ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 3, Issue 11, November 2016

A Survey on Security Attacks and countermeasures in Mobile Ad Hoc Networks

Sheetal. J
Asst. Prof, Department of Computer Science and Engineering,
Ballari Institute of Technology and Management, Ballari-583104,Karnataka,India.

Abstract: **-- The wireless Network is an emerging technology in the field of communication. The communication may take place between computers, networking nodes etc. A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobiles connected wirelessly. The best examples are routers in wired networks or access points in managed wireless networks. Mobile ad-hoc wireless networks (MANETs) exhibit high variability in network topology and communication quality. The network topology is dynamically changing and has no centralized administration. The nodes in the network are connected to transfer data, but the wireless channel suffers from attacks. Security plays an important role in mobile ad hoc network and is an essential requirement in MANETS. The wireless networks need more securitythan wired networks because it has limited resources. There are security issues and challenges. Some challenges here are dynamically changing network structure, limitations of mobile nodes, infrastructure less etc. Thispaper focuses on the routing attacks, as well as solutions against such attacks in existing MANET protocols.**

Keywords**:-- Mobile Ad Hoc Network (MANET), Security, Routing attacks, Communication, Topology, Infrastructure**

I. INTRODUCTION

MANET (Mobile Ad-hoc Network) is generally used wireless network. MANET is a self- organizing and decentralized system [2]. It consists of number ofwireless nodes that work together so that transmission is easy between the nodes in the system. Nodes communicate with each other using the direct shared wireless radio links [6].All the mobile nodes act as routers in the network [5]. Information in the form of packets is transmitted from source node to destination with the help of other nodes in the route. Due to open and dynamic nature,this network suffers from number of attacks.There are certain things that should be noticed like Route selection, Request initiation, topology used etc [7].

The MANETs work without a basestation where the nodes communicate with each other on the basis of mutual understanding. This makes MANET more easily to be exploited by an attacker inside the network. The attack on MANET is also possible with wireless links, which make it easier for the attacker to go into the network and access the ongoing communication. Mobile nodes that are present within the range of wireless link can overhear and participate in the network. Asecure way of transmission and communication must be there. This is a challenging and important issue due to increasing attacks on the Mobile networks. To provide secure communication & transmission, we must know different types of attacks and their effects on the MANET. A MANET is susceptible to security attacks because communication is based on mutual understanding between the nodes. There is no central station for network management, no authorization facility, dynamically changingstructure and limited resources.

II. WIRELESS MOBILE ADHOC NETWORK

Aninfrastructureless network that has dynamic topology is known as Mobile Adhoc network.The fundamental entity used here is known as sensor. This type of network combines different types of nodes andgateways. Due to the movement of the nodes in the network, itsupports the dynamic feature. The figure 2.1 shown belowis an example of the Mobile Adhoc network. lying on different computers as a computer network does not hide the existence of multiple computers. But a distributed system on the other hand provides the feeling that the user is working on a single homogenous more powerful computer with more resources.

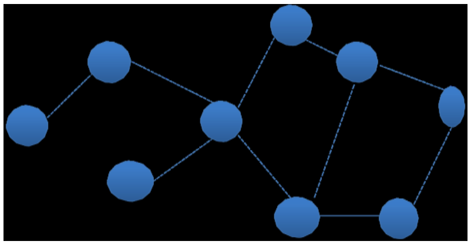

Fig.2.1 Mobile Adhoc network

2.1Security Goals in WSN

The important requirements and goals in securing mobile ad hoc networks are as follows [8] [9] [10].

Availability:The service should be available to the user at any time.

Authentication:It ensures that the sender is an authorized individual.

Integrity: During transmission, the message should not be changed or modified.

Non-Repudiation:No need to resend the message in the network

Confidentiality: It is concerned about the privacy and confirms that the computer resources can be accessed only by authorized parties.

III.ATTACKS

There are various attacks in the MobileAdhoc network. But there are two major classifications:

Internal attacks –These are direct attacks on the node present in the network and the links in between them.

External attack - External attacks are exhibited by nodes that are not the part of the network. The external attacks are classified in two categories: Active and Passive attacks. In active attack, the attacker or the maliciousnode takespartactively in the network. Here theattacker will alter the data packet and send thispacket into the network. The attacker can drop the data packet also. So,such types of attacks arevery harmful for the end users

On other hand the passive attack happens without altering the data packet [1]. Theattacker only analyzes the data. The main intention of this typeof attack is to destroy the confidentiality. Here, the attackertries to determine the activities of the network. It focuses onthe pattern to be sent in the network. On this basis, theattacker will perform illegal action. Detection of passiveattacks is cumbersome since the operation of the networkitself does not get affected.

