A Review of Mobile Ad Hoc Network Attacks

Prof. S. A. Thakare Prof. S. R. Jathe Prof. Priti. H.Jadhav

Abstract Security is an essential requirement in mobile ad hoc network (MANETs). Compared to wired networks, MANETs are more vulnerable to security attacks due to the lack of a trusted centralized authority and limited resources. Attacks on ad hoc networks can be classified as passive and active attacks, depending on whether the normal operation of the network is disrupted or not. In this paper, we are describing the all prominent attacks.

Index Terms: MANET, Survey, Security attacks.

1. INTRODUCTION

In a MANET [1], a collection of mobile hosts with wireless network interfaces form a temporary network without the aid of any fixed 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 temporarily. In a MANET [2], 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 used to prevent, detect and respond to security attacks.

2. WEAKNESSES OF MANETs

Since nodes in mobile network can move freely, the network tends to change its topology very frequently. This mobile nature of the nodes may create many security[7],[8] and other issues in Manets –

- ***Lack of Centralized Management*** **-** Since Manets form a random network and even the nodes are mobile so there is no centre management. Due to lack of centralized management the detection of attacks is very difficult.
- ***Infrastructure less*** **-** Manets infrastructure less nature brings difficulty in detecting any malicious node or faults in the network.
- ***Dynamic Topology*** – Since Manets have a dynamic topology because the nodes are ever changing this may weaken the relationship among nodes.
- ***Packet Loss*** – There are many reasons of packet loss problem in Manets. Packet loss may happen due to mobility of nodes, bit rate error, due to interference.
- ***No network boundary*** – Since Manets have no network boundary because the nodes are movable this may lead to increase in number of attacks on them. Any node may enter the network and may hinder the network communication.
- ***Mobile Nodes-*** At times the mobile nature of nodes may even create network error. Since nodes can freely join or leave a network so it is easy for nodes to behave maliciously.
- ***Scalability*** – Due to mobility of network the scale of the network is changing all the time.
- ***Variation in nodes*** – Each node has different transmission and receiving capabilities. In addition each mobile node has different software/hardware configurations which cause trouble in operating in a network.
- ***Security*** – It is one of the major issue in mantes. All major networking tasks such as routing and packet formatting are done by nodes itself which are mobile. Any attacker can easily attack on the network and can acquire the data.
- ***Resource Availability*** – For manets providing secure communication in such a challenging environment where the network is mobile and is vulnerable to attacks requires various resources and architectures.

3. MANET SECURITY GOALS

There are five major security goals that need to be

- Prof. S. A. Thakare, Assistant Professor, JDIET, Yavatmal (MS), India.
- Prof. S. R. Jathe Assistant Professor, Govt .Poly Jintur (MS), India.

addressed in order to maintain a reliable and secure[3],[9] ad-hoc network environment. They are mainly:

Confidentiality: Protection of any information from being exposed to unintended entities. In ad hoc networks this is more difficult to achieve because intermediates nodes receive the packets for other recipients, so they can easily eavesdrop the information being routed.

Availability: Services should be available whenever required. There should be an assurance of survivability despite a Denial of Service (DOS) attack[11]. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services.

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

Integrity: Message being transmitted is never altered.

Non-repudiation: Ensures that sending and receiving parties can never deny ever sending or receiving the message.

4. ATTACKS ON MANET

The security[5] goals of MANETs are not that different from other networks: most typically authentication, confidentiality, integrity, availability, and nonrepudiation. Authentication is the verification of claims about the identity of a source of information. Confidentiality means that only authorized people or systems can read or execute the protected data or programs. It should be noted that the sensitivity of information in MANETs
may decay much more rapidly than in other information.The characteristics of MANETs make them susceptible to many new attacks. At the top level, attacks can be classified according to network protocol stacks. Table 4.1 gives a few examples of attacks at each layer. Some attacks could occur in any layer of the network protocol stack, for example, jamming at physical layer, hello flood at network layer, and SYN flood at transport layer— all are DoS attacks. Because new routing protocols introduce new forms of attacks on MANETs, we mainly focus on network layer attacks.

