A Review On Security Breaches In Mobile Ad-Hoc Networks

Sireesha Pendem
ECE,SVIT
Secunderabad, India

Alekya Ragukula
ECE,SVIT
Secunderabad, India

Prathibha Tandra
ECE,SVIT
Secunderabad, India

Suresh Kancharla
ECE,SVIT
Secunderabad, India

Abstract - *A mobile ad hoc network (MANET) is a dynamic wireless network that can be composed without any fine-tuned and preexisting infrastructure in which each node can act as a router. In MANET, security is an essential requisite. Compared to wired networks, MANETs are more vulnerably susceptible to security attacks due to the lack of a trusted centralized ascendancy and constrained resources. In this paper ,we categorically examined different routing attacks, such as black hole, impersonation, wormhole etc. These assailments are the major quandary in MANET because of different factor in MANET.*

Keywords: MANET, Survey, Security attacks.

I. I. INTRODUCTION

In a MANET, an accumulation of mobile hosts with wireless network interfaces form an ad interim network without the avail of any fine-tuned infrastructure or centralized administration. A MANET is referred to as an infrastructure less network because the mobile nodes in the network dynamically set up paths among themselves to transmit packets transitorily. In a MANET, nodes within each other's wireless transmission ranges can communicate directly; however, nodes outside each other's range have to rely on some other nodes to relay messages. Any routing protocol must encapsulate an essential set of security mechanism. These mechanisms are acclimated to avert, detect and respond to security attacks. There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment.

They are mainly:

(a)Confidentiality: Aegis of any information from being exposed to unintended entities. In ad hoc networks this is more arduous to achieve because intermediates nodes receive the packets for other recipients, so they can facilely eavesdrop the information being routed.

(b)Availability: Services should be available whenever required. There should be an assurance of survivability despite a Denial of Accommodation (DOS) attack. On physical and media access control layer assailant can utilize jamming techniques to interfere with communication on physical channel. On network layer the assailer can disrupt the routing protocol. On higher layers, the assailer could bring down high caliber accommodations.

(c)Authentication: Assurance that an entity of concern or the inception of a communication is what it claims to be or from. Without which an assailer would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

(d)Integrity: Message being transmitted is never altered.

(e)Non-repudiation: Ascertains that sending and receiving parties can never gainsay ever sending or receiving the message.

II.CHARECTERISTICS OF ATTACK:

Dynamic topology, distributed operation, and resource constraints are some of the unique characteristics that subsist in the ad hoc networks, which ineluctably increase the susceptibility of such network. Many characteristics might be habituated to relegate attacks in the ad hoc networks. Examples would include visually examining the deportment of the assailments (passive vs. active), the source of the assailments (external vs. internal).

III.EXTERNAL AND INTERNAL ATTACKS

External attacks are caused due to congestion, propagating fake routing information, disturbing the nodes from providing the services(denial of service.)Internal attacks directly leads to attacks on nodes present in the networks and links interface between them. Internal attacks are sometimes more difficult to external attacks because ,active attacks are occurs from more trusted nodes, malicious nodes are more difficult to identify.

IV. ACTIVE AND PASSIVE ATTACKS

passive assailments are launched when a intruder intercepts the data travelling through the network. Eves dropping, traffic analysis, monitoring are prevalent passive attacks. Detecting this kind of assailment is arduous because neither the system resources nor the critical network functions are physically affected to prove the intrusions [3].Here the requisite of confidentiality gets contravened. On the other hand active attacks actively alter the data with the intention to obstruct the operation of targeted networks. Message modification ,message replies, whereas, message fabrication are actions of active attacks where as denial of service(dos).

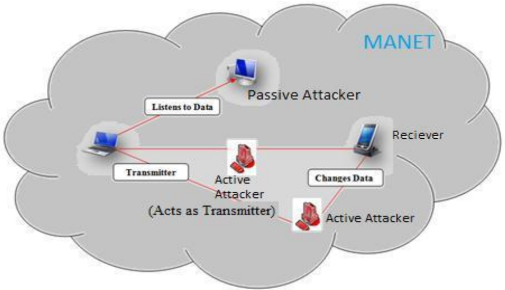

fig1:active and passive attacks

4.1 Eavesdropping:

Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks. It is defined as interception and reading of messages and information by unintended receivers. It aims to obtain some confidential information that should be kept secret during the communication. The information may include the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access.

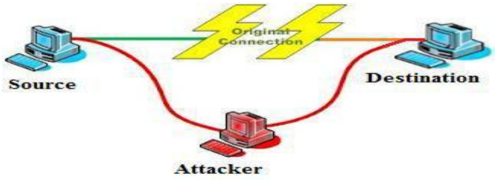

fig2:eavesdropping attack

4.2. Traffic Analysis & Monitoring:

Traffic analysis attack adversaries monitor packet transmission to infer important information such as a source, destination, and source-destination pair.

4.3 Jamming attack:

Jamming is the particular class of DoS attacks, which is initiated by the malicious nodes. The objective of a jammer is to interfere with legitimate wireless communications. A jammer can achieve this goal by either obviating an authentic traffic source from sending out a packet or by obviating the reception of legitimate packets. Jamming attack is a MAC layer attack.

