Security Issues In MANET and Black Hole Attack : A review

Naveen Hemrajani[1], Ashima Tiwari[2]
1. Professor, Dept. of Computer Science and Engineering, JECRC University, Jaipur.
2. M.Tech Scholar, Dept. of Computer Science and Engineering, JECRC University, Jaipur.

Abstract: An Ad Hoc Network, also termed as MANET (Mobile Ad Hoc Network) because of mobility of the nodes, is different from traditional fixed infrastructural approach. In MANET, access points are eliminated and thus it doesn't have any centralized monitoring point or fixed centralized management. The nodes rely on each other to create a network and change the topologies dynamically according to the routings. Along with these, some features of mobile ad hoc networks like open medium, having lack of clear line of defence and decentralized connections make them vulnerable to malicious attacks including Black Hole Attack, that is a simple but considerably effective Denial of Service attack.
In this paper a review on different security issues of MANET and understanding of Black Hole Attack is presented.

Keywords: Ad Hoc Network, MANET, Topologies, Black hole attack, Routing, Malicious nodes, Denial of Service.

1. Introduction:

A Mobile Ad Hoc network is an infrastructure less network which is a group of mobile nodes that are connected in a decentralized manner. The nodes can join or leave the network anytime thus have a dynamic approach of network topology [1]. Here nodes carry the responsibility of router and host both. It does not have any pre-existent infrastructure or centralized controller and the nodes in it rely on each other and can communicate with each other without the help of them. MANETs are efficiently used in the situations where wired or wireless infrastructure cannot be used. For example if an infrastructure is damaged or destroyed due to natural disasters, MANETs are used in rescue operations. Similarly if fixed infrastructure is inaccessible or overloaded in emergency, military or civilian environments, MANET can be used. It offers better coverage and higher throughput with lower operating cost.

2. Ad Hoc Network Threats And Security Issues:

With the help of routing protocols, nodes in a MANET exchange the information organizing the topology accordingly. This information can be sensitive and targeted by malicious adversaries with an objective to

intercept and harm the network or applications. There are two types of security attacks- Active and passive. In passive attack, the attacker does not affect the functionality of routers or we can say does not inject any kind of disturbance. It just spies on or monitors the routing. While in active attack, the attacker intercepts the routing by several means that can be done by impersonating the newly launched node, repeating the old data packets, disturbing the correct routing by faulty information etc. There are mainly two kinds of sources of MANET threats-

i). There can be attackers who attack from outside of the MANET, that is external attacks on a mobile ad hoc network by distortion, overload, redundancy and injecting false routing information.
ii). In second type of approach, sources of attacks are internal that means the compromised nodes can affect the data adversely to cause failure and can misuse the information of routing to other nodes [4].

There are many drawbacks of MANET that make it vulnerable to various malicious attacks. It doesn't have any
fixed infrastructure, nodes can leave and join the network anytime, dynamic topology, limited physical security, frequent routing updates and many other attributes are there due to which MANET often suffers with security attacks. Some main security issues are briefly described here-

- **Decentralized Connection:**
  Unlike the traditional approach of networks having a fixed infrastructure and central points (access points), MANET is connected in a decentralized manner [7]. It works without a pre-existent infrastructure. The nodes in it work as routers and host, forwarding and receiving the data packets. Due to this absence of a central management, detecting the attacks or monitoring the traffic is very difficult in large scale or highly dynamic MANETs.

- **Uncertain Boundaries:**
  Mobile Ad Hoc Networks do not have any clear or secure boundary. As the nodes can leave or join the network anytime and can communicate with other nodes in the network, it is not possible for a MANET to have certain boundaries. If a node is in the radio range of a MANET, it automatically joins it. This characteristic makes a MANET more susceptible to security threats. Network or the applications running in it can be disturbed through redundancy, distortion, leakage and injection of false information [5].

- **Dynamic Topology:**
  In MANET, nodes are free to frequently leave and join the network and move arbitrarily. Thus the routes change very often, changing the topology dynamically. These changes in nodes, routes and topologies are very frequent and unpredictable. This results as partitioning of network and cause loss of data packets affecting the integrity of information.

- **Scalability issues:**
  Mobile Ad Hoc Networks are quite different from the traditional approach of fixed networks, where the network is created by connecting the devices through wires so that one can define the network during the initial phase of design and it does not changes during the use. On the other hand, in MANETs nodes are free to move in and out of the network. Nobody can predict the number of nodes a MANET had in past or can have in future.

- **Compromised Node:**
  Compromised node is a node in MANET, on which the attackers get the control through unfair means with the intentions of performing malicious activities. The nodes in MANET are free to move and autonomous in nature. They cannot prevent the malicious activities they are communicating with.
  As the nodes can join and leave the network anytime, it becomes very difficult to track or monitor the malicious activity because the compromised node changes its position too frequently [6].

- **Physical Security Limitations:**
  MANET often suffers with security attacks. Mobility of nodes increases this possibility and makes it more susceptible to malicious activities. These attacks include monitoring of traffic with unfair intentions, denial of service attack in which a malicious node claims to be a different node to get the sensitive information, masquerading, spoofing etc.

- **Limited resources:**
  The nodes in a MANET rely only on battery power for energy means, as they do not have any centralized management. Bandwidth constraint also affects as they have lower capacity than that of the infrastructure based networks. MANETs have variable capacity links. Along with limited power, the storage capacity of a MANET is also limited.

