International Journal of Research in Advent Technology, Vol.2, No.5, May 2014

E-ISSN: 2321-9637

Attacks on Mobile Adhoc Networks: A Survey

Er. Nitin Aggarwal[1], Ms. Kanta Dhankhar[2]
[1] *ECE Department, ISTK, Kurukshetra University Kurukshetra, Haryana, INDIA*
[2]*CSE Department, ISTK, Kurukshetra University Kurukshetra, Haryana, INDIA*
Email: nitininworld@gmail.com[1] *, kanta.dhankhar@gmail.com*[2]

Abstract-Due to recent developments in technology and uniquely distinct characteristics of MANETs, the applicability of MANETs have become pervasive. As the applications are increasing, the vulnerability of these networks against various attacks has been exposed. MANETs have not clearly and explicitly stated defense mechanisms, so attacker node can easily disrupt the whole system or may take control over the information in the network. Different types of attacks have been introduced by attackers and every attack has its distinct impact on the network. Security is a paramount concern in mobile ad hoc network (MANET) because of its intrinsic vulnerabilities .In this paper state-of-the-art security issues in MANETs are investigated. In particular t a survey on different types of attacks and their different classifications is presented.

Index Terms- MANETs; Attacks; Security

1. INTRODUCTION

Mobile Adhoc Networks are networks formed by nodes which are mobile in nature and connected through wireless links through which they can share information with each other. The most unique features of MANETs are that the whole network works without any centralized administration and every node works as a router. 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 [5]. Thus, a multi-hop communication occurs, where several intermediate nodes relay the packets sent by the source node before 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.

Security is a crucial service for wireless and wired network communications. The applicability of MANET strongly depends on whether its security can be relied or not. However, the characteristics of MANET pose both challenges and opportunities in achieving the security goals. There are many security issues which have been studied in recent years. In [3], authors present a survey on attacks and countermeasures in mobile ad hoc networks. In [4], a survey of routing attacks in mobile ad hoc networks has been presented. In [1], various attacks on network layer have been discussed.

In the following, different kinds of routing protocols are introduced in Sec. 2, which includes proactive routing, reactive routing and hybrid routing protocols. Sec.3 provides an overview of security issues. In Sec.4, different types of attacks classified on different basis are discussed in detail. Finally, this survey is concluded in Sec. 5.

2. ROUTING IN MANETS

Routing in mobile ad-hoc networks is one of the central tasks which help nodes send and receive packets. The purpose of routing in a MANET is to discover the most new topology of a continuously changing network to find a correct route to a specific node. In other words with routing a source node finds out the most fresh route to its destination node. Routing protocols developed for wired networks such as the wired Internet are not sufficient here as they not only assume mostly fixed topology but also have high overheads. This has led to various routing protocols specifically targeted for ad hoc networks. IETF MANET working group was tasked with standardization of routing protocols in MANETs. There are several routing protocols designed for wireless ad hoc networks. Routing protocols for ad hoc wireless networks can be classified into three types based on the nature of routing information update mechanism employed. Mainly there are two types: Reactive protocols and Proactive protocols. There are some ad hoc routing protocols with a combination of both reactive and proactive characteristics. These are referred to as hybrid. Reactive protocols are also called Source Initiated on Demand Driven protocols and Proactive protocols are known as Table Driven protocols.

2.1. *Source-initiated routing*

Source-initiated routing represents a group of routing protocols where the route is created only when the source requests a route to a destination [2]. The route is formed through a route discovery procedure. Whenever a node needs to find out path to destination node, it floods the network with route request packets starting with the immediate neighbors of the source. Once a route is formed or multiple routes are obtained to the destination with the help of route reply packets,

the route discovery process comes to an end. A route maintenance procedure maintains the continuity of the route for the duration it is needed by the source. Some of the famous Reactive protocols are: AODV [11], DSR, and TORA.

