International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 1 119 – 124

A Review on Attacks in Mobile Ad hoc Network (MANET)

Amandeep Kaur Grewal
MTech, Department of Information Technology
Adesh Institute of Engineering & Technology,
Faridkot
ak.grewal10@yahoo.in

Asst. Prof. Gurpreet Singh
Adesh Institute of Engineering & Technology,
Faridkot
aiet.cse.gurpreet@gmail.com

Abstract: MANET (Mobile Ad hoc Network) is a wireless network having no any fixed infrastructure. It consists of autonomous, self-organized wireless mobile nodes, which are to move in or out in the network. MANET performs all the network activities such as message delivery, discovery of route path etc. using its nodes only. It uses the routing protocols such as DSDV, DSR and AODV etc. As there is no clear line of defense in MANET, so, it is more prone to both the legitimate users and the malicious nodes . The presence of these malicious nodes is one of the major the challenges in MANET and it has become necessary to design a very robust solution for the security of MANET. MANET is more vulnerable to attacks because of its openness, dynamic and infrastructure-less nature. The two types of routing attacks are , such as active i.e. Gray Hole Attack, Black Hole Attack, Flooding, Spoofing, Wormhole and passive i.e. Eavesdropping, Traffic Analysis. AODV is used to discover the path from source to destination but its more prone to malicious intent like gray hole and black hole attacks. Gray Hole attack tends to drop the packet while the routing process. In Black Hole attack, the malicious node presents itself as the shortest and newest route to the destination node and attracts the routing packets. This paper presents a focus on the fundamental issues in MANET by describing its related research in the previous year along with its concept, features and vulnerabilities.

KEYWORDS : *MANET, Black Hole, Gray Hole, Wormhole Attack, AODV.*

*****

1. INTRODUCTION

MANET is one of the most prevalent areas of Research and Development in the wireless networking. A MANET is infrastructure less dynamic network consisting of a collection of wireless mobile nodes that communicate with each other without the use of any centralized network [1]. It is decentralized IP based network of mobile machine nodes. MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an ―infrastructure less network [2].

MANET allows all the devices to detect other devices in its network and facilitate the communication between the devices and sharing of data and other services. This self-forming network provides the direct communication between the nodes that lie in the wireless transmission range of each other, but the nodes that lie outside this range depend on the intermediate nodes for the packet transmission. The nodes of MANET can both as host and router. An ad hoc network provides the nodal mobility, that is, adding and removing of the nodes easily from the network and also maintains connections of these nodes to the network.

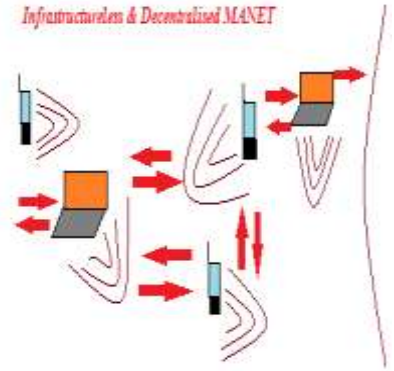

Fig.1 MANET

Because of the dynamic and nodal nature of the mobile ad hoc networks, these are more prone to the threats of malicious nodes. Being infrastructure less and decentralized, nodes can leave or join the network unpredictably over the time.

So, this gives chance to the attacker to become part of the network and carry out its malicious activities. Attacks in MANET could be classified as active and passive attacks.

Active attacks generally include either the creation of some false stream or modify the data stream. These can be internal or external. Active attacks are Gray Hole Attack, Black Hole Attack, Flooding, Spoofing, Worm hole.

Passive attacks do not halt completely the operation of a network but they snoop the confidentiality of the data. Passive attacks are Eavesdropping, Traffic Analysis.

2. MANET VULNERABILITIES

1. **Decentralized Administration**
   The configuration of MANET is not the centralized one. So, the detection and countering of the security attacks becomes difficult as it becomes difficult to monitor this rapidly changing nodal topology over time.
2. **Scalability**
   Mobile ad hoc networks are highly non-scalable networks because of the mobility of the nodes. In such a network security becomes the major of concern. Security mechanism should be easily applicable to both the large and small scale ad hoc networks.
3. **Cooperativeness**
   It is assumed by the routing algorithm of MANET that all the nodes of the network are cooperative and non-malicious. Due to which the malicious attacker can easily become part of the network and can halt the activities of the network.
4. **Dynamic Topology**

   The topology of the MANET is highly dynamic in nature, that is, nodes of the network are free to join or leave the network. This disrupts the trust relationship among the nodes by compromising the security of the network.

