ISSN:0975-9646

A Survey on Security Attacks in Mobile Ad Hoc Networks

Saritha Reddy Venna[1], Ramesh Babu Inampudi[2]

[1]*Assistant Professor, Dept. of CSE, Acharya Nagarjuna University, A.P., India*

[2]*Professor, Dept. of CSE, Acharya Nagarjuna University, A.P., India*

***Abstract*— The recent and rapid advancements in the technology and the distinct features of MANETs have made the use of MANETs more prevalent. With the ever increasing applications, the weakness of these networks against a variety of attacks has been unveiled. MANETs doesn't have clear and efficient mechanisms to detect or prevent the attacks, so attacker node can easily interrupt and destroy the whole system or may take control over the information being transmitted in the network. Attackers introduce various kinds of attacks and every attack has its own degree of impact on the network. Security is a major concern in MANETs because of its intrinsic vulnerabilities. This survey paper focuses on vulnerabilities and various kinds of security attacks in MANETs.**

***Keywords*— MANET, Vulnerabilities , Security Attacks**

I. INTRODUCTION

A Mobile Adhoc Network (MANET) is a "short-lived" wireless network which consists of mobile nodes interconnected with wireless network interfaces [1]. Each mobile node can work either as a host or as a router. There is no necessity of fixed infrastructure and these mobile nodes organize themselves in an arbitrary fashion to form a temporary network with dynamically changing topology. Nodes within each other's wireless transmission ranges can communicate directly but nodes outside each other's range have to depend on neighbouring nodes to relay messages [5]. Thus a multi-hop communication occurs, where several intermediate nodes relay the packets sent by the source node till they reach the destination node. The communication is peer-to-peer, allowing people and devices to seamlessly internetwork in areas with no pre-existing communication infrastructure, e.g., disaster recovery environments, emergency search and rescue operations where a network connection is urgently required. In addition to node mobility, a MANET is characterized by limited resources such as bandwidth, battery power, and storage space. In order to communicate, the nodes dynamically establish paths among themselves. This dynamic nature of MANETs and open medium of communication makes them highly vulnerable to a variety of security attacks. The objective of this paper is to discuss about the vulnerabilities and various attacks in MANETs in accordance with the protocol stack.

II. MANET VULNERABILITIES

Vulnerability is a weakness that is inherent in a security system or a network device such as router, switch, desktop, server or security device itself [2]. Any system connected to the network may be vulnerable to unauthorized data manipulation as it doesn't verify the user's identity to access the data. As MANET is a wireless adhoc network it is much more prone to attacks compared to a wired network. Some of the vulnerabilities are discussed below.

A. Lack of Centralized Management

MANET doesn't possess any centralized authority to monitor the network functioning. This makes attack detection difficult since it is not easy to monitor the network traffic in such a highly dynamic and frequently changing topology.

B. Dynamic Topology

In MANETs, the topology keeps changing dynamically depending on the mobility of nodes. This feature makes the nodes in MANET susceptible to a wide variety of attacks.

C. Resource Availability

Resource availability is an addressable issue in MANET. Since the mobile nodes that comprise of a MANET are portable devices, they possess limited memory capacity. So before sending a replica to the node, the algorithm has to check whether it has sufficient memory to hold the replica.

D. Wireless Links

As the nodes in MANETs are interconnected through wireless interfaces they are highly prone to link attacks. The bandwidths of wireless networks are less as compared to wired networks, which attracts many attackers to prevent normal communication among nodes.

E. Lack of clear line of defence

Since MANETs do not have a clear line of defense attacks can originate from any direction. The nature of attack can be internal or external, active or passive etc.

F. Battery constraints

The mobile devices used in MANETs such as laptops, mobile phones, tablets etc have more limitations on the power source in order to attain features such as portability, size and weight of the device.

G. Scalability

Due to continuous mobility of nodes, the size of ad-hoc network changes all the time. So, scalability becomes an important factor to consider with regard to security. Security mechanisms developed should be able to secure a huge network as well as a small one.

H. Bandwidth constraint

The wireless links are of low capacity when compared to a wired network and are easily prone to external noise, signal interference and attenuation.

I. Cooperativeness

Routing algorithms for MANET usually assumes that all mobile nodes that participate in communication are cooperative and non-malicious. But some nodes can easily turn into malicious nodes and disturb the normal communication of the network by transmitting wrong routing information.

