International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Review on Security Attacks in Mobile Ad-hoc Networks

Amandeep Kaur[1], Dr. Amardeep Singh[2]

[1] M. Tech student, Punjabi University Patiala, India

[2]Professor (CE), Punjabi University Patiala, India

Abstract: ***Security is a major concern for safe communication between mobile nodes in an alien environment. In alien environments, attackers can bunch active and passive attacks against imperceptible routing in routing message and data packets. In this, we focus on significant security attacks in Mobile ad hoc networks. MANET has no clear immunity so; it is available to both legitimate users and malicious attackers. In the existence of malicious nodes, one of the main objectives in MANET is to design the robust security solution that can protect MANET from various routing attacks. However, these solutions are not correct for MANET resource constraints, i.e., battery power and limited bandwidth. Mobile ad-hoc network can operate in isolation or in coordination with a wired infrastructure. This flexibility along with their self organizing facilities is some of MANET's biggest strengths, as well as their biggest security vulnerabilities. In this paper different routing attacks, such as active (black hole, spoofing, wormhole, flooding,) and passive (traffic monitoring, traffic analysis, eavesdropping) are described.***

Keywords: MANET, DOS, AODV, Data Traffic, Attacks, Security.

1. Introduction

A Mobile Ad-hoc Network is a [1] collection of independent mobile nodes that is formed without the support of any existing network framework. The MANET is a self configurable network, in which nodes connect or disconnect from the other nodes automatically at any point of time. The node to node connectivity etc. Routing of the data are done on the basis of the node discovery i.e. the node accept the data and forwards it to neighboring node in the path for the further transmission so that it can be reached to the particular destination. Each node works as a relay agent to route the data traffic. As MANET is dynamic in nature so it is accessible to all the users it may be a legitimate user or the malicious node which reproduce the data or attack in the network.

1.1 Characteristics of MANET

- No Centralized Administration – Each node in the MANET has its own communication capabilities for forwarding the data over [1] the network and adjusts the topology.
- Flexibility- MANET enables fast organization of the ad hoc network. When a node is joining the network, it should have the limited wireless communication range.
- Peer to peer connectivity of the nodes- In MANET, the nodes set communication link to which request response messages are flooded.
- Resource constraints- The node may have finite energy, so this may affect the functionality of the network.
- Dynamic Network topology-A node discovers the service of a nearby node using the service discovery protocol.
- Heterogeneous Nodes – In MANET architecture, any node can participate in forwarding the packets. The node may be Personal Computers, smart phones, smart tablets, embedded systems etc.

1.2 Applications

As Mobile ad hoc network has dynamic network and fewer infrastructures so it is gaining popularity. Ad hoc networks can be established [1] anywhere where the nodes have connectivity with other nodes and can join and leave the network at any time. The applications are as followed:

- Military: The communication among the soldiers, headquarters of military and vehicles can be possible as this area do not have the proper establishment of the base station for the communication.
- Emergency Services: Ad hoc can be used in emergency operations such as search and rescue, recovery from disasters for e.g. Fire, flood, volcano earthquake, eruption etc.
- Commercial environments: Ad hoc networks can autonomously link an instant in business so as to share the daily updates of office.

2. Security Issues and Challenges

Because of dynamic topological, ad hoc networks are more vulnerable at the physical link. An attacker can easily attack ad hoc networks by loading available network resources, such as [2] wireless links and energy (battery) levels of other users, and disturb all users. The following challenges show the inefficiencies and limitations that have to be overcome in a MANET environment:

2.1. Limited computational capabilities

Typically, nodes are modular, independent and limited in computational capability in MANET and therefore may become a source of vulnerability.

2.2. Limited wireless transmission range

In wireless networks the radio band will be limited and hence data rates it can offer are much lesser than wired

network. This requires the routing protocols in ad-hoc networks to use the bandwidth always in an optimal manner by keeping the overhead as low as possible.

2.3. Device Compatibility

MANETs are mostly composed of devices with varying energy profiles, different hardware configurations or running different versions of software. Thus, the first challenge in MANET is to establishing communication between these heterogeneous components.

2.4. Battery constraints

This is one of the limited resources that form a major constraint for the nodes in MANET. Devices used in wireless networks have restrictions on the power source to maintain size, weight and portability of the device.

2.5. Challenging key management

Dynamic topology and movement of mobile nodes in an ad hoc network make key management difficult if cryptography is used in the routing protocol.

