Detection and Prevention Methods of Black Hole & Gray Hole Attacks in MANET – A Critical Survey

Vipin Dwivedi[1], Shish Ahmad[2]

Integral University, Lucknow [2]

Abstract: **Mobile Adhoc Network (MANET) are used all around the world, because it is self-configuring network of mobile nodes formed anytime and anywhere and communicate each other without the help of a fixed infrastructure or centralized management. It is used as potential applications in disaster relief operations, military network, and commercial environments. Since MANET is open, dynamic and has infrastructure-less nature, it is vulnerable to various attacks. Black hole and Gray hole attacks are one of them. Black hole is an attack in which a malicious node claims false RREP message to the source node and correspondingly drops all the receiving packets. Gray hole attack is an attack in which a malicious node poses itself as normal node but causes eavesdropping and selective forwarding attacks. we have reviewed different methods to prevent black & gray hole attacks in MANET.**

Key Words: **MANET, Black Hole, Gray Hole, AODV.**

I. INTRODUCTION

A Mobile Adhoc Network (MANET) is defined as collection of mobile nodes. In MANET, nodes transfer data using multihop wireless links .It does not have any fixed infrastructure. It is a self-configuring network, therefore the mobile nodes in the network dynamically setup paths among themselves to transmit packets from the source to destination. MANET has many important and potential applications, in commercial environments, disaster area, and military operations. Since, wireless networks came into existence, routing in mobile ad hoc networks has been a challenging task. The major reason for this is the constant changes in network topology due to the mobility of nodes. Mobile ad hoc networks are vulnerable to several security issues due to their inherent characteristics, like lack of centralized control, finite transmission bandwidth, open medium, abusive broadcasting messages, dynamic link establishment and restricted hardware caused processing capabilities. Various security threats have been extensively explored and discussed in the wired and wireless networks. The security issues like snooping attacks, wormhole attacks, black hole attacks, gray hole attacks, packet replication, denial of service (DoS) attacks, distributed DoS (DDoS) attacks, et cetera have been studied in recent years. Among these threats, the malicious node problem is one of the popularized security threats such as black hole and gray hole attacks. In this paper, we tried to focuse on various black hole and gray hole detection and prevention methods.

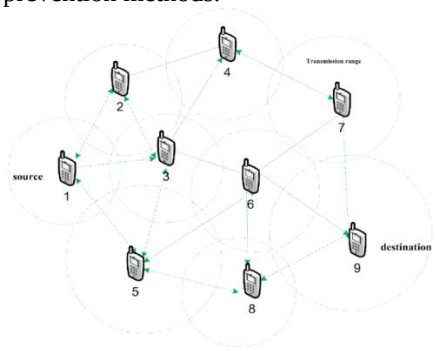

Fig.1 MANET

A. Security Measures of MANET

Ad-hoc and sensor network are particularly prone to malicious activities. Security of MANET is indeed one of the most difficult problems to be solved. Therefore the following security measures should be taken

1) Authentication: Only authenticated nodes can access and use the network by implementing techniques such as digital signature etc.

2) Availability: The network resources should be available only for the authenticated users and this mechanism is helpful to protect against the kind of attacks like black hole, Gray hole etc.

3) Integrity: The data transferred to destination node should not be altered or modified.

4) Confidentiality: Data should be used only by destination node, and intermediate node should not be able to read the data which is not meant for them.

B. Routing Protocols

There are various routing protocols in MANET. In this section, we discuss the popular routing protocols in MANET. Before a mobile node wants to communicate with a target node, it should broadcast its present status to the neighbors. According to the mechanism the information is acquired, the routing protocols can be categorized into proactive, reactive and hybrid routing.

1) *Proactive Routing Protocol:* The proactive routing is also known as table-driven routing protocol. In this routing protocol, mobile nodes broadcast their routing information to the neighbors periodically. Each node needs to maintain its routing table which records the adjacent nodes and reachable nodes the number of hops to reach to them. In other words, all of the nodes have to evaluate their neighborhoods as long as the network topology has changed. Therefore, the disadvantage of these routing protocols is that the overhead increases as the network size increases. However, the advantage is that network status can be immediately reflected if any malicious node joins the network. The most familiar proactive routing protocols are Destination Sequenced Distance Vector (DSDV) routing protocol and Optimized Link State Routing (OLSR) Protocol.