Table 4.1: Some Attacks on the Protocol Stack

Layer	Attacks
Application Layer	Data corruption , viruses and worms
Transport Layer	TCP/UDP Sync Flood
Network Layer	Hello Flood , Blackhole
Data Link Layer	Monitoring , Traffic Analysis
Physical Layer	Eavesdropping , active interference

Attackers against a network can be classified into two groups: insider and outsider. Whereas
an outsider attacker is not a legitimate user of the network, an insider attacker is an authorized node and a part of the routing mechanism on MANETs. Routing algorithms are typically distributed and cooperative in nature and affect the whole system. Although an insider MANET node can disrupt the network communications intentionally, there might be other reasons for its apparent misbehaviors. A node can be failed, unable to perform its function for some reason, such as running out of battery, or collusions in the network. The threat of failed nodes is particularly serious if they are needed as part of an emergency/secure route. Their failure can even result in partitioning of the network, preventing some nodes from communicating with other nodes in the network. We should also consider the misuse goals of attackers. In routing attacks, attackers do not follow the specifications of routing protocols and aim at disrupting the network communication in the following ways:

- **Route disruption***:* modifying existing routes, creating routing loops, and causing the packets to be forwarded along a route that is not optimal, nonexistent, or otherwise erroneous.
- **Node isolation***:* isolating a node or some nodes from communicating with other nodes in the network, partitioning the network, and so on.
- **Resource consumption***:* decreasing network performance, consuming network bandwidth or node resources, and so on.

5. TYPES OF SECURITY ATTACKS

External vs. Internal attacks

External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services. Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors

The security attacks[4],[6] in MANET can be roughly

classified into two major categories, namely passive attacks and active attacks are as described in the figure 1.The active attacks further divided according to the layers.

6. Passive Attacks

6.1 Traffic Analysis & Monitoring

Traffic Analysis is not necessarily an entirely passive activity. It is perfectly feasible to engage in protocols, or seek to provoke communication between nodes. Attackers may employ techniques such as RF direction finding, traffic rate analysis, and time-correlation monitoring. For example, by timing analysis it can be revealed that two packets in and out of an explicit forwarding node at time t and t+€ are likely to be from the same packet flow . 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 (e.g. if the commander issues a daily briefing at 10am, traffic analysis may reveal a source geographic location).

6.2 Eavesdropping

Eavesdropping attack is the process of gathering information by snooping on transmitted data on legitimate network. Eavesdrop secretly overhear the transmission. However, the information remains intact but privacy is compromised. This attack is much easier for malicious node to carry on as evaluate to wired network. Eavesdropping attack in MANET shared the wireless medium, as wireless medium make it more vulnerable for MANET malicious nodes can intercept the shared wireless medium by using promiscuous mode which allow a network device to intercept and read each network packet that arrives.

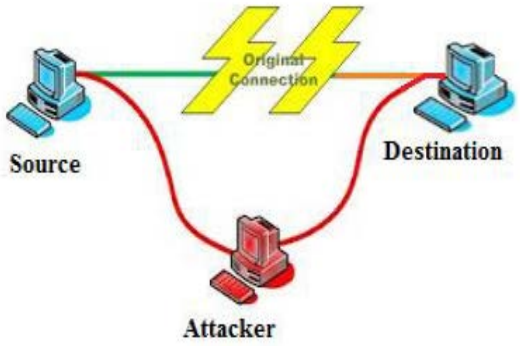

Fig 6.1: Eavesdropping Attack

7. ACTIVE ATTACKS

These attacks cause unauthorized state changes in the network such as denial of service, modification of packets, and the like. These attacks are generally launched by users or nodes with 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.

7.1 Blackhole attack

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. 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. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address. The method how malicious node fits in the data routes varies. Fig. 7.1 shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost.

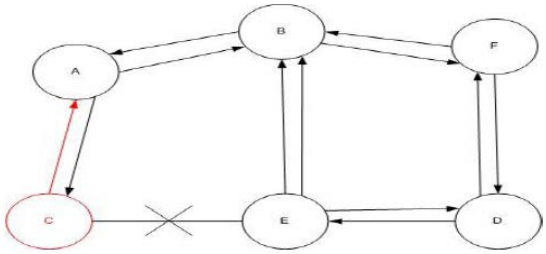

Fig. 7.1 Black Hole Problem

7.2 Jamming attack

Jamming is one sort of denial of service attacks in the wireless communication, which disrupts the operation of physical or link layers in legitimate nodes by transferring illegitimate signals. Jamming is one of such "availability attacks which can be easily carried out. It is defined as the intended transmission of radio signals that disrupt legitimate communication by decreasing signal to noise ratio. In this form of attack, the attacker initially keeps monitoring the wireless medium in order to determine the frequency at which the destination node is receiving signals from the sender. It then transmits signals on that frequency so that error-free reception at the receiver is hindered. Frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) are two commonly used techniques that overcome jamming attacks.