5. **Limited Power Supply**
   The nodes of the ad hoc network works in a very selfish manner when there is very limited power supply. Mechanisms should be employed to security from security threats and improving the power consumption.

6. **Resource availability**
   Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism [3].

3. GRAY HOLE ATTACK IN MANET

Gray Hole attack leads to the serious security breach in the working of the MANET operations. It is also known as routing misbehavior attack or packet drop attack. Gray Hole attack leads the dropping of the packets in two phases. In the first phase, the attacking node uses the Ad hoc On-Demand Distance Vector (AODV) protocol and will present itself as the node having the valid and fresh route to the destination. In the second phase, the node starts behaving maliciously by dropping certain packets and may behave as normal later on. It can behave both as normal and malicious node. So, it is very difficult to detect it in the network. It behaves as the normal node when it has the intention of intercepting the packets in the network and behaves as maliciously when it starts dropping the packets to some extent. It is also known as the variation in the Black Hole attack.

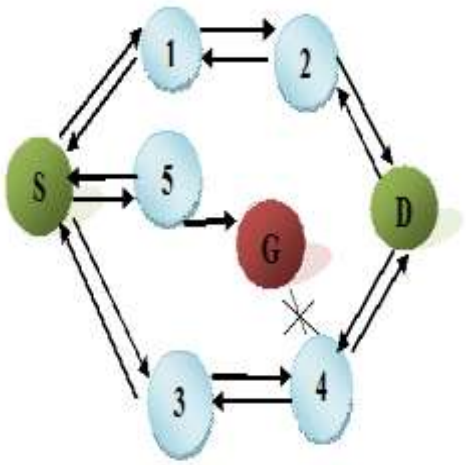

Fig.2 Gray Hole Attack in MANET

4. GRAY HOLE: LITERATURE REVIEW

Piyush et al. [4] presented a solution for providing end-to-end delivery of the packets. The solution is carried out by source and destination nodes, which checks if the data packets are reaches its destination point or not. If it is found that the packets do not reach their destination then the backbone network initiates a protocol for detecting more malicious nodes. The only limitation of this solution is that it is based on the assumption that every node in the network has trusted nodes as its neighbors than the malicious ones. So, this generally does not happen in most of the cases.

S.Banerjee et. al.[5] designed an algorithm for countering and removing of both the black and gray hole attacks in MANET. According to this algorithm, the complete data traffic is divided into small chunks so that the malicious nodes can be easily detected and removed. Flow of traffic is continuously checked by the neighbors of each node.

Destination node sends the acknowledgement number back to the source node, which enables the source node to check for the possibility of any malicious nodes. But this technique leads to some false attributes, that is , even when the node is not the malicious one, it may present it as the false one.

Mr. C.S. Dhamande et al [6] proposed a technique by visualizing the impact of gray hole attacks in MANET in terms of packet delivery ratio (PDR), network load and End to End delay and simulating its effects using Ad- hoc On Demand Vector (AODV) Routing protocol. He proposed the new technique by comparing the results of AODV protocol with and without Gray Hole attack. On the AODV protocol, he set the waiting time for receiving the RREQ (route request) on the source node SSN (source sequence number) , which is sent by the other nodes and then adding current time with this waiting time. Finally, all the RREQ destination sequence numbers (DSN) and their node ids are stored until the computing time exceeds.

Yang et. Al. [7] used the method local collaboration and information cross validation. In local collaboration, each node checks the routing table of every other node in the network to detect the misbehavior. Every node uses a token to validate itself to the network. If any node is found to be threatening to the network, then the other nodes will invalidate its token and add that threatening node to its token revocation list. Information cross-validation is used to cross-check the overheard transmission between the nodes by checking the routing packets of its neighbors.

P. Agrawal et. Al.[8] presented a mechanism of detecting he gray hole attacks using the concept of trustful nodes. Some extra nodes in the network are the strong nodes. These nodes monitor the Gray hole and Black hole attacks in the network. These nodes are considered to be the trustful nodes, which are capable of tuning their antennas to large and short ranges respectively. Every normal nodes fall inside the range these nodes. These strong nodes help to monitor if the data packets are reaching their destination or not by checking the number of data packets sent by the source and number of packets received at destination end. If there is any change in the number of packets sent and received, then strong nodes will start checking the monitoring result of each node. If some node shows the misbehavior, then a protocol is run by the network to detect the malicious node and finally, it announces it to the network by broadcasting messages.

Sarita Chaudhary et al [9] used the concept of maintaining the allocation tables. It broadcasts a message as a request for IP address, whenever it wants to add some new node to the network. The backbone node allots the new IP address to the node by randomly selecting the IP address, which is free in the network.