2.2. *Proactive routing*

In Proactive routing protocols, every node maintains the network topology information in the form of routing tables by periodically exchanging routing information. This is independent of whether or not the route is needed. Routing information is generally flooded in the entire network. In order to accomplish this, control messages are periodically transmitted. Whenever a node requires a path to a destination, it runs an appropriate path finding algorithm on the topology information it maintains. This type of routing strategy has its advantages and disadvantages. One of its main advantages is the fact that nodes can easily get routing information and it's easy to establish a session. The main disadvantage is that lot of bandwidth is consumed for this routing information and some more disadvantages include: there is too much data kept by the nodes for route maintenance and it is slow to reconstitute when there is a failure in a particular link. Examples of Proactive protocols are: DSDV, OLSR, WRP and FSR.

2.3. *Hybrid routing*

The hybrid routing schemes combine elements of on-demand and table-driven routing protocols. The general idea is that area where the connections change relatively slowly are more amenable to table driven routing while areas with high mobility are more appropriate for source initiated approaches. By appropriately combining these two approaches the system can achieve a higher overall performance. Most commonly used Hybrid protocol is ZRP. The protocol uses a pro-active mechanism of node discovery within a node's immediate neighborhood while inter-zone communication is carried out by using reactive approaches.

3. SECURITY ISSUES

As MANET is rapidly spreading for the property of its capability in forming temporary network without the aid of any established infrastructure or centralized administration, security challenges has become a primary concern to provide secure communication. There is no single mechanism that will provide all the security services in MANETs. The common security services are described below:

3.1. *Availability*

Availability states that services and resources must be provided to authorize nodes at all the time [9]. Availability applies both to data and to assets. Availability ensures the survivability of network services despite of various attacks. There should be certain mechanism for detection and protection against such kind of attacks, which makes the network resources unavailable to authorized users like in case of DOS (Denial of service) attack, the availability of network and its resources, would become unavailable to legitimate user.

3.2. *Confidentiality*

Confidentiality refers to hiding of information from unintended receivers. Confidentiality ensures that certain information is only readable or accessible by the legitimate party. Transmission of sensitive information such as military information requires secrecy. In MANET it is very difficult to achieve the secrecy because of intermediate nodes routing, which can easily hear the information which is being routed through them. Basically, it protects data from passive attacks. It should be protected against any revealing attack like eavesdropping where unauthorized reading of message and traffic analysis done by an attacker node to find out which types of communication is going on. In case of war areas it becomes essential to protect and secure such kind of communication. Routing and packet forwarding information must also stay confidential so that the foes could never take the advantages of detecting and locating their targets in a battleground. In MANET it is very difficult to attain the confidentiality because of intermediate nodes routing, which can easily listen the information which is being routed through them.

3.3. *Integrity*

Integrity refers to delivery of message to the intended recipient as such without any modification or alteration. It ensures that assets can be modified only by authorized parties or only in authorized way. Modification includes writing, changing status, deleting and creating. Integrity assures that a message being transferred is never debased.

3.4. *Authentication*

Authentication refers to verifying that the information is coming from a legitimate user. It ensures that the peer node with which communication is going on is not an attacker node. Authenticity is ensured because only the legitimate sender can produce a message that will be decrypted properly with the shared key. One of the methods used in authentication is Digital Signature. In this the sender node signs the message

digitally which will later verify by the receiver node digitally.

3.5. *Non repudiation*

Non repudiation ensures that sending and receiving parties can never deny ever sending or receiving the message. This is helpful when there is need to recognize if a node with some undesired function is compromised or not.

3.6. *Anonymity*

Anonymity means all information that can be used to identify owner or current user of node should default be kept private and not be distributed by node itself or the system software.

3.7. *Authorization and Accounting*

Nodes participating in a network need to have proper authorization to access shared assets on that network. In a MANET, nodes should be able to curtail others from accessing confidential information on their devices. Moreover, in some cases, the authorization policies are accompanied by accounting mechanisms to keep a check on resource utilization to identify chokepoints, charging users for services or for statistical information about the network. Both authorization and accounting require robust methods to guarantee correctness of protocols and proper utilization of assets.

4. ATTACKS IN MANETS

Security aspects were not considered when adhoc protocols were designed. The protocols assume that the environment is friendly and all nodes are cooperative. This assumption is unfortunately not true in an unfriendly environment. Because cooperation is assumed but not enforced in MANETs, malicious attackers can easily disrupt network operations by violating protocol specifications. Now there is vast variety of attacks developed in the past. Many characteristics might be used to classify security attacks in the MANETs. Here a different classification of attacks is presented. Attacks can be broadly classified as shown in fig.1.

