INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

ATTACKS ON MOBILE AD HOC NETWORKS

MS. SUSHMA D. GHODE[1], MS. SHILPA D. GHODE[2]

1. Assist. Prof. Department of Information Technology, Priyadarshini Institute of Engg. & Tech. Nagpur

2. Assist. Prof. Department of Computer Science & Engineering, Kavikulguru Institute of Technology & Science, Ramtek.

Accepted Date: 15/02/2014 ; Published Date: 01/04/2014

Abstract: A mobile ad hoc network (MANET) is a dynamic wireless network that can be formed without any pre-existing infrastructure in which each node can act as a router. MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers. In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. Different mechanisms have been proposed using various cryptographic techniques to countermeasure the routing attacks against MANET. However, these mechanisms are not suitable for MANET resource constraints, i.e., limited bandwidth and battery power, because they introduce heavy traffic load to exchange and verifying keys. In this paper, the current security issues in MANET are investigated. Particularly, I have examined different routing attacks, such as flooding, blackhole, link spoofing, wormhole, and colluding miserly attacks, as well as existing solutions to protect MANET protocols. This paper presents several challenging issues and attacks in MANET.

Keywords: MANET, security attack, routing

PAPER-QR CODE

Corresponding Author: MS. SUSHMA D. GHODE

Access Online On:

www.ijpret.com

How to Cite This Article:

Sushma Ghode, IJPRET, 2014; Volume 2 (8): 672-681

INTRODUCTION

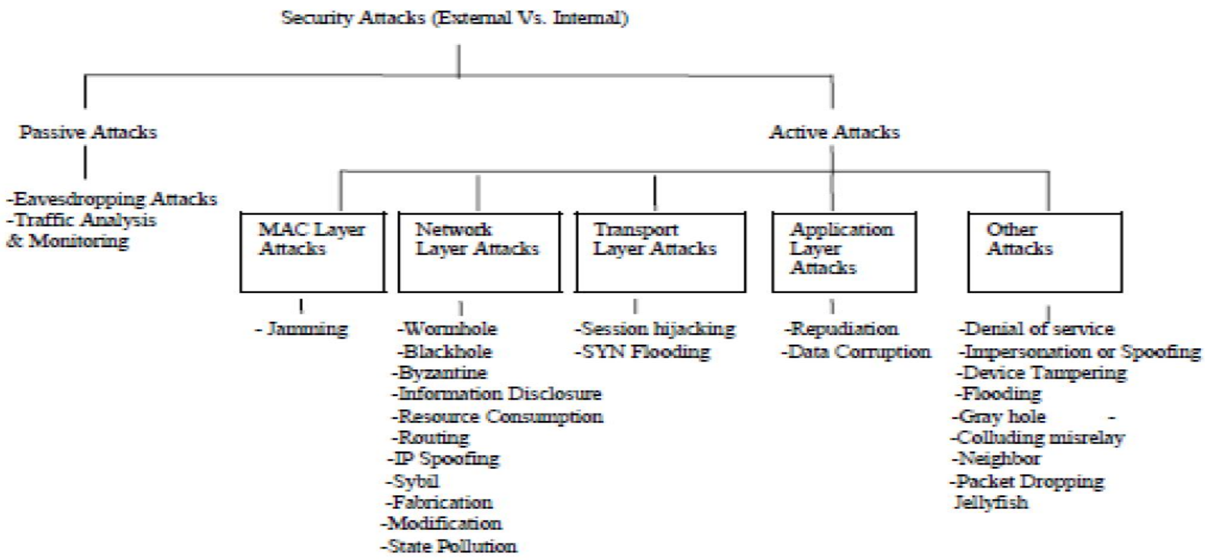
Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self configuration ability, they can be deployed urgently without the need of any infrastructure. There are 15 major issues and sub-issues involving in MANET [3] such as routing, multicasting/broadcasting, location service, clustering, mobility management, TCP/UDP, IP addressing, multiple access, radio interface, bandwidth management, power management, security, fault tolerance, QoS/multimedia, and standards/products. Currently, the routing, power management, bandwidth management, radio interface, and security are hot topics in MANET research.

Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs 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 MANETs against the security threats.

The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication [1, 2]. Mobile nodes present within the range of wireless link can overhear and even participate in the network.

I. SECURITY ATTACKS IN MANET

The malicious node(s) can attacks in MANET using different ways, such as sending fake messages several times, fake routing information, and advertising fake links to disrupt routing operations. In the following subsection, current routing attacks and its countermeasures against MANET protocols are discussed in detail. number of attacks that affect MANET as shown in Fig 1.here I have explained few of them. These attacks can be classified as follows [4]:



A. EXTERNAL AND INTERNAL ATTACK

External Attack: External attacks [7] are carried out by nodes that do not belong to the network. It causes congestion sends false routing information or causes unavailability of services.

Internal Attack: Internal attacks [7] are from compromised nodes that are part of the network. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyze traffic between other nodes and may participate in other network activities.

