Security Issues in MANET: A Review of Black Hole Attacks in MNET

[1]Anshita Dharmawat, [2]Dr. Sanjay Agal
[1]Pacific University, Udaipur, Rajasthan, India
[2]Dr. V. R. Godhania College Of Engineering & Technology, Porbandar, Gujarat, India

Abstract
Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats.

Keyword
Black Hole Attack, MANET

I. Introduction

Previously the works done on security issues i.e. attack (Black Hole attack) involved in MANET were based on reactive routing protocol like Ad-Hoc On Demand Distance Vector (AODV). Black Hole attack is studied under the AODV routing protocol and its effects are elaborated by stating how this attack disrupt the performance of MANET. Very little attention has been given to the fact to study the impact of Black Hole attack in MANET using both Reactive and Proactive protocols and to compare the vulnerability of both these protocols against the attack. There is a need to address both these types of protocols as well as the impacts of the attacks on the MANETs.

II. Flaws in MANETS

MANETs are very flexible for the nodes i.e. nodes can freely join and leave the network. There is no main body that keeps watching on the nodes entering and leaving the network. All these weaknesses of MANETs make it vulnerable to attacks and these are discussed below.

A. Non Secure Boundaries:

MANET is vulnerable to different kind of attacks due to no clear secure boundary. The nature of MANET, nodes have the freedom to join and leave inside the network. Node canjoin a network automatically if the network is in the radio range of the node, thus it can communicate with other nodes in the network. Due to no secure boundaries, MANET is more susceptible to attacks. The attacks may be passive or active, leakage of information, false message reply, denial of service or changing the data integrity. The links are compromised and are open to various link attacks. Attacks on the link interfere between the nodes and then invading the link, destroying the link after performing malicious behavior.

There is no protection against attacks like firewalls or access control, which result the vulnerability of MANET to attacks. Spoofing of node's identity, data tempering, confidential information leakage and impersonating node are the results of such attacks when security is compromised [10].

B. Compromised Node:

Some of the attacks are to get access inside the network in order to get control over the node in the network using unfair means to carry out their malicious activities. Mobile nodes in MANET are free to move, join or leave the network in other words the mobile nodes are autonomous [11]. Due to this autonomous factor for mobile nodes it is very difficult for the nodes to prevent malicious activity it is communicating with. Ad-hoc network mobility makes it easier for a compromised node to change its position so frequently making it more difficult and troublesome to track the malicious activity. It can be seen that these threats from compromised nodes inside the network is more dangerous than attacking threats from outside the network.

C. No Central Management

MANET is a self-configurable network, which consists of Mobile nodes where the communication among these mobile nodes is done without a central control. Each and every node act as router and can forward and receive packets [12]. MANET works without any preexisting infrastructure. This lack of centralized management leads MANET more vulnerable to attacks. Detecting attacks and monitoring the traffic in highly dynamic and for large scale Ad-Hoc network is very difficult due to no central management. When there is a central entity taking care of the network by applying proper security, authentication which node can join and which can't. The node connect which each other on the basis of blind mutual trust on each other, a central entity can manage this by applying a filter on the nodes to find out the suspicious one, and let the other nodes know which node is suspicious.

D. Problem of Scalability:

In traditional networks, where the network is built and each machine is connected to the other machine with help of wire. The network topology and the scale of the network, while designing it is defined and it do not change much during its life. In other words we can say that the scalability of the network is defined in the beginning phase of the designing of the network. The case is quite opposite in MANETs because the nodes are mobile and due to their mobility in MANETs, the scale of the MANETs is changing. It is too hard to know and predict the numbers of nodes in the MANETs in the future. The nodes are free to move in and out of the Ad-Hoc network which makes the Ad-Hoc network very much scalable andshrinkable. Keeping this property of the MANET, the protocols and all the services that a MANET provides must be adaptable to such changes.

III. Classification of Attacks

The attacks can be categorized on the basis of the source of the attacks i.e. Internal or External, and on the behavior of the attack i.e. Passive or Active attack. This classification is important because the attacker can exploit the network either as internal, external or/ as well as active or passive attack against the network.