Sergio Martio et al [10] proposed a technique using the watchdog timer for detecting the malicious nodes. It is based on packet forwarding behavior or packet dropping rate within some predefined period of time. It counts the time that a packet takes while travelling from source to destination using the watchdog timer. It is a simple method of detecting the node's misbehavior. The only con is that the there is no any threshold value, so, it may lead to false interpretations to find the Gray Hole attacks.

5. BLACK HOLE ATTACK

In Black Hole Attack, the routing protocol like AODV is used by the attacker to advertise itself as the shortest path for sending the packets from source to destination. The attacker continuously checks for the route request message sent by the any node. When the attacker gets route request from the node from which it wants to intercepts the packets, it immediately presents itself as the shortest route to the destination by sending a fake route reply to the source node before the actual node could reply. So, the malicious node is able to put itself in between the source and destination node and can do malicious activity with the arriving packets, leading to the dropping of the packets.

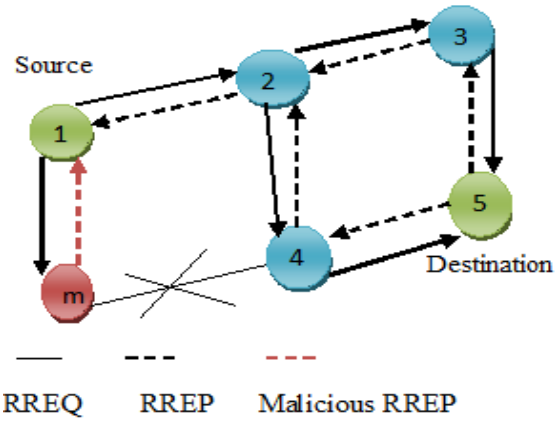

Fig. 3 Black Hole Attack in MANET

For example in the Fig:2 node

(1) i.e. the source node wants to send packets to the node

(2) .i.e. the destination node but the node

(3) In between the route is the malicious node will advertise itself as having the shortest route to node

(4) When once it is able to insert in between source and destination it can do anything with the packets.

6. BLACK HOLE: LITERATURE REVIEW

Deng [11] suggested technique for countering Black hole attacks using AODV protocol. RREP packet along with next hop information is sent by the intermediate nodes to the source node. Then the source node further sends a RREQ to the next hop of replied node for validating the replied node and route to the destination. It can only be used if the next hop is trusted completely. The only limitation is that it can be used for only individual attacks not for the cooperative Black hole attacks.

Payal, Swadas [12] used dynamic learning system on AODV protocol for detecting black hole attacks in MANET. When a node receives the RREP message, it first checks for the sequence number value in its routing table. The sequence number is compared with its threshold value, which is updated dynamically with time. If threshold value is lower than the sequence number, then the node is declared as the malicious. This method has improved the average end-to-end delay and normalized routing overhead. It cannot be used for cooperative attacks.

Chang, Rei Heng, Cheng, and Shun Chao Chang [13] used the cooperative procedure to detect the black hole attacks. Firstly, local problems are detected by each node. Then through the cooperative detective, sender sends message to the neighbor of infected node. The detecting node helps to find if the suspicious node is malicious one or not. If it is the black hole node, the entire network is made alert by sending warning message. It is useful for detecting individual black hole attack, but for cooperative attacks , this scheme becomes quite complex.

Hesiri Weerasinghe [14] proposed a mechanism to detect multiple black hole attacks. The black holes work together as the cooperatives ones. In this method, Data Routing Information (DRI) table and cross checking is used, using Further Request (FREQ) and Further Reply (FREP). This technique is used in order to produce the modified version of AODV protocol. It results in better performance in terms of throughput rate and lower packet loss rate. However, it cannot completely remove the cooperative black hole problem.

Rutvij, Sankita and Devesh [15] proposed detection mechanism of black holes in the network with the increase in packet delivery ratio (PDR) and lowered routing overhead. It is done by confirming the validity of routing information by the nodes receiving RREP packets.

While sending RREQ message to the other nodes, it also broadcasts the list of malicious nodes. Malicious nodes get isolated as the all the other nodes update their routing tables regarding the malicious nodes.

7. WORMHOLE ATTACK

In Wormhole Attack, firstly a tunnel is created between the false nodes. The malicious node will capture the packets from the legitimate node and transmit it to another false node in the network by encapsulating the data packet. The false nodes create a fake route, which will be shorter than the original route. Thereby, it creates misconception regarding the routing paths among the legitimate nodes.