2) *Reactive Routing Protocol:* The reactive routing is also known as on-demand routing protocol. Unlike the proactive routing where node has information in advance, the reactive routing is simply started when a nodes desire to send data packets. The advantage is that the wasted bandwidth induced from the cyclically broadcast can be reduced. Nevertheless, this might also be the fatal

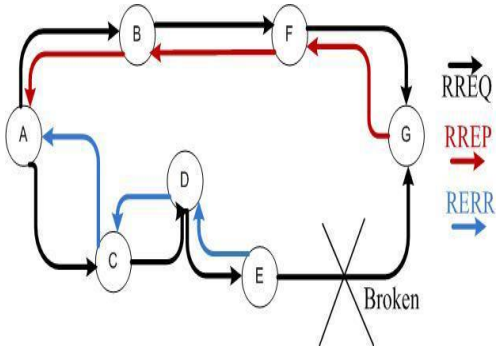

Fig.2 Route Discovery and Maintenance in AODV

wound when there are any malicious nodes in the network environment. The disadvantage is that it leads to some packet loss. The most familiar reactive routing protocols are Ad-hoc On-demand Distance Vector (AODV) routing protocol and Dynamic Source Routing (DSR) protocol. AODV is designed based on DSDV routing. AODV establishes route to the destination node when it is desired by the source node. It also maintains the routing path from source to destination node. One of the remarkable feature of AODV protocol is its use of destination sequence number designated to every route. Destination sequence number is generated by the destination node to include route information that is sent to the requesting node. Mobile nodes communicate to each other by sending Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) messages defined by AODV. Whenever a source node desires to connect
to a destination node, first it checks in the existing route table, as to whether a fresh route to that destination node is available or not. If there is no fresh route available, the route discovery process will be executed immediately. In this phase, the source node broadcasts the route request (RREQ) packet
first. Then all intermediate nodes receive the RREQ packets, but only those nodes send the route reply (RREP) packet to the source node which have destination node information in their routing table. On the other hand, the route maintenance process is
started when the network topology has changed or the connection has failed. The source node is informed by a route error (RERR) packet first. Then it utilizes the present routing information to decide a new routing path or restart the route discovery
process to update the information in routing table.

3) *Hybrid Routing Protocol:* The hybrid routing protocol comes with the strength of proactive routing and reactive routing. Hybrid routing protocols are designed as a hierarchical or layered network framework. Initially, proactive routing is employed to completely gather the unfamiliar routing information, then reactive routing is used to maintain the routing information when topology changes. The familiar hybrid routing protocols are Zone Routing Protocol (ZRP) and Temporally-Ordered Routing Algorithm (TORA).

C. Network Layer Attacks

In ad-hoc network's routing mechanism, Network layer, Physical layer and MAC sub-layer of Data Link layer play a big role. As we know MANETs are very much vulnerable to various attacks, and these three layers suffer from different

attacks and causes routing disorders. The different kind of attacks in the network layer varied such as black hole attack, and Gray Hole attack etc.

1) Black Hole attack : In the figure 3, consider a malicious node 3. When node 1 broadcasts a RREQ packet to get a route to node 4; nodes 2, and 3 receive it. Node 3, being a malicious node, does not check up with its routing table. Hence, it immediately replies back with a false RREP packet, claiming a shortest route to the destination. Node 1 Receives the RREP from 3 ahead of the RREP from 2. Node 1 assumes that the route through 3 is the shortest route and sends data packets to the destination through it. When the node 1 sends data to 3, it receives all the data and drops this data. As this data can not reach to the destination It is called as a Black hole attack. Due to this, source and destination nodes are unable to communicate with each other. The malicious node sends RREP as soon as it receives RREQ without performing standard procedures of AODV routing protocol, while keeping the Destination Sequence number very high. Since in AODV routing protocol RREP having higher value of destination sequence number is considered as fresh route, the RREP sent by the malicious node is treated fresh. So, by this way malicious nodes succeed in injecting Black Hole attack.