2.6. Packet losses due to transmission errors

Ad hoc networks experiences a much higher packet loss due to factors such as high bit error rate (BER) in the wireless channel, increased collisions due to the presence of hidden terminals, presence of interference, location dependent contention, unidirectional links, frequent path breaks due to mobility of nodes, and the inherent fading properties of the wireless channel .

2.7. Bandwidth usage

Bandwidth availability affects connectivity. In ad-hoc wireless networks, bandwidth is used for connectivity establishment, maintenance and for data exchange. If all available bandwidth is used up by data communication and other connection establishment activities then newer connections may not be established or existing connections may not be re-established when mobile nodes relocate themselves.

3. Security Attributes for MANET Networks

There are several important requirements to achieve security in MANETs, which are discussed as follows.

3.1. Authentication

Nodes should respond only to the messages transmitted by legitimate [3] members of the network. Thus, it is very important to authenticate the sender of a message.

3.2. Data Verification

Once the sender is authenticated the receiving node performs data verifications to check whether the message contains the correct or corrupted data.

3.3. Availability

The network should be accessible even if it is under an attack using alternative mechanisms without affecting its performance.

3.4. Data Integrity

It ensures that data or messages are not altered by attackers. Otherwise, users are directly affected by the altered emergency data.

3.5. Non-repudiation

A sender must not deny a message transmission whenever an investigation or identity of a node is required.

3.6. Privacy

The personal information must be maintained against unauthorized access.

3.7. Real-time constraints

Since nodes are connected to MANETs for a short duration, real-time constraints should be maintained.

4. Types of Security Attacks

Mobile Ad hoc networks are vulnerable to various attacks not only from outside but also from inside i.e. network itself. Ad hoc network are mainly subjected to two different levels of [4] attacks. The first level of attack occurs on the basic mechanisms of the ad hoc network such as routing. Whereas the second level tries to damage the security mechanisms employed in the network.

4.1. Internal Attacks

Internal attacks are directly leads to the attacks on nodes presents in network and links interface between them. These attacks may broadcast wrong routing information to other nodes. Internal attacks are sometimes more difficult to handle as compare to external attacks, because internal attacks occurs due more reliable nodes. The inaccurate routing information generated by malicious nodes is difficult to identify.

4.2. External attacks

These types of attacks try to cause congestion in the network, denial of services (DoS), and advertising wrong routing information etc [2]. External attacks prevent the network from normal communication and producing additional overhead. External attacks can divided into two categories:

4. 2.1 Passive attacks

MANETs are more susceptible to passive attacks. The passive attack does not alter the data transmitted within the network. But it includes the unauthorized “listening” to the network traffic. Passive attacker does not alter the operation of a routing protocol, but attempts to discover the important information from traffic. Detection of passive attacks is

difficult since the operation of network itself doesn't get affected. In order to overcome these attacks, powerful encryption algorithms are used to encrypt the data being transmitted.

4.2.2 Active Attacks

Active attacks are very severe attacks on the network that prevent message flow between the nodes. Active attacks can be internal or external. Active external attacks can be executed by outside sources that do not belong to the network. Active Internal attacks are malicious nodes which are part of the network. Internal attacks are more rigid and hard to detect than external attacks. These attacks generate illegal access to network that helps the attacker to make changes such as packets modification, DOS and congestion etc.

Table 1: Security attacks with their attacker types and security attributes.

Name of Attack	*Attackers Type*	*Security Attributes*
Bogus Information	Insider	Data Integrity, Authentication
Denial of Service(DOS)	Malicious, Active, Insider	Availability
Masquerading	Active, Insider	Authentication
Black Hole	Passive, Outside	Availability
Malware	Malicious, Insider	Availability
Spamming	Malicious, Insider	Availability
Timing Attack	Malicious, Insider	Data Integrity
GPS Spoofing	Outside	Authentication
Man-in-the-Middle	Insider, Monitoring Attack	Data Integrity, Confidentiality
Sybil	Insider	Authentication
Wormhole	Outside, Malicious, Monitoring Attack	Confidentiality, Authentication
Illusion Attack	Malicious, Insider	Authentication
Purposeful attack	Active, Insider, Malfunctioning hardware	Authentication
Impersonation	Insider	Authentication

5. Types of Active Attacks on Various Layers

The characteristics of MANETs make them susceptible to new attacks. These attacks can occur in different layers of the network.