III. MANET SECURITY ATTACKS

In the design of adhoc protocol specifications security aspects were not taken into consideration. These protocols were developed with an assumption that all the mobile nodes in the network are not malicious and cooperate among themselves for smooth functioning of the MANET. This assumption is not true in a real-time environment where malicious nodes can disrupt the network functioning by violating the protocol specifications. Due to insecure protocols and many vulnerabilities such as limited bandwidth, dynamically changing topology, wireless links, no predefined boundaries and limited battery power, Manets are prone to a variety of attacks.

A. Classification based on Location

Security attacks can be mainly categorized into Internal and External on the basis of Location.

1) *Internal Attack:* Internal attack originates from a node or nodes that exist within the network. The malicious nodes inside the network can broadcast wrong routing information to its neighbouring nodes effecting the normal functioning of the network. Internal attacks are hard to detect as the compromised nodes are capable of generating valid digital signatures using their private keys.

2) *External Attack:* External attack originates from a node or nodes that don't belong to the network. They can cause network congestion, unavailability of network services and also produces additional network overhead thereby preventing the network from information exchange.

B .Classification based on the Nature of Attack

Attacks can be further classified into active and passive based on the nature of attack.

1) Passive Attack: In passive attack, the attacker does not corrupt the information exchanged but listens to it. They try to gain confidential information and analyze the traffic patterns transmitted. They are hard to detect as they do not interrupt or modify the data being sent or received.

2) Active Attack: In Active attack, the attacker actively participates in the network activities and attempts to modify the messages being transmitted. The attacker can modify, inject, forge, fabricate or drop data by disturbing the whole network operation. The severity of this attack is high as they can bring down the entire network. They are easy to detect as the network performance degrades significantly.

C. Attack classification based on different layers of protocol stack as shown in Table1.

Table1. Attacks on MANET Protocol Stack

Layer	Attacks
Physical layer	Eavesdropping, Jamming, Active Interference
Data link layer	Selfish misbehaviour of nodes, Malicious behaviour of nodes, Traffic Analysis
Transport layer	SYN flooding, Session hijacking
Network layer	Wormhole, Sybil, Blackhole, Grayhole, Jellyfish, Byzantine, Link Withholding, Link Spoofing, Location Disclosure, Partitioning Attack, Rushing Attack, Replay Attack
Application layer	Malicious Code, Repudiation
Multilayer Attacks	Denial of Service, Impersonation

1) Physical layer Attacks: These attacks are hardware based and require assistance from hardware sources to occur. The execution of these attacks is simple as we do not require in-depth knowledge about the technology being used.

(a) Eavesdropping

It is defined as interception and reading of messages and conversations by unintended receivers [4]. As the medium is wireless anyone within the radio range and receiver tuned to the proper frequency can listen to the ongoing communication. The main goal of this attack is to gain access to the confidential information transmitted such as private key, public key or node passwords.

(b) Jamming

Jamming is a special class of DoS attacks which are caused by a compromised node after learning the frequency of communication. The jammer transmits signals with security threats and also prevents receiving the legitimate packets.

(c) Active Interference

An Active Interference is a Denial of Service attack which blocks the wireless communication channel. The effect of this attack depends on the routing protocol used and the duration of it [3, 4]. The intruder can reorder the messages or replay the old messages.

2) Data Link / MAC Layer Attacks: MANET is an open multipoint peer-to-peer network architecture. Specifically, single-hop connectivity among neighbours is maintained by the link layer protocols [8]. The protocols used in 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. The effects can be measured in terms of route discovery failure, energy consumption, link breakage, initiating route discovery and so on. The misbehaviour of a node can be either selfish or of malicious nature.

(a) Selfish misbehaviour of nodes

These are selfish nodes that either deny forwarding the packets or drop the packets intentionally in order to conserve battery power or gains unwanted share of bandwidth. Packet dropping is one of the major attacks by selfish node which causes congestion in network. These attacks exploit the routing protocol to their own advantage because most of the routing protocols have no mechanism to detect whether the packets are being forwarded or not except the Dynamic Source Routing protocol.

(b) Malicious behaviour of nodes

They disrupt operation of routing protocol and its effect will be considerable only when more communication takes place between neighbouring nodes [7].

(c) Traffic Analysis

In this type of attack the adversaries analyze the traffic patterns to gain important information on network topology that in turn reveals the information about the nodes. Information such as location of nodes, network topology used to communicate and roles played by the nodes can be gathered.