A. External and Internal Attack

External attackers are mainly outside the networks who want to get access to the network and once they get access to the network they start sending bogus packets, denial of service in order to disrupt the performance of the whole network. This attack is same, like the attacks that are made against wired network. These attacks can be prevented by implementing security measures such as firewall, where the access of unauthorized person to the network can be mitigated. While in internal attack the attacker wants to have normal access to the network as well as participate in the normal activities of the network. The attacker gain access in the network as new node either by compromising a current node in the network or by malicious impersonation and start its malicious behavior. Internal attack is more severe attacks then external attacks.

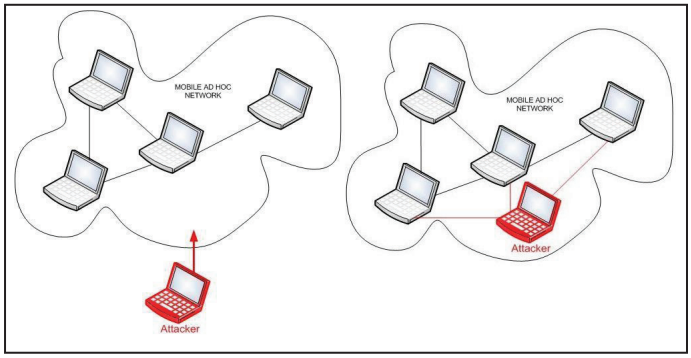

Fig. 1: External and Internal Attacks in MANETs

B. Active and Passive Attack

In active attack the attacker disrupts the performance of the network, steal important information and try to destroy the data during the exchange in the network [13]. Active attacks can be an internal or an external attack. The active attacks are meant to destroy the performance of network in such case the active attack act as internal node in the network. Being an active part of the network it is easy for the node to exploit and hijack any internal node to use it to introduce bogus packets injection or denial of service. This attack brings theattacker in strong position where attacker can modify, fabricate and replays the massages. Attackers in passive attacks do not disrupt the normal operations of the network [13]. In Passive attack, the attacker listen to network in order to get information, what is going on in the network. It listens to the network in order to know and understand how the nodes are communicating with each other, how they are located in the network. Before the attacker launch an attack against the network, the attacker has enough information about the network that it can easily hijack and inject attack in the network.

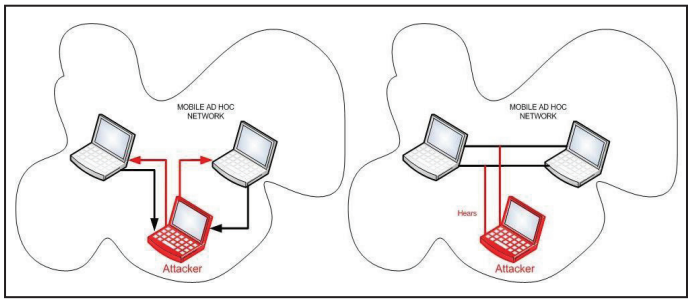

Fig. 2: Active and Passive Attack in MANETs

IV. Black Hole Attack in MANET

MANETs face different securities threats i.e. attack that are carried out against them to disrupt the normal performance of the networks. These attacks are categorized in previous chapter "security issues in MANET" on the basis of their nature. In these attacks, black hole attack is that kind of attack which occurs in Mobile Ad-Hoc networks (MANET). This chapter describes Black Hole attack and other attacks that are carried out against MANETs.

A. Black Hole Attack

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept.

This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [21]. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address [22].

The method how malicious node fits in the data routes varies. Fig. 3 shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost.

