ISSN 2394-739X
International Journal for Research in Science Engineering and Technology

A survey on Different Security Attacks in MANET

[1] **V.SARAVANAN,**
[1] Associate Professor,
[1] Dept.of PG & Research in Computer Applications,

[2] **R. RAGHU,**
[2] M.Phil Research Scholar,
[2] Dept.of PG & Research Computer Science,

[1 & 2] Hindusthan College of Arts & Science.

Abstract:-

Mobile ad-hoc network (MANET) is one of the most promising fields for research and development of wireless network. As the popularity of mobile device and wireless networks significantly increased over the past years,wireless ad-hoc networks has now become one of the most vibrant and active field of communication and networks. Due to severe challenges, the special features of MANET bring this technology great opportunistic together.We found that many of the presently existing attacks have some commonfeatures and have been categorized into different attacks based on their minor differences.

Keywords: - [MANET Security, Security Attacks, different Routing attacks,]

1. INTRODUCTION

A mobile ad hoc network (MANET) is a self-configuring network of mobile nodes. It lacks any fixed infrastructure like access points or base stations. It lacks centralized administration and is connected bywireless links/cables.

Wireless ad hoc network can be build upwherethere is no support of wireless access or wired backbone is not feasible. All network servicesof ad hoc networkare configured and created on the fly. Thus it is obvious that with lack of infrastructural support and susceptible wireless link attacks, security in ad hoc network becomes inherent weakness.

Nodes within nomadic environment with access to common radio link can easily participate to set up ad hoc infrastructure. But the secure communicationamong nodes requires the secure communication link to communicate. Before establishing secure communication link the node Should be capable enough to identify another node. As a result node needs to provide his/heridentity as well as associated credentials to another node. However delivered identity and credentials need to be authenticated and protected so that authenticity and integrity of delivered identity and credentials cannot be questioned by receiver node.

The proliferation of cheaper, small and more powerful devices make MANET a fastest growing network. An ad-hoc network is self-organizing and adaptive. Device in mobile ad hoc network should be able to detect the presence of other devices and perform necessary set up to facilitate communication and sharing of data and service. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. Due tonodal mobility, the network topology may change rapidly and unpredictably over time. The network is decentralized, where network organization and message delivery must be executed by the nodes themselves.

Message routing is a problem in a decentralize environment where the topology fluctuates.

2. SECURITY THREATS IN MANAET

Ad hoc Networks are the networks formed for a particular purpose. These networks assume that an end to end path between the nodes exists. They are often created on –thefly and for one-time or temporary use. They find their use in special applications like military, disaster relief etc that arein a need of forming a new infrastructure less network with all pre-existing infrastructure being destroyed.Characteristics of Ad hoc networks include:

1) Lack of fixed infrastructure: An ad-hoc network is a collection of nodes that do not rely on pre -existing infrastructure for their connectivity. So these types of networks are flexible and easily reconfigurable.

2) Limited resources: Due to lack of fixed infrastructures, these networks have limited resources for their use. Resources like battery power, bandwidth, computation power, memory etc have to be used judiciously for the survival and proper functioning of the network.

3) Dynamic Topology: Nodes in the ad hoc networks are often mobile wireless devices like laptops, PDAs, smartphones etc resulting in frequent change of their location, resulting in a dynamic topology.

4) Autonomous Networks i.e. stand-alone self-organized system: Due to their decentralized nature, these networks eliminate the complexities of infrastructure setup, enabling devices to create and join networks "on the fly" anywhere, anytime, for any application. A node in the ad hoc networks can communicate with all other nodes which are in its transmission range. Nodes in the network are self-sufficient for the purposes like routing application messages, assuring security of the network and so on.

5) Cost effective: All the above described features make these networks cost effective by removing the necessity of servers, cables for internet connectivity, routers etc.

3. CLASSIFICATION OF ATTACKS

As previously discussed, we have categorized the presently existing attacks into two broad categories: DATA traffic attacks and CONTROL traffic attacks.This classification is based on their common characteristics and attack goals. For example: Black-Hole attack drops packets every time, while Gray-Hole attack also drops packets but its action is based on two conditions: time or sender node. But from network point of view, both attacks drop packets and Gray-Hole attack can be considered as a Black-Hole attack when it starts dropping packets. So they can be categorized under a single category.

Attacks

We can classify attacks as passive or active.