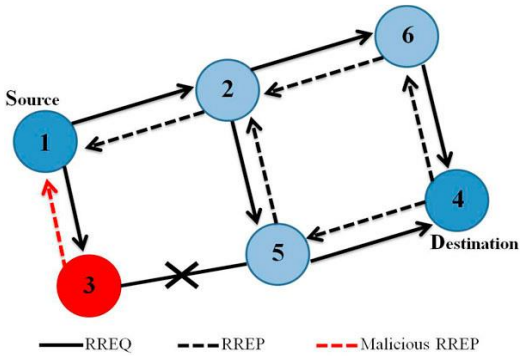

Fig.3 Black Hole Attack

2) Gray Hole Attack: A variation of black hole attack is gray hole attack, in which the nodes will forward the selective packets only and drop rest of the packets. Gray hole is a node that can switch from behaving normal to behaving like a black hole. So we can't identify the attacker easily since it behaves as a normal node. In MANET every node maintains a routing table that stores the next hop node information. Whenever a source node desires to route a packet to the destination node it uses a specific route that will be checked in the routing table whether it is available or not. When a node initiates a route discovery process to a destination node by broadcasting Route Request (RREQ) message to its neighbors, the intermediate nodes will update their routing tables on receiving the route request for reverse route to the source. A route reply message is sent back to the source node by destination node or by intermediate node(s) which has a current route to destination node. The gray hole attack completes in two phases:

Phase 1: A malicious node use the AODV routing protocol to show itself as having a valid route to destination node, with the intention of interrupting packets.

Phase 2: In this phase, packets has been selectively forwarded with a certain probability, that's why detection of gray hole attack is a difficult process. Normally in the gray hole attacks both normal node and attacker are same. Due to this it is very hard to find out in the network to figure out such kind of attacks.

D. Work Done on Black Hole Attack

1) Next Hop Information Based Method : Deng et.al [3] used Ad-hoc On-Demand Distance Vector (AODV) and proposed a solution for black holes attacks. They discussed a protocol that needs the intermediate nodes to send RREP message along with the next hop information. When the source node get this information, it sends a FREQ to the next hop to verify that the replied node (i.e. the node that just sent back the RREP packet) a route to the destination. When the next hop receives a FREQ, it sends a FREP which includes the check result to the source node. Based on information in FurtherReply, the source node judges the validity of the route. This approach helps to know the reliability of the replied node. In this protocol, the RREP control packet is modified to attach the information about next hop. Since, the source node will again send RREQ to the node specified as next hop in the received RREP, this exercise not only increases the routing overhead but also end-to-end delay. In addition, the intermediate node requires to send RREP message twice for a single route request. This method could prevent individual black hole attacks but cannot avoid cooperative attacks, where the next hop node cooperate with the replied node in malicious activity and reply with "yes " for FREQ sent by source node to it and the source node will trust on next hop and send data within the replied node.

2) Neighborhood-Based Method: Sun Guan and Chen [4] proposed a method using Ad-hoc On-Demand Distance Vector (AODV) as their routing protocol and claimed that the on-demand routing protocols such as DSR can also be suitably applied after a slight modification. The detection scheme deployed neighborhood-based technique to identify the black hole attacks and represent a routing recovery protocol to have a correct path to the destination. The neighborhoodbased method is employed to identify the unconfirmed nodes. They designed a method having two parts to mitigate black hole attack. These parts include detection and response. The authors simulated their work by NS2. In this scheme, not only a lower detection time and

higher throughput are acquired, but the accurate detection probability is also achieved to find black hole attack. The routing control overhead also does not increase in this techmique. The authors found that the amount of passing packet over the network might be enhanced by at least 15% and the false positive possibility will be less than 1.7%. It is found that this method will not work to detect black hole attack when that attacker decides to forge the fake reply packets selectively and also detection of cooperative black hole attack
was the next problem of this solution.