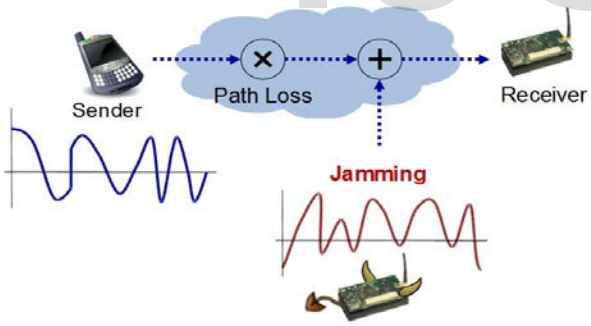

Fig. 7.2 Jamming Attacks

7.3 Wormhole attack

In wormhole attack, a malicious node, receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as wormhole. It could be established through wired link between two colluding attackers or through a single long-range wireless link. In this form of attack the attacker may create a wormhole even for packets not addressed to itself because of broadcast nature of the radio channel. For example in Fig. 7.3, X and Y are two malicious nodes that encapsulate data packets and falsified the route lengths Suppose node S wishes to form a route to D and initiates route discovery. When X receives a route request from S, X encapsulates the route request and tunnels it to Y through an existing data route, in this case {X --> A --> B --> C --> Y}. When Y receives the encapsulated route request for D then it will show that it had only traveled {S --> X --> Y --> D}. Neither X nor Y update the packet header. After route discovery, the destination finds two routes from S of unequal length: one is of 4 and another is of 3. If Y tunnels the route reply back to X, S would falsely consider the path to D via X is better than the path to D via A. Thus, tunneling can prevent honest intermediate nodes from correctly incrementing the metric used to measure path lengths. Though no harm is done if the wormhole is used properly for efficient relaying of packets, it puts the attacker in a powerful position compared to other nodes in the network, which the attacker could use in a manner that could compromise the security of the network.

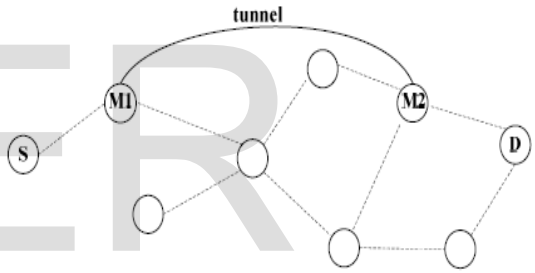

Fig 7.3 Wormhole attack

7.4 Denial of Service attack

A Denial-of-Service (DoS) attack[11] is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) the service or resource they expected. Victims of DoS attacks often target the web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle fig 6.4 shows denial of service attack. There are two general methods of DoS attacks: flooding services or crashing services. Flood attacks occur when the system receives too

much traffic for the server to buffer, causing them to slow down and eventually stop. Popular flood attacks include:

- Buffer overflow attacks – the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks
- ICMP flood – leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.
- SYN flood – sends a request to connect to a server, but never completes the handshake. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.

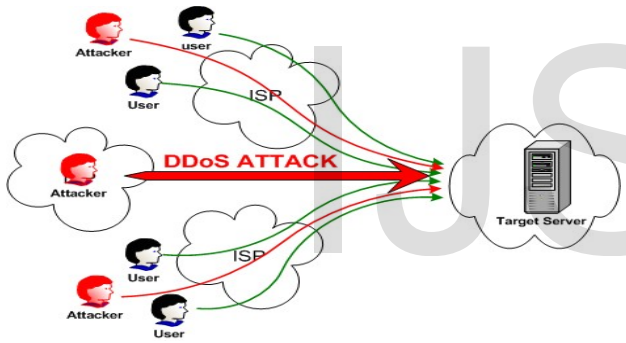

Fig 7.4: Denial of service attack

7.5 Flooding attack

Flooding attack is a denial of service type of attack in which the malicious node broadcast the excessive false packet in the network to consume the available resources so that valid or legitimated user can not able to use the network resources for valid communication. Because of the limited resource constraints in the mobile ad hoc networks resource consumption due to flooding attack reduces the throughput of the network. The flooding attack is possible in all most all the on demand routing, even in the secure on demand routing SRP, SAODV, ARAN, Ariadne etc. Depending upon the type of packet used to flood the network, flooding attack can be categorized in two categories.