3.1Active Attacks in Network Layers

Blackhole Attack:

In blackhole attack, a malignant node sends spurious routing information, claiming that it has best route and makes other nodes to route data packets through the malignant one. For example, in AODV (Ad-hoc On-demand Distance Vector), the attacker can send a fake RREP (Route Reply) to the source node, claiming that it has a fresh route to the destination node.This makes the source node to select the route that passes through the attacker. So, all traffic from the node will be routedthrough the attacker, and therefore, he can misuseor discard the traffic.

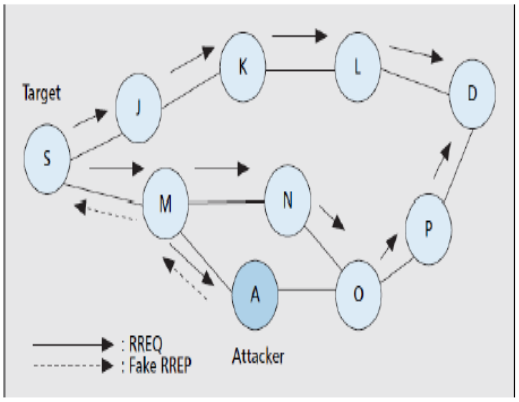

Fig 3.1 Example of Blackhole Attack

The above figure shows an example of a blackhole attack, where attacker A sends a dummy RREP to the source node S, claiming that it has a fresh route than other nodes. Since the sequence number enclosed by attacker is larger than other node’s sequence number, the source node S will select the route that passes through node A.

Countermeasures for Blackhole Attack

(i) Collect multiple RREP messages from more than two nodes and thus hoping many repeated paths to the destination node and then buffer the packets until a safe route is found.

(ii) In each node, maintain a table with previoussequence number in the incremental order. Before forwarding packets, each node increments the sequence number. The sender broadcasts RREQ(Route Request) message to its neighbors and when RREQ reaches the destination, it replies with a RREP includingfinal packet sequence number.If the intermediate node determines that RREP does not contain the correctsequence number, it understands that somewhere something went wrong.

Wormhole Attack:

In wormhole attack, malignant node receive data packet atsome point in the network and tunnels them to othermalignant node [4]. The tunnel existing between two malignantnodes is referred to as a wormhole. Wormhole attacks aresevere problems to mobile network routing protocols. Attackers usewormholes in the network to keep their nodes appearmore attractive so that large amount of data is routed through theirnodes. When the attacker uses wormhole attacks inrouting protocolslike DSR & AODV, the attackprevents the detection of routes other than through wormhole. If appropriate mechanism is not used in the network,then existing routing protocols cannot be used to discovervalid routes.

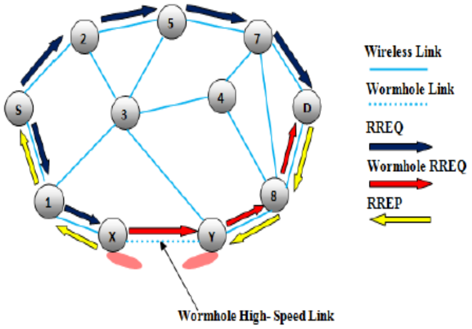

Fig 3.2 Example of Wormhole Attack

In fig 3.2, the nodes “X” and “Y” aremalignant nodes that form the tunnel in network. Thesource node “S” triggers the RREQ message to determinethe route to destination node “D”. The immediateneighbor of source S are“2” and “1” thattransfers the RREQ to their corresponding neighbours “5” and “X”. The node “X” when receives the RREQ, it immediately share with it “Y” and then sends RREQ to its neighbor node “8”, through which the RREQ is sent to the destination “D”. This causes the source node to select route <S-1-8-D>for destination. Thus “D” ignores RREQ that arrives afterwards and invalidates the actual route <S- 2-5- 7-D>.

Countermeasures for Wormhole Attack

TrueLink is a time based preventative countermeasure to this attack. To detect this attack, the Packet leashesalso are proposed.The information added to a packet that restricts the packet’s maximum allowed transmission length is called leash. Geographical leash ensures that the recipient of the packet is within a certain distance from the sender. Temporal leashassures that the packet has an upper bound of its lifetime (restricts the maximum travel distance).The SECTOR mechanism is proposed to detect wormholes without the need of clock synchronization. The other mechanism used to prevent this attack is Directional antennas.