3) Network Layer Attacks: The network layer protocols for MANETs were designed to connect the mobile nodes with one another and for routing packets from a source to a destination. The connectivity among nodes in the network layer extends from single hop neighbour nodes to multihop mobile nodes. In order to launch a routing attack, the attacker places itself in the active path between the source and destination. The malicious node then gains access to the packets being routed, drops the packets and even generates routing loops that give rise to network congestion. Attacks on routing protocols can damage the operation of the entire network. Network layer attacks are discussed below.

(a) Wormhole Attack

It becomes a major challenge to defend against wormhole attack since it is one of the most severe and well planned attacks [11]. To launch this attack, two or more compromised nodes collaborate among themselves and establish a tunnel using a high-speed wireless connection [6]. Hence it is also known as tunnelling attack. In Fig. 2, W_1 and W_2 are two malicious nodes which created a tunnel. The source node S sends RREQ packets to its neighbouring nodes to find the route to destination node D. The first malicious node W_1 receives RREQ from source S and sends it via high speed link to second attacker W_2 which forwards it to destination earlier than any other node. Hence RREQs which arrive later are discarded and these malicious nodes are included in the path from S to D. Once W_1 and W_2 are included in the routing path, these malicious nodes can either drop all the packets or drop the packets selectively to avoid attack detection.

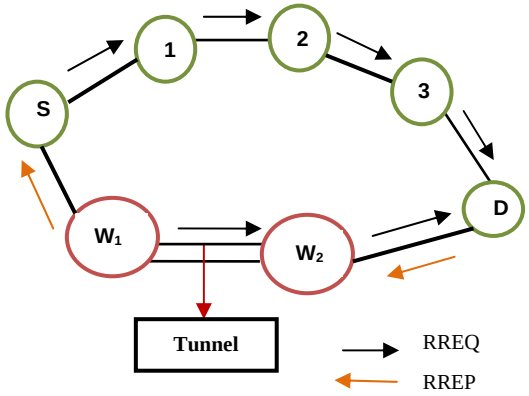

Fig.2 Wormhole Attack

(b) Sybil Attack

In MANET the routing mechanism is predominantly based on the unique node identity that forms the one-to-one mapping between the node and its identity i.e., two identities implies two distinct nodes. But the malicious node illicitly generates multiple identities of a single node by violating this one-to-one mapping of node and identity philosophy. Such malicious nodes with multiple identities are termed as Sybil nodes. To launch the Sybil attack, the Sybil node can either use multiple identities at a time to create a lot of misjudgements among the nodes or use the identity of other legitimate node to create a false impression of that node. This type of attack is called Sybil attack. This attack causes lot of packets to be routed towards the fake identity nodes which eventually disturbs the normal communication among the nodes. The presence of these Sybil nodes makes it difficult to find misbehaving node as well as prevents fair resource allocation among the nodes in the network [7].

(c) Link Withholding Attack

In this attack, the malicious node does not broadcast information about the links to specific nodes or a group of nodes in the network. This results in losing the links to these nodes.

(d) Blackhole Attack

This attack predominantly affects the route discovery mechanism of reactive routing protocols. The attacker pretends to be a new node and bearing shortest path to the destination by sending fake RREPs to the RREQs sent by the source or victim node(S). It asserts the newness by replying with the highest sequence number and minimum hop count. The path between the victim(S) and the attacker (i.e., node 5) is established and then the victim node starts sending packets to attacker node. The attacker drops all the packets received and hence it is known as a blackhole node.

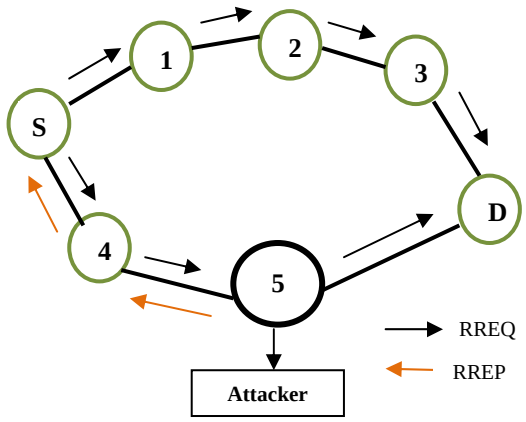

Fig.3 Blackhole Attack

(e) Grayhole Attack

Grayhole attack is similar to Blackhole attack with a minor difference. The attacker sends fake RREP to source (or victim) node as in Blackhole attack but it doesn't drop all the data packets. It drops few packets selectively and forwards the rest of them. This attack is relatively difficult to detect as it drops some selective packets and forwards the rest. This situation can be mistaken for network congestion or some other valid reason.