3) *Redundant Route and Unique Sequence Number Method:* Mohammad Al-Shurman and Park [5] propose two solutions to avoid the black hole attacks in MANET. The first solution will find more than one route (at least two routes) from the source node to the destination node. In other words, there exist some redundant routes within the routing path. The redundant route mechanism is: First, the source node sends a ping packet, and a RREQ packet, to the destination. The intermediate node who has a route to the destination will reply this request to source node. Then the source node start buffering the RREP packet until there are more than two received RREP packets, and then transmit these packets after identifying a safe route. It represents that there are at least two routing paths coexisting at the same time. After that, the source node recognizes the safe route from the number of hops or nodes, and mitigates the black hole attacks. In the second solution, the technique of unique sequence number is used. In this, two values are required to be recorded in two different tables. One is the last-packet-sequence-numbers for the last packet sent to every
node and the other is for the last packet received. Whenever any packet are transmitted to or received from, these two tables will be updated automatically. According to their values, the sender node can identify whether there is any malicious
nodes or not. They simulated the proposed approach on NS2. these techniques work with less numbers of RREQ and RREP in comparison with current AODV. It is found that solution two is better than solution one due to the inclusion of sequence number in every packet in the original routing protocol.
Both the solutions can't detect the cooperative black hole attacks.

4) *DRI Table and Cross Checking Scheme :*Sanjay Ramaswamy et al. [6,7] implemented data routing information (DRI) table and cross checking technique to identify the cooperative black hole nodes, and used modified Ad-hoc On-demand Distance Vector (AODV) routing protocol to build up this methodology.

All nodes need to have an extra DRI table, in which 1 represents for true and 0 for
false. The table has two entries, "From" to have the information on routing data packet from the node and "Through" to have the information on routing data packet through the node.

Node ID	**Routing Information**	
	From	**Through**
2	0	0
6	1	1

Table 1. DRI Table

As shown in Table 1, the entry 1 1 means that node 1 has routed data packet from or through node 6 successfully, and the entry of 0 0 means that node 1 has not routed any data packets from or through node 2. The course of action of proposed solution is described as follows. The source node sends Route Request (RREQ) message to each node and wait for Route Reply (RREP) message. Then it sends packets to the node which replies the Route Request (RREP) packet. The intermediate node then send next hop node (NHN) information and DRI table to the source node (SN). Now source node cross checks its own table and the DRI table received from the intermediate node to verify the IN's honesty. After that, source node sends the further request (FREQ) message to IN's next-hop-node for gathering
its routing information, including the current NHN, the NHN's Data Routing Information (DRI) table and its own DRI table. Lastly, the SN compares the above details by cross checking to judge the malicious nodes in the routing path. Authors proposed a detection method to mitigate the multiple black hole problems and the collaborative attacks, and showed the simulation result in [Paper_3_37]. The simulation result shows that the performance of this solution is almost 50% better than other solutions. However, it wastes 5 to 8% communication overhead, and increases the packet loss percentage very slightly as a delay to secure route discovery.

5) *Distributed Cooperative Mechanism (DCM):* Chang Wu Yu et al. [8] suggest a distributed and cooperative mechanism (DCM) to solve the collaborative black hole attacks. Since, nodes works cooperatively, they can detect, investigate, and mitigate multiple black hole attacks. The DCM has four phases: In the local data collection phase, each node in the network constructs and maintains an estimation table. Information of overhearing packets is evaluated by each node to find out whether there is any malicious node. If there is one

doubtful node, the detect node enters to the local detection phase to identify whether there is possible black hole. The initial detection node sends a check packet to ask the cooperative node. If it receives the positive inspection value, the doubtful node is regarded as a normal node. Otherwise the initial detection node runs the cooperative detection procedure, and deals with broadcasting and notifying all one-hop neighbors to participate in the decision making process. The network traffic is increased because the notify step utilizes broadcasting, Therefore, a constrained broadcasting algorithm is run to limit the notification range within a fixed hop count. A threshold say thr contains the maximum hop count range of cooperative detection message. Lastly, the global reaction phase is executed to set up a notification system to send warning messages to the whole network. Global reaction phase contains some reaction modes. Role of first reaction mode is to notify all nodes in the network, but it might waste lots of communication overhead. Each node maintains its own black hole list and arranges its data transmission route in other mode, however there is a chance to exploit this route by malicious nodes and requires more operation time. In the simulation outcome, the notification delivery ratio is from 64.12 (thr = 1) to 92.93% (thr = 3) when different threshold values are used. On Comparing with the popular AODV routing protocol in MANET, the result shows that DCM has a higher data delivery ratio and detection rate even if there are multiple black hole nodes. Even though the control overhead can be reduced by using distributed design method, DCM still wastes few overhead inevitably.