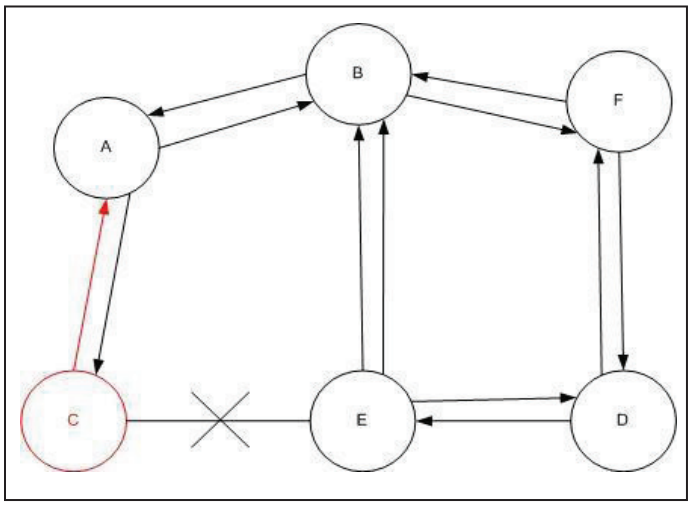

Fig. 3: Black Hole Problem

B. Black Hole Attack in AODV

Two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack.

1. Internal Black Hole Attack

This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node.

(i). External Black Hole Attack

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET. External black hole attack can be summarized in following points

1. Malicious node detects the active route and notes the destination address.
2. Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
3. Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
4. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node.
5. The new information received in the route reply will allow the source node to update its routing table.
6. New route selected by source node for selecting data.
7. The malicious node will drop now all the data to which it belong in the route.

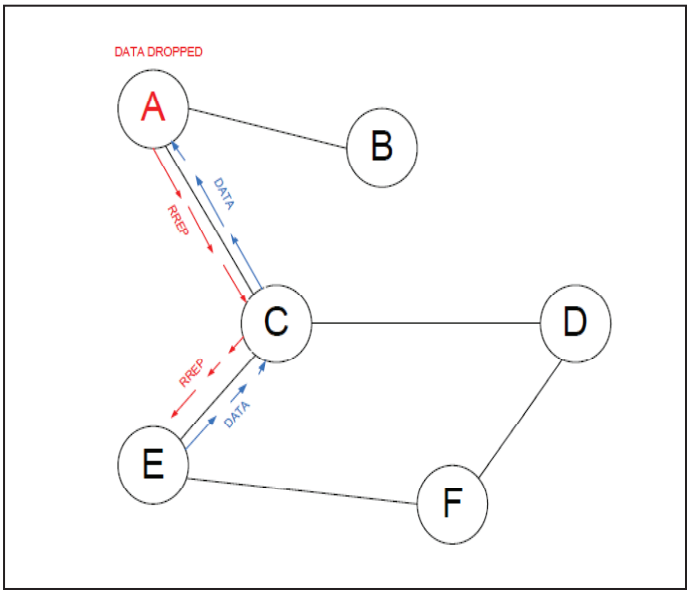

Fig. 4: Black Hole Attack Specification

In AODV black hole attack the malicious node "A" first detect the active route in between the sender "E" and destination node "D". The malicious node "A" then send the RREP which contains the spoofed destination address including small hop count and large sequence number than normal to node "C". This node "C" forwards this RREP to the sender node "E". Now this route is used by the sender to send the data and in this way data will arrive at the
malicious node. These data will then be dropped. In this way sender and destination node will be in no position any more to communicate in state of black hole attack.

2. Black hole attack in OLSR

In OLSR black hole attack, a malicious node forcefully selects itself as MPR which is discussed in chapter 3. Malicious node keep its willingness field to Will always constantly in its HELLO message. So in this case, neighbors of malicious node will always select it as MPR. Hence the malicious node earns a privileged position in the network which it exploits to carry out the denial of service attack.

The effect of this attack is much vulnerable when more than one malicious node is present near the sender and destination nodes.

V. Conclusion

Mobile Ad-Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. With the importance of MANET comparative to its vast potential it has still many challenges left in order to overcome. Security of MANET is one of the important features for its deployment. In our thesis, we have analyzed the behavior and challenges of security threats in mobile Ad-Hoc networks with solution finding technique.