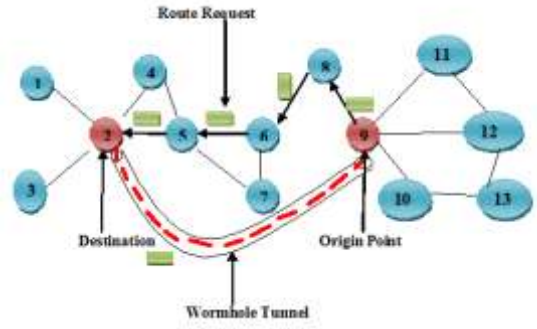

Fig.4 Wormhole Attack in MANET

8. WORMHOLE ATTACK : LITERATURE REVIEW

Ashish Kumar Jain[16] investigated a new solution by using trust based approach in MANET. In order to defend against the wormhole attack, he uses the combination of parameters like energy, number of connections and buffer length of a node. Trust value of node is computed based on these parameters. The proposed approach compares trust of each node with threshold value of the network trust. The result of this comparison clarifies that selected node is either fake or legitimate.

Darshana Sorathiya[17] used the path tracing algorithm and he used two parameters for finding wormhole link or path: 1) hop count 2) RTT (delay).They calculated delay/hop count ratio when RREP is received by the sender. When receiver gets back RREP message, source compare delay/hop count and then this ratio is compare with threshold value which previously counted by source. If this ratio is too large then simply discard RREP message.

Swaijit Kaushal[18] provides the information about wormhole attack and explains how to provide security to the path of the packets by using Delphi method. By using delay per hop method, nodes which can cause the wormhole attack can be isolated. With the help of hop count method and using the AODV routing protocol, the fake node can be

detected and a new path is formed to transfer the packets to their destination node.

In this way, packet loss problem can be reduced. The performance metrics used for evaluating network performance are packet loss, throughput and end to end delay.

9. DISCUSSION

Wireless networks are more prone to the security issues. MANET is a mobile network with no infrastructure and without a centralized server. Because of this, it is vulnerable to attacks like Gray Hole and Black Hole. These two attacks have been focused in this paper.

Various authors have proposed different techniques and mechanisms for detecting the Black hole and Gray Hole attacks. Gray Hole attacks can be countered using the SCAN approach, Watchdog timer, using local collaboration and information cross validation, using strong nodes etc. And Black Hole attacks can be detected and prevented using RREP and RREQ packets, Dynamic Learning System in AODV protocol, DRI tables and using intermediate nodes. There is still a lot to work in the area of detecting cooperative Black Hole attacks. Attacks that are to be countered and removed should not compromise with the performance of the network. It should have improved results in terms of the lowered packet dropping rate, maximizing the packet forwarding rate and decreasing the overhead issues in the MANET.

So, comparisons of various techniques of Gray Hole and Black Hole attacks have been presented in the form of tables given below.

Table1. Gray Hole Attack

Techniques for Gray Hole attack	Advantage	Disadvantage
Based on Source & Destination node	Provides end-to-end delivery of data packets.	Assumes that every node has trusted nodes as its neighbors.
Based on Data Traffic flowing in the network	Traffic divided into small chunks, attacks can be easily detected.	May lead to false attributes by showing a true node as the malicious one.
Based on waiting time in AODV protocol	Lowered the impact of Gray Hole attack by setting waiting time on SSN.	Difficult to manage routing entries.
Based on Local Collaboration & Information cross Validation	Uses SCAN approach by using tokens to validate a node. Each node uses a token which authenticates the node to the whole network.	Creates overhead because of using token for each node.
Based on Strong Nodes	Strong nodes decrease the number of monitoring of neighbors.	Assumes that strong nodes are trustable. There is no limit for detection of maliciousness of one node that increases mistakes.
Based on Allocation Tables	Detects Gray Hole attack allotting the IP address to new nodes.	Maintenance of Allocation Table is difficult.
Based on Watchdog Timer	Simple way of detecting Gray Hole attack by monitoring the packet forwarding rate using Watchdog Timer.	No use of any Threshold value to detect Gray Hole attacks.