(f) Jellyfish Attack

This is a selective black hole attack in which malicious node disrupts the network operation by modifying the order of packets, dropping selective packets or increasing jitter of the packets that pass through it. This prevents the attack from being detected and misleads the nodes in the network that packet loss or transmission delay is because of some environmental issues [9].

(g) Byzantine Attack

A single malicious intermediate node or a set of compromised intermediate nodes carries out attacks by creating routing loops, forwarding packets through non optimal paths, or selectively drops packets, resulting in disruption or degradation of the entire routing mechanism [10].

(h) Link Spoofing Attack

In a link spoofing attack, a compromised node signalizes an incorrect set of neighbours or advertises fake links with non-neighbour nodes in order to distort the normal routing process. This attack mainly affects the OLSR protocol. A misbehaving node X may perform link spoofing in its HELLO messages advertising a link with non-neighbour node A, as in Fig.4. This will result in C and the others neighbours of X, storing an incorrect 2-hop neighbourhood and therefore selecting a wrong MPR (Multi Point Relay) set. In fact, node C will probably select {X, D} as its MPR set, instead of the correct MPR set {X, B, D}, because the first set is smaller. As a consequence, messages originating from E and relayed through the MPR mechanism will not reach node A.

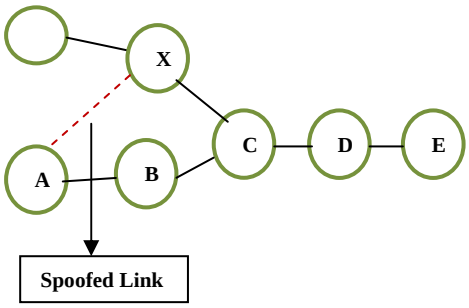

Fig.4 Link Spoofing Attack

(i) Location Disclosure Attack

In this attack, an attacker node leaks out information regarding the network topology, geographic location of nodes, or optimal routes to authorized nodes. This leaked information is then used by other nodes to launch further attacks and also turns out to be a major threat in security-sensitive scenarios.

(j) Partitioning Attack

A malicious node can try to partition the network by injecting forged routing packets to prevent one set of nodes from reaching another [13].

(k) Rushing Attack

Rushing attack mainly affects the on-demand routing protocols that use duplicate elimination during the route discovery phase. The malicious node after receiving a route request (RREQ) packet from the source node floods the entire network rapidly with these packets before other nodes receiving the same RREQ packet can react. Since the malicious node rushes packets it is known as Rushing Attack. Nodes receiving the legitimate RREQ packets at a later point in time treat them as duplicates and discard them. The source node will not be able to find any route without the attacker node thus forcing the entire network traffic to flow through it. Hence every route established comprises of the malicious node as one of its intermediate nodes [9].

(l) Replay Attack

The topology of MANET keeps changing dynamically because of the frequent node mobility. Due to this property of mobile nodes, the valid routes in the past could have become invalid at present. In replay attack, the attacker records some valid control messages sent in the past and resends these control messages at a later point in time. The remaining nodes in the network adds invalid routes in their routing tables based on these control messages which eventually disturbs the entire routing process.

4) Transport Layer Attacks: The objectives transport layer protocols in MANET include setting up of end-to-end connection, reliable end-to-end message delivery with acknowledgements, message traffic control i.e., flow control, congestion control, and clearing of end-to-end connection. Similar to TCP protocols in the Internet, the

mobile node is vulnerable to the classic Synchronization (SYN) flooding attack or session hijacking attacks.

(a) SYN Flooding Attack

The SYN flooding attack is a type of denial-of-service (DoS) attack that generates a large number of half-opened TCP connections with a victim node, but never completes the handshake to fully open the connection. For two nodes to communicate using TCP, they must first establish a TCP connection using a three-way handshake. The three messages

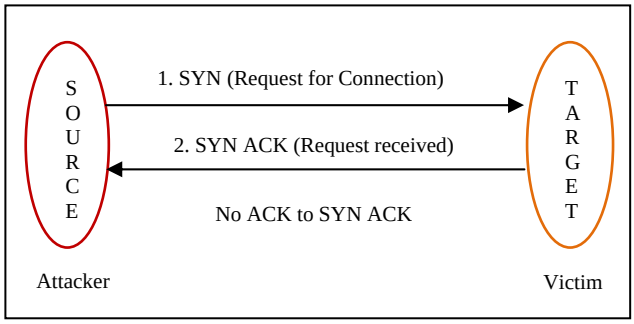

Fig.5. Handshake Process with TARGET where the SOURCE is an attacker that doesn't complete 3-way handshake.

exchanged during the handshake allow both nodes to learn that the other is ready to communicate and to agree on initial sequence numbers for the conversation. In this attack, the attacker node sends continuous stream of SYN packets to target. The target allocates memory on its connection queue to keep track of half-opened TCP connections and replies with a SYN-ACK. The attacker does not complete 3-way handshake by sending ACK to SYN-ACK to fully open the connection thus filling up all slots on connection queue of target node [7].