4.4 Wormhole attack:

In the wormhole attacks, a compromised node in the ad hoc networks colludes with external attacker to create a shortcut in the networks. By creating this shortcut, they could trick the source node to win in the route discovery process and later launch the interception attacks. Packets from these two connections to create the fastest route from source to the destination node. In addition, if the wormhole nodes consistently maintain the bogus routes, they could permanently deny other routes from being established. As a result, the intermediate nodes reside along that denied routes are unable to participate in the network operation.

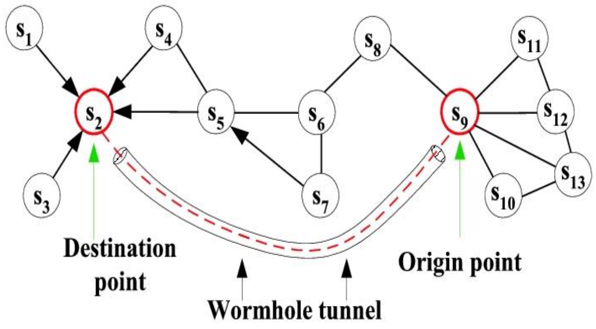

fig3: warm hole attack

4.5 Black hole attack:

The black hole attack has two properties. First, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, albeit the route is spurious, with the intention of intercepting packets. Second, the assailed consumes the intercepted packets without any forwarding. However, the assailant runs the peril that neighboring nodes will monitor and expose the perpetual attacks. There is a more subtle form of these assailant's when an assailant selectively forwards packets. An assailant suppresses or modifies packets originating from some nodes while leaving the data from the other nodes unaffected, which limits the suspicious malfeasance.

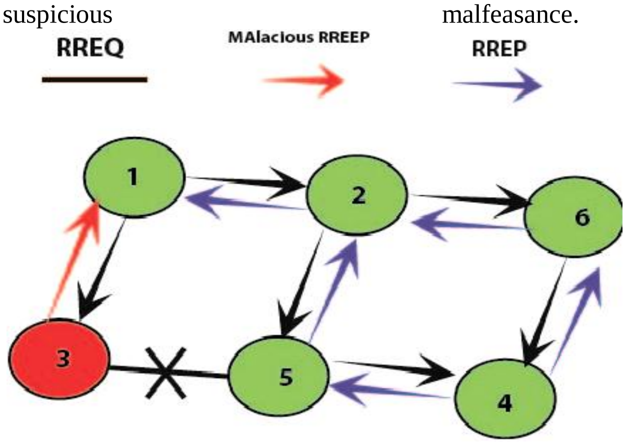

fig4: black hole attack

4.6 Byzantine attack:

A compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as engendering routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing accommodations.

4.7 Modification Attack:

In a message modification attack, assailer makes some changes to the routing messages, and thus imperils the integrity of the packets in the networks. Since nodes in the ad hoc networks are at liberty to move and self-organize, relationships among nodes at sometimes might include the malevolent nodes. These malevolent nodes might exploit the arbitrary relationships in the network to participate in the packet forwarding process and later launch the message modification attacks. Examples of attacks that can be relegated under the message modification assailants are impersonation attacks and packet misrouting: sink hole attacks are the examples of modification attacks.

fabrication attack: in fabrication attack, the attacker send fake message to neighboring nodes without receiving any related messages. the attacker can also send fake route reply messages in response to related legimate route request messages.

4.8 Slap Deprevatiomn Attack:

the aim of this kind of attack is to drain the resources in mobile ad-hoc nodes (e.g.; batteries) by constantly making them busy to run unnecessary units . This kind of attacks are mostly launched by flooding of packets to a particular node in routing protocol. For example attacker may send a huge number of route requests(RREQ) route replies(RREP) to a particular node. These kind of attacks are more specific to mobile networks.

4.9 sinkhole attack:

In sinkhole attack, a malicious node advertises the wrong routing information that itself advertising as a specific node and receives whole network traffic, and modifies the secret information. A malicious node will attract the secure information from all other nodes. In DSR protocol, sinkhole attack modifies the sequence in RREQ .

4.10 spoofing attack:

Fake links with neighbors advertized by malicious nodes will disrupt routing information. Resulting in malicious node manipulates data or routing traffic. It is also called link spoofing attack.

4.11 Gray hole attack:

We now describe the gray aperture attack on MANETS. The gray aperture attack has two phases. In the first phase, a malignant node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, albeit the route is spurious. In the second phase, the node drops the intercepted packets with a certain probability. This assailment is more arduous to detect than the ebony aperture attack where the malignant node drops the received data packets with certainly. A gray aperture may exhibit its malignant comportment in different ways. It may drop packets emanating from (or destined to) certain concrete node(s) in the network while forwarding all the packets for other nodes. Another type of gray aperture node may deport malevolently for some time duration by dropping packets but may switch to mundane deportment later. A gray aperture may withal exhibit a deportment which is an amalgamation of the above two, thereby making its detection even more arduous.