4.1. On the basis of nature

On the basis of nature attacks are classified as Active and Passive Attacks. They are discussed below:-

4.1.1 *Passive Attacks*

In passive attacks, the attacker does not actively participate in the attack. A passive attacker obtains data exchanged in the network without disrupting the

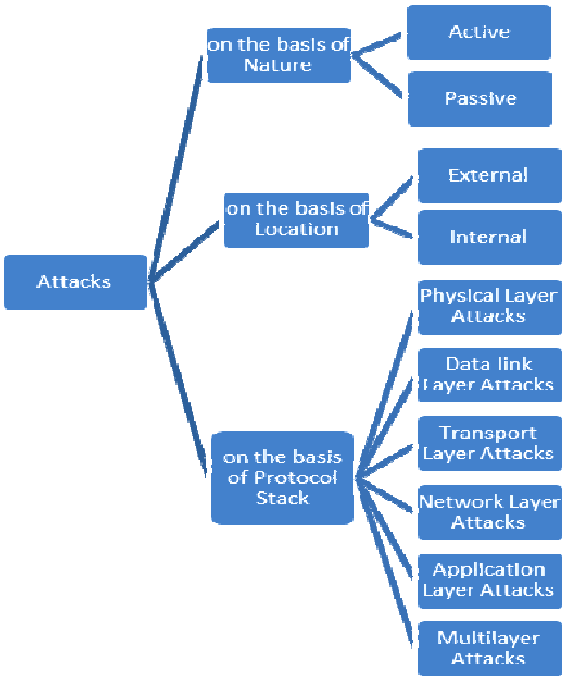

Fig.1. Types of Attacks

normal operation of the communications. Passive attacks include only the network and information monitoring. The main motive of attacker is to track down the packets and then extracting information from them. These attacks are mainly to steal the confidential data moving in the network and monitor the traffic pattern over the network. Because they do not perform the actions on the network, they are hard to detect. Detection of passive attack is very difficult since the normal operation of the network itself doesn't get affected. Some examples of passive attacks are as follows:

4.1.1.1. *Eavesdropping*

Eavesdropping can be defined as interception and reading of messages and conversations by unintended receivers. As the channel in MANETs is wireless, anyone within radio range and with a transreceiver can listen to the ongoing communication. The main aim of this attack is to gain the access over secret information. This information may be private key, public key, location or passwords of the nodes. This is hard to detect as the authorized users have no knowledge that someone is listening their communication. It is considered as a severe attack in case of military communication. In order to overcome this type of attacks powerful encryption algorithms are used to encrypt the data being transmitted.

4.1.1.2. *Traffic Monitoring and Location Disclosure*

In this type of attack, attacker monitors the data flowing through the channel and then analyzes this data to extract information regarding locations of nodes. The attacker measures the intensity of traffic or the type of traffic flow at different time intervals over the specific period of time. For example, in a battlefield scenario, a large amount of network traffic normally flows to and from the headquarters. Traffic pattern analysis therefore allows an intruder to discover the commanding nodes in the network [1].

4.1.2 *Active attacks*

In Active attacks, attacker actively participates in the network activities to execute the attack. An Active attacker attempts to alter system resources or affect their operation. These attacks are more severe as intruders launch intrusive activities such as modifying, injecting, forging, fabricating or dropping data or routing packets, resulting in various disruptions to the network. Active attacks disturb the operations of the network and can be so severe that they can bring down the entire network. They can be detected easily as they degrade the performance of network significantly. Attacks on different layers come under the category of active attacks and will be discussing them in detail in further sections.

4.2 On the basis of Location

On the basis of nature attacks are classified as External and Internal Attacks. They are discussed below:-

4.2.1 *External attacks*

External attacks are executed by attacker that does not legally belong to the network. These attacks usually aim to cause network congestion, denying access to specific network function or to disrupt the whole network operations.