5.1. Attacks at Physical Layer

The attacks on physical layer are hardware oriented and they need help from hardware sources to come into effect. These attacks are simple to execute. They do not have complete knowledge of technology. Some of the attacks given below:

5.1.1. Eavesdropping

Eavesdropping can also be defined as interception and reading of messages and conversations by unintended receivers. As the communication takes place on wireless medium can easily be intercepted with receiver tuned to the proper frequency. The main aim is to obtain the confidential information that should be kept secret during the communication. The information may include private key, public key, location or passwords of node. Data can be eavesdropped by tapping communication lines.

5.1.2. Jamming

Jamming is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication. In this, the jammer transmits signals along with security threats. Jamming attacks prevents the reception of legitimate packets.

5.1.3. Active Interference

An active interference is a denial of service attack which blocks the wireless communication channel, or distorting communications. The effects of such attacks depend on their duration, and the routing protocol in use. Attacker can change the order of messages or attempt to replay old messages. Old messages may be replayed to reintroduce out of date information.

5.2. Attacks at Data link / MAC layer

The algorithms used in data link layer/MAC layer are susceptible to many DoS attacks. MAC layer attacks can be classified as to what effect it has on the state of the network as a whole [4]. The effects can be measured in terms of route discovery failure, energy consumption, link breakage initiating route discovery and so on. The misbehavior of a node can be purely in selfish interest or with malicious intents.

5.2.1. Selfish Misbehavior of Nodes

Attacks under this category, are directly affects the self-performance of nodes and does not interfere with the operation of network. It may include two factors: Conservation of battery power and Gaining unfair share of bandwidth.

The selfish nodes may refuse to take part in the forwarding process or drops the packets intentionally. These attacks exploit the routing protocol to their own advantage. Packet dropping is one of the main attacks by selfish node which leads to congestion in network. However most of routing protocols have no mechanism to detect whether the packets being forwarded or not except DSR (dynamic source routing).

5.2.2. Malicious Behavior of nodes

The main aim of malicious node is to disrupt normal operation of routing protocol. The impact of the attack is increased, when the communication takes place between nodes. Attacks of such type are fall into following categories: Denial of Service (DOS), Attacks on Network integrity, Misdirecting traffic.

5.2.3. Traffic Analysis

In MANETs the data packets as well as traffic pattern both are important for attackers. For example, confidential data about network topology can be derived by analyzing network traffic patterns. Network traffic analysis can also be conducted as active attack by destroying nodes, which prompt self organization in the network, and data about the topology can be gathered. Traffic analysis in MANET may reveal following type of information.

- Location of nodes.
- Network topology used.
- Roles played by nodes.
- Available source a destination nodes.

5.3. Attacks at Network Layer

The network layer protocols enable the MANET nodes to be connected with another through hop-by-hop. In MANETs every individual node takes route decision to forward packet, so it is very easy for malicious node to attack on such network. The basic idea behind network layer attacks is to inject itself in the active path from source to destination or to absorb network traffic. In such attacks, the attackers can create routing loops to form severe congestion. Different type of attacks are identified which are initiated by malicious node.

5.3.1. Black hole Attack

In this type of attacks, malicious node claims having an optimum route to the node whose packets it wants to intercept. On receiving the request the malicious node sends a fake reply with extremely short route. Once the node has been able to place itself between the nodes, it is able to do anything with the packets passing between them.

5.3.2. Rushing Attack

Rushing attacks are mainly against the on-demand routing protocols. These types of attacks subvert the route discovery. On-demand routing protocols i.e. DSDV etc. that use duplicate suppression during the route discovery process is vulnerable to this attack. When compromised node accepts a route request packet from the source node, it floods the packet throughout the network before other nodes which also receive the same route request packet can react.

5.3.3. Wormhole Attack

In wormhole attack, malicious node receive data packet at one point in the network and tunnels them to another malicious node. The tunnel exist between two attacker nodes is referred to as a wormhole. Wormhole attacks are rigid threat to MANET routing protocols. When the wormhole attacks are used by attacker in routing protocol such as DSR and AODV, the attack prevent the discovery of any routes other than through the wormhole. If there is no defense mechanism are introduced in the network along with routing protocols, than existing routing protocols are not suitable to discover valid routes.