1. Passive attacks:

In a passive attack an unauthorized node monitors and aims to find out informationabout the network. The attackers do nototherwiseneed to communicate with the network. Hencetheydo not disrupt communications or cause any direct damage to the network. However, they can be usedto get information for future harmful attacks. Examples of passive attacks are eavesdropping and trafficanalysis.

Eavesdropping Attacks, also known as disclosure attacks, are passive attacks by external or internalnodes. The attacker can analyze broadcast messages to reveal some useful information about thenetwork. Solutions protecting the radio interface from attacks suchas eavesdropping(and jamming)attacks have been proposed in the literature, e.g. spread spectrum communication and frequencyhopping [3].Traffic Analysisis not necessarily an entirely passive activity. It is perfectly feasible to engage inprotocols, or seek to provoke communication between nodes. Attackers may employ techniques such asRF direction finding, traffic rate analysis, and time -correlation monitoring.

1. Traffic analysis in ad hoc networks may reveal:

- The existence and location of nodes;
- The communications network topology;
- The roles played by nodes;
- The current sources and destination of communications; and
- The current location of specific individuals or functions

Active Attacks:

These attackscauseunauthorized state changes in the network such as denial ofservice, modification of packets, and the like. These attacks are generally launched by users or nodeswith authorization to operate within the network. We classify active attacks into four groups: dropping,modification, fabrication, and timing attacks.

It should be noted that an attack can be classified into more than one group.

Dropping Attacks:

Malicious or selfish nodes deliberately drop all packets that are not destined forthem. While malicious nodes aim to disrupt the network connection, selfish nodes aim to preserve theirresources. Dropping attacks can preventend-to – endcommunications between nodes, if the droppingnode is at a critical point. It might also reduce the networkPerformance bycausing data packets to bere transmitted, new routes to the destinationto be discovered, and the like.Unfortunately most routing protocols (DSR is an exception [2]) have no mechanism to detect whetherdata packets have been forwarded or not. However, they can be detected by neighboringnodesthrough passive acknowledgement or hop-by-hop acknowledgement at the data link layer.An attacker can choose to drop only some packets to avoid being detected; this is called aselectivedropping attackbesides data packets or route discovery packets, an attacker can also drop route errorpackets, causing the source node to be unaware of failed links.

Modification Attacks:

Insider attackers modify packets to disrupt the network. For example, in thesinkhole attackthe attacker tries to attract nearly all traffic from a particular area through acompromised node by making the compromised node attractive to other nodes. It is especially effectivein routing protocols that use advertised information such as remaining energy and nearest node to thedestination in the route discovery process. A sinkhole attack can be used as a basis for further attackslike dropping and selective forwarding attacks. A black hole attack is like a sinkhole attack that attractstraffic through itself and uses it as the basis for further attacks.

The goal is to prevent packets beingforwarded to the destination. If the black hole is a virtual node or a node outside the network, it is hardto detect

Fabrication Attacks:

Here the attacker forges network packets. Fabrication attacks are classifiedinto “active forge” in which attackers send faked messages without receiving any related message and“forge reply” in which the attacker sends fake route reply messages in response to related legitimateroute request messages.

In the forge reply attack, the attacker forges a Route Reply message after receiving a Route Requestmessage.The reply message contains falsified routing information showing that thenode hasa freshroute to the destination node on AODVin ordertosuppress real routes to the destination.It causesroute disruption by causing messages to be sent to a nonexistent node or putting the attacker itself intothe route between two endpoints of a communication channel if the insider attacker has already have aroute to the destination.

Attackers can initiate frequent packets to cause denial of service (DoS). Example DoS attacksThatexploitMANETs' features are sleep deprivation torture attacks, routing table overflow attacks, ad hocflooding attacks, rushing attacks, and the like thesleep deprivation tortureattack consumes a node'sbattery power and so disables the node. It does so by persistently making service requests of one formor another.

The hello flood attackis another attack that makes theadversary attractive for many routes. In some routing protocols, nodes broadcast Hello packets todetect neighboring nodes. These messages are received by all one-hop neighbor nodes, but are notforwarded to further nodes. The attacker broadcasts many Hello packets with large enoughtransmission power that each node receiving Hello packets assumes the adversary nodeto be itsneighbor. It can be highly effective in both proactive and reactive MANET protocols.A further significant attack on MANETs is the collaborative.