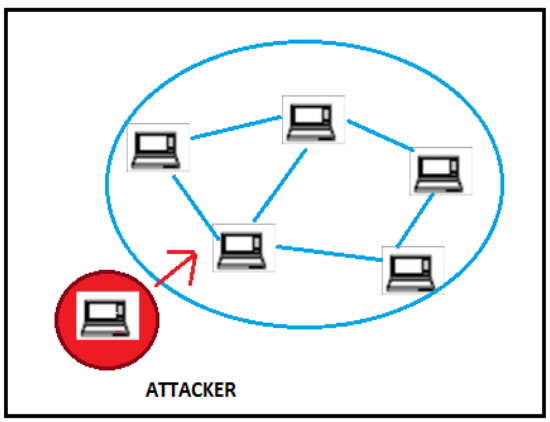

Fig.2. External Attack

4.2.2 *Internal attacks*

Internal attacks are from nodes that are a part of the network. In this type of attack one of the nodes or some nodes of the network are captured and then compromised. Then these nodes being a part of network starts to disrupt the normal operation of communication. This type of attacks may broadcast wrong type of routing information to other nodes or may consume packets. Attacks that are caused by the misbehaving internal nodes are difficult to detect because to distinguish between normal network failures and misbehavior activities in the ad hoc networks is not an easy task.

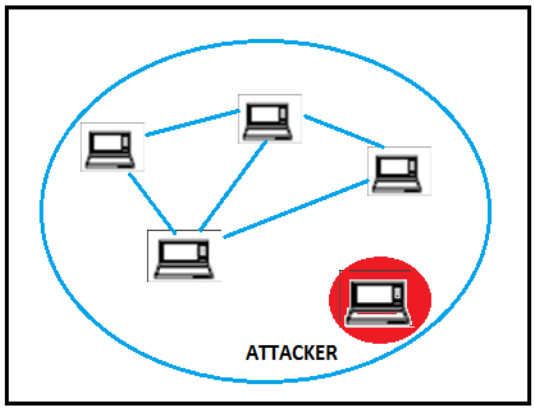

Fig.3. Internal Attack

4.3 On the basis of Protocol Stack

Attacks can also be classified according to the layers of protocol stack. The table below shows classification of attacks on different layers.

Table1. Layer wise Attacks

LAYER	ATTACKS
Physical layer	Jamming, Interference , Stolen or compromised attack
Data link layer	MAC targeted, WEP targeted, Bandwidth Stealth
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, blackhole, Byzantine, flooding, resource consumption, location disclosure attacks, Link withholding, link spoofing, Jellyfish, Colluding Misrelay, Rushing
Application layer	Repudiation, Viruses or Worms
Multilayer Attacks	DoS, impersonation

4.3.1 *Physical Layer Attacks*

The attacks on physical layer are hardware centered and they need help from hardware sources to come into effect. An attacker with sufficient transmission power and knowledge of the physical and medium access control layer mechanisms can gain access to the wireless medium. Some of the attacks identified at physical layer include eavesdropping, interference and jamming, Stolen or compromised attack, Device Tampering etc. Eavesdropping has already been discussed under external attacks. The rest of them are discussed as follows:

4.3.1.1 *Jamming*

Attacker exploits the property that more than one host within MANET share a single wireless medium, which naturally is dispersing airwave signals so other participants (or participating nodes) in its range can receive this signals. A powerful transmitter can generate signal that will be strong enough to overpower the target signal and can disrupt communications. This condition is called jamming. Jamming can be Trivial Jamming, In which an attacker constantly transmits noise or Periodic Jamming Attack, in which an attacker transmits a short signal periodically. These transmissions can be scheduled often enough to disrupt all other communications.

4.3.1.2 *Interference*

Interference is that type of attack in which the intruder tries to interfere with the original signal and main motive in this is to decrease the signal to noise ratio of received signal. It does so by introducing noise signals of the same frequency range as used in the communication.

4.3.1.3 *Stolen or compromised attack*

These kinds of attacks are happened from a compromised entities or stolen device like physical capturing of a node in MANET. It may occur due to device tampering.

4.3.2 *Data Link Layer Attacks*

MANET is an open multipoint peer-to-peer network architecture. Specifically, single-hop connectivity among neighbors is maintained by the link layer protocols, and the network layer protocols extend the connectivity to other nodes in the network. Attacks may target the link layer by disrupting the cooperation of the layer's protocols [3].