- RREQ flooding
  In the RREQ flooding attack, the attacker broadcast the many RREQ packets per time interval to the IP address which does not exist in the network and disable the limited flooding feature.
- DATA flooding
  In the data flooding, malicious node flood the network by sending useless data packets. To launch the data flooding, first malicious node built a path to all the nodes then sends the large amount of bogus data packets. These useless data packet exhausts the network resources and hence legitimated user can not able to use the resources for valid communication

7.6 Byzantine attack

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

7.7 Routing Attacks

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

1) *Routing Table Overflow:* In this attack, the attacker attempts to create routes to nonexistent nodes. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. Proactive routing algorithms attempt to discover routing information even before it is needed, while a reactive algorithm creates a route only once it is needed. An attacker can simply send excessive route advertisements to the routers in a network. Reactive protocols, on the other hand, do not collect 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 parts of the network inaccessible.

3) Packet Replication: In this attack, an adversary node replicates stale packets. This consumes additional bandwidth and battery power resources available to the nodes and also causes unnecessary confusion in the routing process.

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

5) Rushing Attack: On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack. An adversary node which receives a Route Request packet from the source node floods the packet quickly throughout the network before other nodes which also receive the same Route Request packet can react. Nodes that receive the legitimate Route Request packets assume 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 extremely difficult to detect such attacks in ad hoc wireless networks.

7.8 IP Spoofing attack

In conflict-detection allocation, 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.

7.9 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[10]. 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.

7.10 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. 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.

7.11 SYN Flooding attack

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.

7.12 Repudiation attack

In the network layer, firewalls can be installed to keep packets in or keep packets out. 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

7.13 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. 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.

7.14 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.

7.15 Gray hole attack

A variation of black hole attack is the gray hole attack, in which the nodes will drop the packets selectively. Selective forward attack is of two types they are

- Dropping all UDP packets while forwarding TCP packets.

- Dropping 50% of the packets or dropping them with a probabilistic distribution. These are the attacks that seek to disrupt the network without being detected by the security measures

7.16 Link spoofing attack

In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations. For example in the OLSR protocol, an attacker can advertise a fake link with a target's two-hop neighbors. This causes the

target node to select the malicious node to be its MPR. As an MPR node, a malicious node can then manipulate data or routing traffic for example, modifying or dropping the routing traffic or performing other types of DoS attacks.

8. CONCLUSION

In this review paper, we try to inspect the security threats in the mobile adhoc networks, which may be a main disturbance to the operation of it. Due to nature of mobility and open media MANET are much more prone to all kind of security risks as covered. As a result, the security needs in the MANET are much higher than those in the traditional wired networks. At the time of review, we also find some points that can be further explored in the future, such as to find some effective security solutions and protect the MANET from all kinds of security risks.

REFERENCES

[1] Yi-an Huang and Wenke Lee, A Cooperative Intrusion Detection System for Ad Hoc Networks, in Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks, Fairfax, Virginia, 2003, pp. 135 –147.

[2] Mohammad Ilyas, "The Handbook of Ad Hoc Wireless Networks",

[3] Zubair Muhammad Fadlullah, Tarik Taleb, and Marcus Schöller, "Combating against Security Attacks against Mobile Ad Hoc Networks (MANETs)".

[4] Vikrant Gokhale, S.K.Gosh, and Arobinda Gupta, "Classification of Attacks on Wireless Mob Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks a Survey".

[5] Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks - A Survey".

[6] PRADIP M. JAWANDHIYA, MANGESH M. GHONGE "A Survey of Mobile Ad Hoc Network Attacks". International Journal of Engineering Science and Technology Vol. 2(9), 2010, 4063-4071

[7] K.P. Manikandan, Dr. R .Satyaprasad, Dr. Rajasekhararao. "Analysis and Diminution of Security Attacks on Mobile Ad hoc Network".IJCA Special Issue on "Mobile Ad-hoc Networks "MANETs, 2010

[8] G. S. Mamatha and Dr. S. C. Sharma "analyzing the manet variations, challenges, capacity and protocol issues" in proceedings of International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.1, August 2010.

[9] Ping Yi, Yue Wu and Futai Zou and Ning Liu, "A Survey on Security in Wireless Mesh Networks", Proceedings of IETE Technical Review, Vol. 27, Issue 1, Jan-Feb 2010.

[10] J.R.Douceur, "The Sybil Attack," in Proc. of 1st International Workshop on Peer-to-Peer Systems, Pages 251-260, March 2002, LNCS 2429.

[11] I. Aad and J.P. Hubaux, E.W. Knightly, "Denial of Service Resilience in Ad hoc Networks", Proceedings of ACM MobiCom 2004, Philadelphia, PA, Sep. 2004, pp. 202-215.