4. ROUTING ATTACKS

There are severalattackswhich can bemounted on the routing protocols and may disruptthe proper operation ofthe network. Brief descriptions of such attacks are given below:

Routing Table Overflow: In the case of routing table overflow, the attacker creates routes to nonexistent nodes. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. In the case of proactive routing algorithms we need to discover routing information even before it is needed, whilein the case of reactive algorithmswe need to find a route only when it is needed. Thus main objective of such an attack is to cause an overflow of the routing tables, which would in turn prevent the creation of entries corresponding to new routes to authorized nodes.

Table Poisoning: IN routing table poisoning, the compromised nodes presentin the networks send fictitious routing updates or modify genuineroute updatepackets sent to other authorizednodes. Routing table poisoning may result in sub-optimal routing, congestion in portions of the network, or even make some parts of the network inaccessible.

Packet Replication: In the case of packet replication, an attackerreplicates stale packets. This consumes additional bandwidth and battery power resources available to the nodes and also causes unnecessary confusion in the routing process.

Route Cache Poisoning: In the case of on-demand routing protocols, each node maintains a route cache which holds information regarding routes that have become known tothe node in the recent past. Similar to routing table poisoning, an adversary can also poison the route Cache to achieve similar objectives.

Rushing Attack:On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack. An attackerwhich receives a routerequestpacket from the initiatingnode floods the packet quickly throughout the network before other nodes which also receive the samerouterequestpacket can react. Nodes that receive the legitimate routerequestpackets assume those packets to be duplicates of the packet already received through the attackerand hence discardthose packets. Any route discovered by the source node would contain the attackeras one of theintermediate nodes. Hence, the source node would not be able to find secure routes, that is, routesthatdo not include theattacker It is extremely difficult to detect such attacks in ad hoc wireless networks.

CONCLUSION

This paper presented a number of popular attacks like, active and passive attacks,routing table poisoning attack, impersonation and rushing attacks in MANETs. There is a need to make them more secure and robust to adapt to the demanding requirements of these networks. The flexibility, ease and speed with which these networks can be set up imply they will gain wider application. This leaves Ad-hoc networks wide open for research to meet these demanding application. The research on MANET security is still in its early stage. The existing proposals are typically attack-oriented in that they first identify several security threats and then enhance theexisting protocol or propose a new protocol to thwart such threats.

REFERENCES

[1]. Garg, R.P.Mahapatra.“MANET Security Issues”.IJCSNS International Journal of Computer Science and Network Security, Volume .9,No.8,2009.

[2]. Hoang Lan Nguyen, UyenTrangNguyen.“A study of different types of attacks on multicast in mobile ad hoc networks”.Ad Hoc Networks, Volume 6, Issue 1,Pages 32 -46, January 2008.

[3].F. Kargl, A. Geiß, S. Schlott,M. Weber. “Secure Dynamic Source Routing”.Hawaiian International Conference on System Sciences 38 Hawaii, USA, January 2005.

[4] M.A. Shurman, S.M. Yoo, and S. Park, “Black Hole Attack in Mobile Ad Hoc Networks,” ACM Southeast Regional Conference, pp. 96-97, 2004.

[5] J. CAI, P. YI, J. CHEN, Z. WANG, N. 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 (AINA),Perth, Australia, April 20-23, 2010, pp.775-780,.

[6] Y.C. Hu, A. Perrig and D. Johnson, “Rushing Attacks and Defense in Wireless Ad Hoc NetworkRouting Protocols,” Proceedings of the ACM Workshop on Wireless Security (WiSe), SanDiego, California, pp. 30-40, September 2003

[7] Rashid HafeezKhokhar, MdAsriNgadi&Satria Mandala,A Review of Current Routing Attacks inMobile Ad Hoc Networks,International Journal of Computer Science andSecurity, volume (2) issue (3).

[8] MahaAbdelhaq, Rosilah Hassan, Mahamod Ismail, RaedAlsaqour, DaudIsraf, Detecting Sleep DeprivationAttackover MANET Using a Danger Theory –Based Algorithm , International Journal on New ComputerArchitectures andTheir Applications (IJNCAA) 1(3): 534-541 The Society of Digital Information and Wireless Communications, 2011 (ISSN: 2220-9085).

[9] Rishabh Jain, CharulDewan, Meenakshi,A Survey on Protocols & Attacks in MANET Routing,IJCSMS International Journal of Computer Science & Management Studies, Vol. 12, Issue 03, September 2012ISSN (Online): 2231 –5268