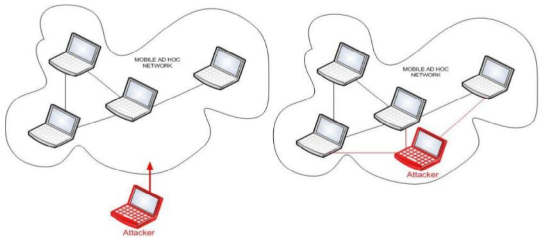


Fig. 2.1 External and Internal Attacks in MANETs

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 [6]. Active attacks can be an internal or an external attack [7]. 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 the attacker 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 [6].

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.

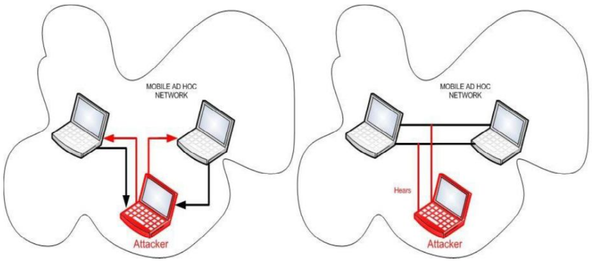


Fig. 2.2 Active and Passive Attack in MANETs

1) Eavesdropping

Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks. 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.

2) Traffic Analysis & Monitoring

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

3) Jamming attack

It is MAC layer attack. Jamming is the particular class of DoS attacks. The objective of a jammer is to interfere with legitimate wireless communications. A jammer can achieve this goal by either preventing a real traffic source from sending out a packet, or by preventing the reception of legitimate packets. In jamming, attacker initially keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered.

4) Wormhole attack

A wormhole attack [6] is one of the most sophisticated and severe attacks in MANETs. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network. In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunnelled. This tunnel between two colluding attacks is known as a wormhole [4].

5) Blackhole attack

In a blackhole attack [7], a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. 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 [5]. 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

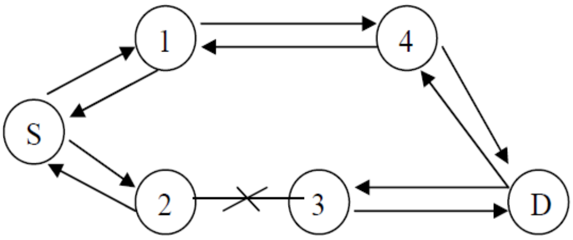


Fig. 2.3 Blackhole attack

6) Byzantine

A compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services [8].

7) Resource consumption attack

This is also known as the sleep deprivation attack [9]. An attacker or a compromised node can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to the victim node. **Sleep deprivation torture** These kinds of attacks are most specific to wireless ad hoc networks, but may be encountered in conventional or wired networks as well. The idea behind this attack is to request the services a certain node offers, over and over again, so it cannot go into an idle or power preserving state, thus depriving it of its sleep (hence the name). This can be very devastating to networks with nodes that have limited resources, for example battery power.

8) IP Spoofing attack

In conflict-detection allocation [8], the new node chooses a random address (say y) and broadcast a conflict detection packet throughout the MANET. Any veto from a node will prevent it from using this address. If the malicious node always impersonates a member that has occupied the same IP address and keeps replying with vetoes, it is called an IP Spoofing attack

9) State Pollution attack

If a malicious node gives incorrect parameters in reply, it is called the state pollution attack[8][9]. For example, in best effort allocation, a malicious allocator can always give the new node an occupied address, which leads to repeated broadcast of Duplication Address Detection messages throughout the MANET and the rejection of new node.

10) Sybil attack

If a malicious node impersonates some nonexistent nodes, it will appear as several malicious nodes conspiring together, which is called a Sybil attack [6]. This attacks aims at network services when cooperation is necessary, and affects all the auto configuration schemes and secure allocation schemes based on trust model as well. However, there is no effective way to defeat Sybil attacks.

11) Fabrication

Instead of modifying or interrupting the existing routing packets in the networks, malicious nodes also could fabricate their own packets to cause chaos in the network operations [6][7]. They could launch the message fabrication attacks by injecting huge packets into the networks such as in the sleep deprivation attacks. However, message fabrication attacks are not only launch by the malicious nodes. Such attacks also might come from the internal misbehaving nodes such as in the route salvaging attacks

12) Modification

In a message modification attack, adversaries make some changes to the routing messages, and thus endanger the integrity of the packets in the networks. Since nodes in the ad hoc networks are free to move and self-organize, relationships among nodes at some times might include the malicious nodes. These malicious nodes might exploit the sporadic relationships in the network to participate in the packet forwarding process, and later launch the message modification attacks [7].

13) Session Hijacking

Session hijacking takes advantage of the fact that most communications are protected (by providing credentials) at session setup, but not thereafter. In the TCP session hijacking attack, the attacker 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 attacker impersonates the victim node and continues the session with the target.

14) SYN Flooding

The SYN flooding attack is a denial-of-service attack. The attacker creates a large number of half-opened TCP connections with a victim node, but never completes the handshake to fully open the connection [7].