5.3.4. Sinkhole Attack

Sinkhole attack is one of the severe attacks in wireless Ad hoc network. In sinkhole, malicious node advertises wrong routing information to produce itself as a specific node and receives whole network traffic. After receiving network traffic, it modifies the secret information. An attacker node tries to attract the secure data from neighboring nodes. Sinkhole attack affects the performance of Ad hoc networks protocols such as AODV by using flaws as maximizing the sequence number and minimizing the hop count. By this the path presented through the malicious node appears to be the best available route for the nodes to communicate. In DSR protocol, sinkhole attack modifies sequence no in RREQ.

5.3.5. Replay Attacks

In MANETs, the topology is not fixed; it changes frequently due to mobility of nodes. In replay attack, a malicious node record control messages of other nodes and resends them. By this other nodes have to record their routing table with stale routes. These replay attacks are misused to disturb the routing operation in a MANETs.

5.3.6. Link Spoofing Attacks

In Link spoofing attacks, a malicious node broadcasts or advertises the fake route information to disrupt the routing operation. It results in, malicious node manipulate the data or routing traffic.

5.3.7. Sybil Attack

In Sybil attack, Sybil attacker may generate fake identities of number of additional nodes. In this, a malicious node produces itself as a large number of instead of single node. The additional identities that the node acquires are called Sybil nodes. A Sybil node may create a new identity for itself or it steals an identity of the legitimate node.

5.4. Attacks at Transport Layer

5.4.1. Session Hijacking

Attacker in session hijacking takes the advantage to exploits the unprotected session after its initial step. In this, the attacker spoofs the victim node's IP, finds the correct sequence number and then launches various DOS attacks. In Session hijacking, the attacker node tries to collect secure data (passwords, secret keys, logon names etc) and other information.

5.4.2. SYN Flooding Attack

The SYN flooding attacks are the type of Denial of Service (DOS) attacks, in which attacker creates a large number of half opened TCP connection with node. These connection are never completes the handshake to fully open the connection.

5.5. Attacks at Application Layer

Application layer protocols are also vulnerable to many DOS attacks. This layer contains user data. It supports protocols such as HTTP, SMTP, TELNET and FTP, which provides many vulnerabilities and access points for attackers.

5.5.1. Malicious code attacks

Malicious code attacks include Worms, Viruses, Spywares, and Trojan horses can attack both operating system and user application.

5.5. 2. Repudiation attacks

Repudiation refers to a denial of participation in all or part of the communications. Many of encryption schemes and firewalls used at different layer are not sufficient for security. Application layer firewalls may take into account in order to provide security to packets against attacks. For example, spyware detection software has been developed in order to monitor mission critical services.

Table 2: Attacks on different layers.

Layers	*Attacks*
Physical Layer	Eavesdropping, Jamming, Active Interferences
Data Link Layer	Selfish misbehavior, Malicious behavior, Traffic analysis
Network Layer	Black hole, Wormhole, Sinkhole, Link spoofing, Rushing, Replay Attack, Sybil Attack
Transport Layer	Session hijacking, SYN flooding Attack
Application Layer	Malicious code, Data corruption, Viruses and Worms

6. Conclusion and Future Work

Due to dynamic infrastructure of MANETs and having no centralized administration makes such network more vulnerable to many attacks. In this paper, we discuss about security challenges and how different layers protocols become vulnerable to various attacks. These attacks can classified as an active or passive attacks. Different security technologies are introduced to prevent such network. In future study we will try to invent such security algorithm, which will be work along with the routing protocols that helps to reduce the impact of different attacks.

References

[1] Swati Jain, Naveen Hemrajani, "Detection and Mitigation Techniques of Black Hole Attack in MANET: An Overview", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, Volume 2 Issue 5, May 2013.
[2] Sapna, Gambhir, Saurabh Sharma," PPN: Prime Product Number based Malicious Node Detection Scheme for MANETs", 2013, 3rd IEEE International Advance Computing Conference (IACC).
[3] Mohammed Saeed Al-kahtani, "Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs)," IEEE 2012.
[4] Gagandeep, Aashima, Pawan Kumar," Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.
[5] Priyanka Goyal, Sahil Batra, Ajit Singh "A Literature Review of Security Attack in Mobile Ad-hoc Networks", International Journal of Computer Applications (0975 – 8887) Volume 9– No.12, November 2010.
[6] A. Chirag Tehlanl and Divya Sharma "A Study on Different Security Threats in Mobile Ad-hoc Network" International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 4, Number 1 (2014), pp. 1-10