(b) Session Hijacking

The authentication of a node is done only once at the start of a session. An adversary takes advantage of this weakness and can easily hijack the session by retrieving information of an authentic user such as Session ID from the user's session state. The attacker spoofs the victim node's IP address, finds the correct sequence number and continues the session with the target by generating a DoS attack on the victim node.

5) Application Layer Attacks: The application layer comprises of user data. It supports many protocols such as HTTP, SMTP, TELNET, and FTP, which bring forth many vulnerabilities and access points for attackers [10].

(a) Malicious Code Attacks

Malicious code attacks include Viruses, Worms, Spywares, and Trojan horses that can replicate themselves and damage operating system or the entire network.

(b) Repudiation Attacks

Repudiation refers to a denial of participation in all or part of the communication by an adversary node. For example a selfish node can deny the processing of an online bank transaction. Firewalls at the network layer to check incoming and outgoing packets and end-to-end encryption mechanisms used at transport layer are not sufficient for packet security.

6) Multilayer Attacks

(a) Denial of Service (DoS) Attack

A denial-of-service attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. This attack can be launched at different layers. At the physical layer, by signal jamming attack normal communication is disturbed. At the link layer, malicious nodes take hold of the channel and prevent other nodes from channel access. At the network layer, DoS attacks are launched on routing protocols to degrade the network performance by flooding different kinds of routing packets. At the transport layer by SYN flooding and session hijacking and at the application layer by malicious programs and repudiation.

(b) Impersonation Attacks

Impersonation attacks use fake or legitimate node's identity, such as MAC or IP address to launch the attack. Each wireless node in MANET should possess a unique address but this identity check is not possible as there is no central authority. An attacker node can take advantage of this weakness and send control packets with differing identities which eventually disturbs the entire routing process popularly known as Sybil attack [6].

IV CONCLUSION

MANETs can be used in various situations ranging from emergency operations and disaster relief to military service and task forces. Providing security in such scenarios is critical. This paper gives a brief analysis of vulnerabilities and different types of attacks in MANET in accordance with the protocol stack. The reliability on MANETs is mainly constrained by its security. The survey presented in this paper will be a helpful instrument in studying MANET attacks layer wise and then developing protocols for secure communication.

REFERENCES

[1] Mohammad Ilyas, "The Handbook of Ad Hoc Wireless Networks".
[2] 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.
[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 Mobile AdHoc Networks and Vehicular Ad Hoc Networks a Survey".

[5] C. Perkins, Ad Hoc Networks, Addison-Wesley, 2001.
[6] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato, "A Survey of Routing Attacks in Mobile Ad Hoc Networks," IEEE Wireless Communications, vol. 14, issue 5, pp. 85-91, October 2007.
[7] Gangandeep, 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.
[8] 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.) pp107-139, @ 2006 Springer.
[9] Tarunpreet Bhatia and A.K.Verma, "Security Issues in Manet: A Survey on Attacks and Defense Mechanisms" IJARCSSE, vol. 3, june 2013.
[10] Vikrant Gokhale, S.K. Ghosh, and Arobinda Gupta, "Classification of Attacks on Wireless Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks: A Survey),"Security of self-organizing networks: MANET, WSN, WMN, VANET, AS. K.Pathan pp195-225, CRC Press, Taylor & Francis Group 2011.
[11] Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks," IEEE JSAC, vol. 24, no. 2, Feb. 2006.
[12] J. Sen, "Security and Privacy Issues in Wireless Mesh Networks: A Survey", Wireless Networks and Security, Khan, S. (eds.), pp. 189-272, Springer-Verlag, Berlin, Heidelberg, February 2013.
[13] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani, "A Survey of Secure Mobile Ad Hoc Routing Protocols", IEEE Communications Surveys & Tutorials, Vol. 10, No. 4, Fourth Quarter 2008.