Rushing Attack:

Generally, the on demand routing protocols suffer from this attack. These attacks destabilize the route discovery function. On-demand routing protocols that make use ofduplicate suppression during the route discoveryare vulnerable to thisattack. The compromised node when receives a route request packet from the source node, it transmits the packet quickly all over the network before other nodes, that also receive the same route request packet can react.

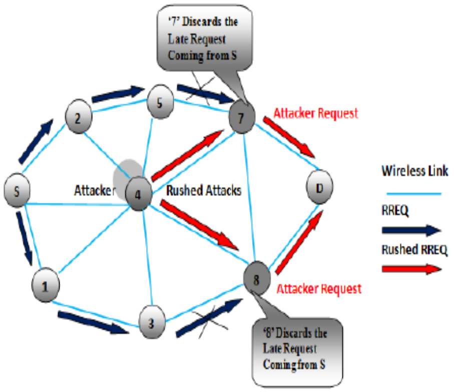

Fig 3.3 Example of Rushing Attack

In figure 3.3 the node "4" indicates therushing attack node, where "S" and "D" indicates source and destinationnodes respectively. The rushing attack of compromised node "4" quickly transmits the route request messages to ensure that the message from itself arrive earlier than those from other nodes. Whenneighbor nodesof "D", "7" and "8",take the route request from source, they discard requests. So in the presence of such attacks, "S" fails to determinesafe route without the involvement of attacker.

Countermeasures for Rushing Attack

SEDYMO: Secured Dynamic MANET On-Demand is same as DYMO but it says that intermediate node must add routing information while broadcasting and intermediate node should not delete any routing information from previous sender. It also uses hash chains and digital signature to secure the identity [4].

SRDP: Secure Route Discovery Protocol is security implemented Dynamic Source routing (DSR) protocol.

SND: Secure Neighbor Detection is other way of verifying everyneighbor's identity within a maximum transmission range.

Grayhole Attack

If a malignant node is deliberately misbehaving, Gray Hole attack may occur. A Gray hole is a type of the black hole attack, where the malignant node is not initially malicious but it turns hostile sometime later. The gray hole attack has two phases. In the first phase, a malicious node exploits the AODV protocol claiming that ithas a valid route to a destination node, with the intention of intercepting packets, even though the route is illegitimate. In the second phase, the node drops the intercepted packetswith a certain probability. This is more difficult to detect than the black hole attack where the malicious node drops the received data packets certainly. A gray hole may exhibit its hostilebehavior in different ways. It may drop packets coming from (or destined to) certain node(s) in the network while forwarding all the packets for other nodes [3]. Another type of gray hole node may act maliciously for some time duration by dropping packets but may switch to normal behavior later.

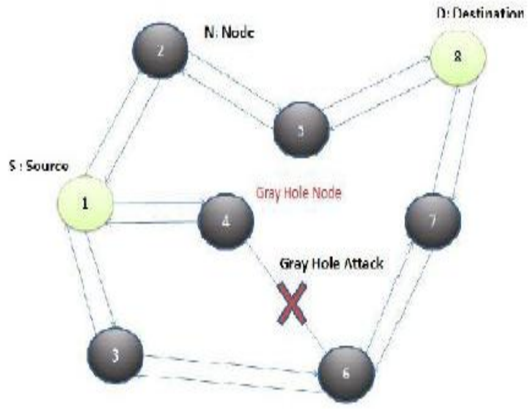

Fig 3.4 Example of Grayhole Attack

Fig 3.4 shows an example of gray hole attack on the adhoc network. In this figure node 1 act as a source node, node 8 acts as a destination node. Node 4 representsthe gray hole node in above diagram. Node 4 takes the packets from the neighboring node and drops the certain packets during the packet transmission.

Countermeasures for Gray hole Attack

Priority protocols schemes: Whenever a node enters Mobile Ad Hoc network, IP allocation is thefirst step in which the node receives its IP along with initialpriority and for this, we have adopted the technique of PrimeDHCP. Neighbor Discovery is the next step of theproposed scheme. New node will send the HELLO packets to its neighbors and determine the identity of the neighbours with their priority. Authentication is the further step of the scheme in which it will broadcast information regarding its existence and exchange keys with the neighbors according to the scheme HEAP which is a hopby hop authentication protocol. This authenticates packets at every hop by using a modified HMAC based algorithm with two keys and drops any packets that originate from outsides.

Sybil Attack

In Sybil attack, the attacker may generate fake identities of number of nodes. In this, a malicious node produces itself in a large number. The additional identities that the node acquires are called Sybil nodes. A Sybil node may construct a new identity for itself or it steals an identity of the legitimate node [4]. Afaulty node or an attackermay present multiple identities to a network in order to appear and function as multiple distinct nodes. After becoming part of the network, theattacker may then overhear communications or actmaliciously. By presenting multiple identities, the attacker will be able to control the network.