3. Black Hole Attack:

Due to these above mentioned issues, MANET is susceptible to many security attacks. Black Hole Attack is one of these attacks. It is a simple but certainly effective Denial of Service attack[8] in which a malicious node, through its routing protocol, advertises itself for having the shortest path to the destination node or to the node whose packets it wants to intercept. It pretends to have enough of fresh routes for a certain destination. The source node assumes it to be true and the data packets are forwarded to a node which actually doesn't exist, causing the data packets to be lost. When a source node wants to initiate the communication, it broadcasts a RREQ message for route discovery. As soon as the malicious node receives this RREQ packet, it immediately responds with a false RREP message to the respective node advertising itself as the destination or having the shortest path for that destination. Since the malicious node needs not to check its routing table before responding to a

routing request, it is often the first one to reply compared

to other nodes. When the requesting node receives this RREP [9], it terminates its routing discovery process and ignores all other RREP messages coming from other nodes. Thus the data packets are sent to such a "hole" from where they are not sent anywhere and absorbed by the malicious node.

Often many nodes send RREQ simultaneously, the attacker node is still able to respond immediately with false RREP to all requesting nodes and thus easily takes access to all the routes. In this way source nodes are bluffed by malicious node which gulps a lot of network traffic to itself resulting severe loss of data. Black Hole nodes may also work as a group in a network. This kind of attack is called Collaborative Black Hole attack or Black Hole Attack with multiple malicious nodes[2][3].

4. AODV Protocol:

Avoidance and detection of Black Holes in the network, can be done by enhancement of AODV protocol that is used in MANET.

There are various routing protocols that are used in Ad Hoc Networks. These Protocols are affected by Black Hole Attack. AODV protocol is one of them. AODV stands for Ad hoc On demand Distance Vector Protocol.

In AODV, routing tables are updated when first packet is transmitted. For each route entry a destination sequence number is used. This number is generated by the destination when a connection is requested from it [10].

It is made sure that the route to the destination is the shortest path among all and also that it doesn't create any loop. The source wanting to initiate the communication broadcasts a RREQ message to all the nodes within a zone, and the node which is the destination itself or intermediate node having enough fresh routes and shortest path to the destination, unicasts a RREP message. Many nodes can respond to the requesting node according to their routing tables.

S. L. Dhende and Prof. Mrs. D. M. Bhalerao have presented a solution for mitigation and detection of black hole attack in their paper "A Mechanism for Detection of Black Hole Attack in Mobile Ad Hoc Networks", in which the data receiving nodes send an acknowledgement to transmitting node. Thus malicious node is recognized by getting no acknowledgement and the genuine path is used for transmission [11].

5. Conclusion:

Ad Hoc Network is independent of any fixed infrastructure or central management and have frequent routing updates which makes it easy to set up, low in cost, provides communication by wireless means with nodes working as routers as host. But along with advantages these features of MANET make it vulnerable to many active and passive security attacks, which affects the confidentiality, integrity and availability of data being transmitted. Black Hole Attack is one of these

effective attacks. It is an active and DoS attack. Here the attacker node causes loss of data by pretending to be a genuine node suitable for the requesting node. It then absorbs or sucks the data packets transmitted to it.

REFERENCES:

[1]. Charles E. Perkins, "Ad Hoc Networking", Addison- Wesley, Pearson edu., Jan. 2001.

[2]. Chang Wu Yu, Tung-Kuang Wu, Rei Heng Cheng, and Shun Chao Chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks", PAKDD 2007 Workshops, LNAI 4819, pp. 538–549, 2007

[3]. Santhosh Krishna B V, Mrs.Vallikannu A.L, "Detecting Malicious Nodes For Secure Routing in MANETS Using Reputation Based Mechanism" International Journal of Scientific & Engineering Research, Vol. 1, Issue 3, ISSN 2229-5518, December-2010.

[4]. Hao Yang et al., "Security in mobile ad hoc networks: challenges and solutions**"**, IEEE Wireless Communications, Volume 11, Issue 1, Page(s): 38 – 47, Feb. 2004.

[5]. M.Parsons and P.Ebinger, "Performance Evaluation of the Impact of Attacks on mobile ad hoc networks".

[6]. D.B.Roy, R.Chaki and 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, April, 2009.

[7]. N.Shanti, Lganesan and K.Ramar, "Study of Different Attacks On Multicast Mobile Ad Hoc Network".

[8]. The Ns-Manual By Kevin Fall and Kannan Vardhana , May 9, 2010

[9]. Nital Mistry, Devesh C Jinwala, Member, IAENG, Mukesh Zaveri" Improving AODV Protocol against Blackhole Attacks" Proceeding of International MultiConference of Engineers and Computer Scientists 2010 Vol II, IMESC 2010, March 17-19 2010,Hong Kong

[10]. Anu Bala, Jagpreet Singh and Munish Bansal "Performance Analysis of MANET under Blackhole Attack" First International Conference on Network and Communication 2009

[11]. S. L. Dhende1, Prof. Mrs. D. M. Bhalerao2 "A Mechanism for Detection of Black Hole Attack in Mobile Ad Hoc Networks", International Journal of Engineering, Science and Technology. ISSN: 2278-0181, Vol. 1 Issue 6, August – 2012