E. Work Done on Gray Hole Attack

1) Path Based Method: Jiwen CAI et.al suggested a path-based scheme to overhear the next hop's action [9]. In this method, a node does not observe every neighboring node, but only observes the next hop in recent route path. each node should keep a packet digest buffer say FwdPktBuffer. Whenever a packet is forwarded to, its digest is added into the FwdPktBuffer and the detecting node overhears. Once it is overheard that the next hop forwards the packet, the digest will be released from the FwdPktBuffer. The detecting node should calculate the overhear rate of its next hop in a fixed period of time, and compare it with a threshold. Author define overhear rate as (total overheard packet no/total forward packet no). In this method, every node only depends on itself to detect a gray hole. Routing Packet Overhead is not more, because algorithm does not send out extra control packets. Extensive amount of calculation is done in this method.

2) Optimal Route & Hash Based Method: Hizbullah Khatt ak et. al. [10] proposed a solution for the avoidance of black and gray hole attacks by leaving the first and choosing the second shortest path for data packets transmission [8] .First ,it prevents gray hole attacks by choosing the secure route for data packets transmission. Second, it gives more security for data integrity and detection of malicious node on the safe route. When source node receives Route Reply (RREP) messages from other nodes connected with destination node, it simply rejects the first RREP message coming from any intermediate node connected with destination node to avoid the black /gray hole. In this method, source selects second shortest route to transmit data packets to destination node rather than choosing the first optimal route. This solution avoids black hole / gray hole attacks by using the second shortest path for data packets transmission, so, it is tough for malicious node to check the entire network to know where to place itself in the network and deceive the source node by claiming that it has the second shortest route to the destination.

II. CONCLUSION

Due to the inherent design disadvantages of routing protocols and misbehavior of nodes have been caused Serious damage to the MANET and it has been attacked in the form of Black Hole, and Gray Hole attack. This paper presents a critical survey on detection and prevention methods of black & gray hole attack. MANET is an easy target for these attacks due to its limitations and weakness. It can be concluded, based on the survey, that detection and prevention methods developed so far are good to mitigate these attacks with some overheads and trade off such as energy consumption and performance of MANET. Future work is needed to improve and develop methods to mitigate these threats along with lesser amount of overheads and improved performance of MANET.

REFERENCES

[1] Ebrahim Mohamad, Louis Dargin. "Routing Protocols Security." In: Ad Hoc Networks". A Thesis at Oakland University School of Computer Science and Engineering.

[2] Dokurer,Seimih "Simulation of Black hole Attackin wireless ad-hoc Networks" Master's Thesis Atihm University,Septeber 2006

[3] Deng H., Li W. and Agrawal, D.P., "Routing security in wireless ad hoc networks," Communications Magazine, IEEE, vol.40, no.10, pp. 70- 75, October 2002

[4] Bo Sun,Yong Guan,Jian Chen,Udo W.Pooch "Detecting Black-hole Attack in Mobile Ad Hoc Network". 5th European Personal Mobile Communications Conference, Glasgow, April 2003 Volume 492, Issue, 22-25 pp. 490 – 495..

[5] Al-Shurman M, Yoo S-M, Park S (2004) Black Hole Attack in Mobile Ad Hoc Networks. Paper presented at the 42nd Annual ACM Southeast Regional Conference (ACM-SE'42), Huntsville, Alabama, 2-3 April 2004

[6] Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K (2003) Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks. Paper presented at the International Conference on Wireless Networks, Las Vegas, Nevada, USA, 23-26 June 2003
[7] Weerasinghe H, Fu H (2007) Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation. Paper presented at the Future Generation Communication and Networking, Jeju-Island, Korea, 6-8 December 2007
[8] Yu CW, Wu T-K, Cheng RH, Chang SC (2007) A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network. Paper presented at the PAKDD workshops, Nanjing, China, 22-25 May 2007
[9] 2010 24th IEEE International Conference on Advanced Networking and Applications An Adaptive Approach to Detecti Black and Gray Hole Attacks in Ad Hoc Network Jiwen CAI, Jialin CHEN, Zhiyang WANG, Ning LIU
[10] Preventing Black and Gray Hole Attacks in AODV using Optimal Path Routing and Hash. Hizbullah Khatt ak, Ni-zamuddin, F ahad Khurshid, Noor ul Amin 2013 IEEE