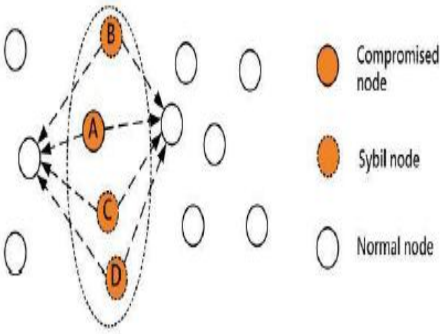

Fig 3.5 Example of Sybil Attack

Countermeasures for Sybil Attack

One way to overcome this attack is to maintain a chain of trust, so single identity is generated by a hierarchical structure which may be hard. Another approach would be based on signal strength. A robust Sybil attack detection framework is recommended for MANETs based oncooperative monitoring of network activities.Validation techniques can be used to avoid Sybil attacks and dismiss masquerading hostile entities. A local entity may accept a remote identity based on a central authority that ensures a one-to-one correspondence between an identity and an entity and may even provide a reverse lookup. An identity may be justified either directly or indirectly. In direct validation, the local entity informs the central authority to justify the remote identities. In indirect validation, the local entity depends on already accepted identities that in turn assurethe validity of the remote identity. A validation authority can attempt to preserve user's anonymity by refusing to perform reverse lookups, but this makes the validation authority a prime target for attack. Alternatively, the authority can use method other than knowledge of a user's real identity - such as verification of an unidentified human's physical presence at anappropriate place and time - to enforce a one-to-one correspondence between online identities and real-world users.

IV. CONCLUSION

Mobile Ad Hoc Network (MANET) is a kind of Ad hoc network with mobile, wireless nodes. Due to its special characteristics like open network boundary, dynamic topology and hop-by-hop communications MANET faces a variety of challenges. Since all nodes participate in communication and nodes are free to join and leave the network, security become the most important challenge in MANET.

In this paper, we discussed about the security of ad hoc networks. Lot of work is going on regarding the security attacks. This paper is a survey on various attacks occurring in MANET and the methods that are proposed to prevent security attacks.

REFERENCES

[1] Sachin Khasdev, Dr.VarshaNamdeo, Dr.TriptiArjariya, "Attacks and Security Issues over Mobile Adhoc Network", International Journal of Scientific Research Engineering Technology Volume 2, Issue 2, March-2016

[2] TharinduGuruge, P. J. K. Pathirathna, DhishanDhammearatchi, B. S. De. Silva & D. M. K. S. S. Dassanayake, "Security Attacks and Challenges in Mobile Ad-hoc Networks", Imperial Journal of Interdisciplinary Research (IJIR) Vol-2, Issue-5, 2016

[3] Ranjana Sharma, AnuradhaPanjeta, "A Survey on Trust Based Mobile Ad-hoc Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 6, June 2016

[4] R. DivyaParamesvaran, Dr. D. Maheswari, "Study of Various Security Attacks in Network Layer and the Mitigation Techniques for MANET", International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 2, February 2016

[5] R. Sudha, ,Dr. D. Sivakumar, "A Temporal table Authenticated Routing Protocol for Adhoc Networks", 978-1-4577-1894-6/11/$26.00©2011 IEEE

[6] Poonam, K. Garg, M. Misra, “Trust Based Multi Path DSR Protocol”, 2010 International Conference on Availability, Reliability and Security

[7] Nilesh N. Dangare M. Tech. (CSE) BDCOE, R. S. Mangrulkar, “Design and Development of Trust Based Approach to Mitigate Various Attacks in Mobile Ad-hoc Network”, International Journal of Computer Applications, International Conference on Quality Up-gradation in Engineering, Science and Technology (ICQUEST2015).

[8] Monika, Mr., Mukesh Kumar, and Rahul Rishi. "Security Aspects in Mobile Ad Hoc Network (Manets): Technical Review". International Journal of Computer Applications 12.2 (2010): 37-43.

[9] Al-Jaroodi, Jameela. "Routing Security in Open/Dynamic Mobile Ad Hoc Networks". The International Arab Journal of Information Technology, Vol 4.No.1 (2016)

[10] Chezhian, Umadevi, and ZaheerUddin Khan. "Security Requirements In Mobile Ad Hoc Networks". International Journal of Advanced Research in Computer and Communication Engineering Vol. 1. Issue 2 (2012)