Table2. Black Hole Attack

Techniques for Black Hole attack	Advantage	Disadvantage
Based on RREP and RREQ	Uses the RREP & RREQ messages for validating the nodes using AODV protocol.	Cannot detect cooperative Black Hole attacks. Also assumes that next node is trusted one.
Based on Dynamic Learning System	Sequence number compared with threshold value to detect the attack. Consumes no energy during monitoring.	May lead to false interpretations as node with higher sequence - number may be entered into blocked list.
Based on Cooperative Detective Nodes	Easy detection black holes by sending warning messages through cooperative detective nodes.	Detection for cooperative Black Hole attacks with this method becomes complex.
Based on DRI Tables	Detects cooperative Black Hole attacks through DRI tables & cross checking, using FREQ and FREP.	Creates huge overhead checking all nodes in a route. No prevention of Gray Hole attacks.
Based on Intermediate Nodes	Using intermediate node to detect malicious node i.e. the Cooperative Black Hole attacks and improved PDR.	Can still improve the performance.

CONCLUSION

In this paper, I have put forth a survey on countering and detection of Black Hole and Gray Hole attacks in mobile ad hoc networks. Black Hole, Gray Hole and Wormhole attacks are the security threats that cause a very breach in the MANET. Black Hole attack is when malicious node drops the packets by advertising itself as the shortest route to destination, whereas the Gray Hole attack is the special variation of Black Hole attack, which is very difficult to detect. Many researchers have proposed various methods and techniques to prevent and detect the Black Hole, Gray Hole Wormhole attacks, which are included in this paper. In our thesis we have analyzed the behavior and challenges of security threats in mobile ad hoc networks with solution finding technique.

REFERENCES

[1] Ravinder Kaur and Jyoti Kalra, "Detection and Pfrevention of Black Hole with Digital Signature", IJARCSSE, Vol.4, Issue 4, August 2014.

[2,3] Priyanka Goyal, Vinti Parmar and Rahul Rishi, "MANET : Vulnerabilities, Challenges, Attacks, Applications", IJCEM, Vol.11, January 2011

[4] Piyush Agrawal, R. K. Ghosh and Sajal K. Das, Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks, 2nd International Conference on Ubiquitous Information Management and Communication, pp. 310–314, (2008).

[5] 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.

[6] Dhamande C.S and Deshmukh H.R "A Competent to diminish the brunt of gay hole attack in MANET" Vol.2, Issue 2 Mar 2012.

[7] Yang, H., Shu, J., Meng, X., and Lu, S., "SCAN: Selforganized network-layer security in mobile ad hoc networks", IEEE journal, Vol. 24-No. 2, pp. 261-273, Feb-2006.

[8] P. Agrawal, R. K. Ghosh and S. K. Das, "Cooperative black and gray hole attacks in mobile ad hoc networks", In Proceedings of the 2nd International Conference on Ubiquitous Information Management and Communication,pp.-310-314,January-2008.

[9] Sarita Chaudhary, Kriti Sachdeva, "Discovering a secure path in MANET by avoiding black/ gray holes", International journal of recent technology and engineering, ISSN: 2277-3878, volume-1, Issue 3, Aug 2012.

[10] Sergio Marti, T.J.Giuli, Kevin Lai, Mary Baker," Mitigating Routing Misbehavior in Mobile Ad-hoc Networks" , Department of Computer Science, Stanford University, Stanford, CA 94305 U.S.A.

[11] . Deng H, Li W, Agarawal DP (2002) Routing Security in Wireless Ad-hoc Networks. IEEE Communications Magazine 40(10):70–75. do: 10.1109/MCOM.2002.1039859.

[12] Payal N. Raj, Prashant B. Swadas "DPRAODV: A Dynamic Learning System against Blackhole Attack in Aodv Based Manet" IJCSI International Journal of Computer Science Issues, Vol. 2, pp 54-59 2009

[13] . Chang Wu Yu, Wu T-K, Cheng RH, Shun chao chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network", Emerging Technologies in knowledge Discovery and Data Mining, Vol. 4819, Issue 3, pp 538-549,2007.

[14] Hesiri Weerasinghe , 2011, on Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks Proceedings of the IEEE International Conference on Communications, Jun. 24-28.

[15] . Rutvij H. Jhaveri , Sankita J. Patel. (2012). DoS Attacks in Mobile Ad-hoc Networks: A Survey. 2012 Second International Conference on Advanced Computing & Communication Technologies. 2 (2), p535-540.

[16] Ashish Kumar Jain, Ravindra Verma,"Trust - Based solution for Wormhole Attacks in Mobile Ad Hoc Network ",(GJMS), Volume-4, Issue-12, November- 2015

[17] Darshana Sorathiya, Haresh Rathod, "Algorithm to Detect and Recover Wormhole Attack in MANETs ", (IJCA), Volume 124, No. 14, 2015

[18] Swaijit Kaushal , Reena Aggarwal, "Avoidance of Wormhole Attack by using Delphi method", (IJRET), Volume: 02 Issue: 07 , Oct-2015