[12] J.Sen, S.Koilakonda and A.Ukil, "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks", Second International Conference on Intelligent System, Modeling and Simulation ,Innovation lab, Tata consultancy services ltd. , Kolkata, 25-27January 2011.

[13] Kartik Kumar Srivastava, AvinashTripathi and Anjnesh Kumar Tiwari, " Secure Data Transmission in MANET Routing Protocol" IJCTA , Int.J.ComputerTechnology &Applications,Vol 3 (6), 1915-1921 Nov-Dec 2012. Available online@www.ijcta.com

[14] Vineetha S. H. and ShebinKurian, "Performance Analysis of Cluster Based Secure Multicast Key Management in MANET" **I**nternational **J**ournal of **C**omputer **S**cience and **T**elecommunications [Volume 4, Issue 4, April 2013].