15) Repudiation

In the network layer, firewalls can be installed to keep packets in or keep packets out [6]. In the transport layer, entire connections can be encrypted, end-to-end. But these solutions do not solve the authentication or non-repudiation problems in general. Repudiation refers to a denial of participation in all or part of the communications. For example, a selfish person could deny conducting an operation on a credit card purchase, or deny any on-line bank transaction, which is the prototypical repudiation attack on a commercial system

16) Denial of service (DoS) attack

Denial of service (DoS) is another type of attack, where the attacker injects a large amount of junk packets into the network [6][7]. These packets overspend a significant portion of network resources, and introduce wireless channel contention and network contention in the MANET. A routing table overflow attack and sleep deprivation attack are two other types of the DoS attacks. In the routing table overflow attack, an attacker attempts to create routes to nonexistent nodes. Meanwhile the sleep deprivation attack aims to consume the batteries of a victim node.

S ↔A↔ B↔ M ↔C↔ D↔ X

17) Location disclosure attack

An attacker reveals information regarding the location of nodes or the structure of the network. It gathers the node location information, such as a route map, and then plans further attack scenarios. Traffic analysis, one of the subtlest security attacks against MANET, is unsolved [4]. Adversaries try to figure out the identities of communication parties and analyze traffic to learn the network traffic pattern and track changes in the traffic pattern. The leakage of such information is devastating in security sensitive scenarios.

18) Flooding attack

In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance [2][6]. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service.

19) Impersonation or Spoofing attack

Spoofing is a special case of integrity attacks whereby a compromised node impersonates a legitimate one due to the lack of authentication in the current ad hoc routing protocols. The main result of the spoofing attack is the misrepresentation of the network topology that may cause network loops or partitioning. Lack of integrity and authentication in routing protocols creates fabrication attacks that result in erroneous and bogus routing messages.

20) Gray hole attack

The gray hole attack has two phases. In the first phase, a malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the node drops the intercepted packets with a certain probability. This attack is more difficult to detect than the black hole attack where the malicious node drops the received data packets with certainly.: This attack is also known as routing misbehaviour attack [4][6] which leads to dropping of messages.

21) Neighbour attack

Upon receiving a packet, an intermediate node records its ID in the packet before forwarding the packet to the next node. However, if an attacker simply forwards the packet without recording its ID in the packet, it makes two nodes that are not within the communication range of each other believe that they are neighbours (i. e. one-hop away from each other), resulting in a disrupted route [6].

22) Jellyfish attack

Similar to the blackhole attack, a jellyfish attacker first needs to intrude into the forwarding group and then it delay data packets unnecessarily for some amount of time before forwarding them [7]. This result in significantly high end-to-end delay and thus degrades the performance of real time applications

23) Link spoofing attack

In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations.

24) Colluding misrelay attack

In colluding misrelay attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET. This attack is difficult to detect by using the conventional methods such as watchdog and pathrater [9].

25) Replay Attack:

An attacker that performs a replay attack are retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

26) Man- in- the- middle attack:

An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender.

Conclusion:

Due to the inherent design disadvantages of routing protocol in MANETs, many researchers have conducted diverse techniques to propose different types of prevention mechanisms for various attacks in MANET. This paper offers an explanation on which specific layer what type of attack can be executed and also what countermeasures can be taken in order to prevent this specific attack. Because MANET is a dynamic network, which has no antecedent and strictly defined infrastructure, there is also no clear line of defense. So in order to improve the level of security within MANET, the weaknesses of each layer should be handled.

REFERENCES:

1. P. V. Jani, “Security within Ad-Hoc Networks,” Position Paper, PAMPAS Workshop, Sept. 16/17 2002.

2. K. Biswas and Md. Liaqat Ali, “Security threats in Mobile Ad-Hoc Network”, Master Thesis, Blekinge Institute of Technology” Sweden, 22nd March 2007

3. C. R. Dow, P. J. Lin, S. C. Chen*, J. H. Lin*, and S. F. Hwang. A Study of Recent Research Trends and Experimental Guidelines in Mobile. Ad-hoc Networks. 19th International Conference on Advanced Information Networking and Applications, 2005. AINA 2005,Volume: 1, On page(s): 72- 77 vol.1.

4. Priyanka Goyal, Vinti Parmar, Rahul Rishi: MANET: Vulnerabilities, Challenges, Attacks, Application: IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011

5. Irshad Ullah Shoaib Ur Rehman: Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols: School Master Thesis Electrical Engineering Thesis no: MEE 10:62 June, 2010

6. C.Wei, L.Xiang, B.yuebin and 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, Aug, 2007.

7. Zdravko : Attacks on Mobile Ad hoc Netwoks: Integrate Information System,2008

8. Rashid Hafeez Khokhar; Md Asri Ngadi; Satria Mandala. A Review of Current Routing Attacks in Mobile Ad Hoc Networks. International Journal of Computer Science and Security, 2:12, 2008

9. Mihaela Cardei; BingWu; Jianmin Chen; JieWu. A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks. Wireless/Mobile Network Security, page 38, 2006.