V.ROUTING ATTACKS:

There are several types of attacks mounted on the routing protocol which are aimed at disrupting the operation of the network. Sundry attacks on the routing protocol are described briefly below:

1) Routing Table Overflow: In this assailment, the assailant endeavors to engender routes to nonexistent nodes. The goal is to engender enough routes to obviate incipient routes from being engendered or to inundate the protocol implementation. Proactive routing algorithms endeavor to discover routing information even afore it is needed, while a reactive algorithm engenders a route only once it is needed. An assailer can simply send exorbitant route advertisements to the routers in a network. Reactive protocols, on the other hand, do not amass routing data in advance.

2) Routing Table Poisoning: Here, the compromised nodes in the networks send fictitious routing updates or modify genuine route update packets sent to other uncompromised nodes. Routing table poisoning may result in sub-optimal routing, congestion in portions of the network, or even make some components of the network inaccessible.

3)Packet Replication: In this assailment, an adversary node replicates stale packets. This consumes adscititious bandwidth and battery power resources available to the nodes and additionally causes dispensable mystification in the routing process.

4)Route Cache Poisoning: In the case of on-demand routing protocols (such as the AODV protocol [11]), each node maintains a route cache which holds information regarding routes that have become kenned to the node in the recent past. Akin to routing table poisoning, an adversary can withal poison the route cache to achieve homogeneous objectives.

5)Rushing Attack: On-demand routing protocols that use duplicate suppression during the route revelation process are vulnerably susceptible to this assailment. An adversary node which receives a Route Request packet from the source node floods the packet expeditiously throughout the network afore other nodes which withal receive the same Route Request packet can react. Nodes that receive the legitimate Route Request packets postulate those packets to be duplicates of the packet already received through the adversary node and hence discard those packets. Any route discovered by the source node would contain the adversary node as one of the intermediate nodes. Hence, the source node would not be able to find secure routes, that is, routes that do not include the adversary node. It is astronomically arduous to detect such attacks in ad hoc wireless networks.

6.Resource consumption attack

This is additionally kenned as the slumber deprivation attack. An assailant or a compromised node can endeavor to consume battery life by requesting exorbitant route revelation, or by forwarding nonessential packets to the victim node.

VI.TRANSPORT LAYER ATTACK

(a)Session Hijacking attack:

Session hijacking capitalizes on the fact that most communications are forfended (by providing credentials) at session setup, but not thereafter. In the TCP session hijacking attack, the assailant spoofs the victim’s IP address, determines the correct sequence number that is expected by the target, and then performs a DoS attack on the victim. Thus the assailer impersonates the victim node and perpetuates the session with the target.

(b)SYN Flooding attack:

The SYN flooding assailment is a denial-of-accommodation attack. The assailant engenders a sizably voluminous number of half-opened TCP connections with a victim node, but never consummates the handshake to planarity open the connection.

VII.APPLICATION LAYER ATTACKS

(a) Repudiation attack:In the network layer, firewalls can be installed to keep packets in or keep packets out. In the convey layer, entire connections can be encrypted, end-to-end. But these solutions do not solve the authentication or non-repudiation quandaries in general. Repudiation refers to a denial of participation in all or part of the communications.

CONCLUSION

Due to the dynamic infrastructure of MANETs and having no centralized administration makes such network more vulnerable susceptible to many assailants. In this paper, we discuss how different layers of protocol stack become vulnerable susceptible to sundry attacks. These assailments can be relegated as active or passive attacks. Different security mechanisms are introduced in order to obviate such network. In the future study, we will endeavor to invent such security algorithm, which will be installed along with routing protocols that avail to reduce the impact of different attacks.

References:

[1]Shin Yokoyama, Yoshikazu Nakane Osamu Takahashi, Eiichi Miyamoto, "Evaluation of the Impact of Selfish Nodes in Ad Hoc Networks and Detection and Countermeasure Methods",

[2]. JosephMacker and Scott Corson. Mobile ad-hoc networks(MANET).http://www.ietf.org/proceedings/ 01dec/183. htm, December 2001.

[3]. JosephMacker and Scott Corson. Mobile ad-hoc networks(MANET).http://www.ietf.org/proceedings/01 dec/183. htm, December 2001.

[4]. Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks ," Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp, @ 2006 Springer.

[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]. N.Shanthi, Dr.Lganesan and Dr.K.Ramar , "Study of Different Attacks on Multicast Mobile Ad hoc Network," Journal of Theoretical and Applied Information Technolog

[7].V. Madhu Viswanatham and A.A. Chari, "An Approach for Detecting Attacks in Mobile Adhoc Networks ," Journal of Computer Science 4 (3): 245-251, 2008 ISSN 1549-3636 © 2008 Science Publications.

[8]Hoang Lan and Uyen Trang Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad hoc Networks", Proceedings of ICNICONSMCL'06, 0-7695-2552-0/06@ 2006 IEEE.

[9].S. Murphy, "Routing Protocol Threat Analysis," Internet Draft, draft-murphy-threat-00.txt, Octomber 2002.

[10].P. Papadimitratos and Z.J.Haas, "Securing the Routing Infrastructure", IEEE Communications, vol. 10, no. 40. Octomber 2002, pp. 60-68.