Although many solutions have been proposed but still these solutions are not perfect in terms of effectiveness and efficiency. If any solution works well in the presence of single malicious node, it cannot be applicable in case of multiple malicious nodes. After studying all the approaches, our conclusion is that the approach offered by Deng suit well in our scenario. The intermediate reply messages if disabled leads to the delivery of message to the destination node will not only improve the performance of network, but it will also secure the network from Black Hole attack.

In our study we analyzed that Black Hole attack with four different scenarios with respect to the performance parameters of end-to-end delay, throughput and network load. In a network it is important for a protocol to be redundant and efficient in term of security. We have analyzed the vulnerability of two protocols OLSR and AODV have more severe effect when there is higher number of nodes and more route requests. The percentage of severances in delay under attack is 2 to 5 percent and in case of OLSR, where as it is 5 to 10 percent for AODV. The throughput of AODV is effected by twice as compare of OLSR. In case of network load however, there is effect on AODV by the malicious node is less as compare to OLSR.

Based on our research and analysis of simulation result we draw the conclusion that AODV is more vulnerable to Black Hole attack than OLSR.

References

[1] [Online] Available: http://en.wikipedia.org/wiki/Personal_area_network , last visited 12, Apr, 2010.
[2] [Online] Available: http://en.wikipedia.org/wiki/Mobile_ad_hoc_network, last visited 12, Apr, 2010.
[3] C.E.Perkins and E.M.Royer, "Ad-Hoc On Demand Distance Vector Routing," Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applictions, pp.90-100, Feb, 1999.
[4] C.M barushimana, A.Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad-Hoc Networks," Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-684, May, 2003.

[5] [Online] Available: http://www.faqs.org/rfcs/rfc3561.html
[6] M.Abolhasan, T.Wysocki, E.Dutkiewicz, "A Review of Routing Protocols for Mobile Ad-Hoc Networks," Telecommunication and Infromation Research Institute University of Wollongong, Australia, June, 2003.
[7] [Online] Available: http://www.faqs.org/rfcs/rfc3626.html
[8] [Online] Available: http://www.netmeister.org/misc/zrp/zrp.html#SECTION00041000000000000000, last visited 12 Apr, 2010.
[9] P.V.Jani,"Security within Ad-Hoc Networks," Position Paper, PAMPAS Workshop, Sept. 16/17 2002.
[10] M.Parsons, P.Ebinger,"Performance Evaluation of the Impact of Attacks on mobile Ad-Hoc networks".
[11] D.B.Roy, R.Chaki, N.Chaki,"A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-Hoc Neworks," International Journal of Network Security and Its Application (IJNSA), Vol. 1, No. 1, 2009.
[12] N.Shanti, Lganesan, K.Ramar,"Study of Different Attacks on Multicast Mobile Ad-Hoc Network".
[13] C.Wei, L.Xiang, B.Yuebin, G.Xiaopeng,"A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks", Second International Conference on Communications and Networking in china, pp. 366-370, 2007.
[14] S.Marti, T.J.Giuli, K.Lai, M.Baker,"Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks".
[15] Zhu, C. Lee, M.J.Saadawi, T.,"RTT-Based Optimal Waiting time for Best Route Selection in Ad-Hoc Routing Protocols", IEEE Military Communications Conference, Vol. 2, pp. 1054-1059, 2003.
[16] M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy,"A Reputation-Based Mechanism for Isolating Selfish nodes in Ad-Hoc Networks", Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, pp. 3-11, 2005.
[17] V.Mahajan, M.Natue, A.Sethi,"Analysis of Wormhole Intrusion attacks in MANETs", IEEE Military Communications Conference, pp. 1-7, 2008.
[18] F.Stanjano, R.Anderson,"The Resurrecting Duckling: Security Issues for Ubiquitous Computing," Vol. 35, pp. 22-26, 2002.
[19] H.L.Nguyen, U.T.Nguyen,"Study of Different Types of Attacks on Multicast in Mobile Ad-Hoc Networks", International Conference on Networking, Systems, Mobile Communications and Learning Technologies, 2006.