4.3.2.1. *MAC Targeted Attack*

The IEEE 802.11 MAC is vulnerable to DoS attacks. To launch the DoS attack, the attacker may exploit the binary exponential backoff scheme. The binary exponential scheme favors the last winner amongst the contending node. This will lead to a phenomenon called capture effect. The nodes that are heavily loaded tend to capture the channel by continuously sending data, thereby causing lightly loaded neighbors to backoff endlessly. Malicious node can take the advantage of this capture effect vulnerability [3].

4.3.2.2 *WEP Targeted Attack*

IEEE 802.11 WEP, wired equivalent privacy is designed to improve the security in wireless communication that is privacy and authorization. However it is well known that WEP has number of weaknesses and is subject to attacks. Some of them are [7]:-

- WEP protocol does not specify key management.
- The initialization vector (IV) used in WEP is a 24-bit field which is sent in clear and is a part of the RC4 leads to probabilistic cipher key recovery attack or most commonly known as analytical attack.
- The combined use of a non-cryptographic integrity algorithm, CRC 32 with the stream chipper is a security risk and may cause message privacy and message integrity attacks.

4.3.2.3 *Bandwidth Stealth*

In this kind of attack the attacker node illegally consume the large fraction of bandwidth which leads to congestion in the network.

4.3.3 *Network Layer Attacks*

The protocols in network layer are for different connections among the nodes. They extend connectivity from single hop neighbor nodes to multihop mobile nodes. These protocols work on the cooperation of different nodes. By attacking routing protocols the whole network can be disrupted. Network layer attacks are discussed below:

4.3.3.1. *Attacks at the routing discovery phase*

There are attacks that target the route discovery phase in routing protocols. Routing protocols in MANETs are to discover and maintain routes for communication. Proactive protocols like DSDV discover their route before any demand of route where Reactive protocols like AODV discover route after demand of route. Due to this proactive algorithms are

more prone to route discovery attacks. Routing table overflow, Routing cache poisoning, and Routing Table Poisoning are simple examples of routing attacks targeting the route discovery phase. They are discussed as follows:

- *Routing table overflow attack*

As the name suggests, in this attacker node tries to overflow the victim node's routing table. It does so by initiating route discovery to non-existent nodes. This leads to consumption of limited memory of mobile node by having such entries in their routing table which in turn prevents the creation of new routes to authorized nodes in the network. Proactive routing algorithms are more vulnerable to these attacks as they update routing information periodically. An attacker can simply send excessive route advertisements to overflow the victim's routing table.

- *Routing cache poisoning attack*

In route cache poisoning attacks, attackers capitalize on the promiscuous mode of routing table updating. In this mode a node maintains its route cache by overhearing any packet in its neighborhood transmission and then adds the routing information contained in that packet header to its own route cache, even if that node is not on the path. In the case of on-demand routing protocols (such as AODV, DSR), each node maintains a route cache which holds information regarding routes that have become known to the node in the recent past. An attacker could broadcast spoofed packets with source route to victim node via itself; thus, neighboring nodes that overhear the packet may add the route to their route caches.

- *Routing table poisoning attack*

In this type of attack, the compromised nodes in the networks send fabricated routing updates or modify true route update packets sent to other uncompromised nodes. It may result in forwarding packets along sub optimal routes, congestion in the network, formation of loops or blackmail attack.

4.3.3.2 *Attacks at the routing maintenance phase*

In routing protocols some control messages are usually employed for maintenance of active and valid paths. Attackers target these control messages to launch attacks during route maintenance phase. Adversaries broadcast spoofed control or signaling messages (e.g., broken link error messages) that activate costly route reconfiguring or repairing procedures from a source to a destination. For example, in case of AODV and DSR mechanisms are adopted for recovering from broken routes. In such mechanisms, when the destination node and/or other nodes along the path from a source to destination move, the upstream node of the broken link transmits a route error message to each of the other upstream hosts. In addition, the node also purges this particular route to the destination. A malicious user may exploit this by broadcasting false route error messages and prevent the source node (i.e., the victim node in this case) from communicating with the destination [13].

4.3.3.3. *Attacks at Data Forwarding Phase*

In this type, malicious nodes attack the data forwarding functionality of nodes. It does not affect route discovery or route maintenance in this case. In this the attention is focused on data packets. For instance, a malicious user may drop silently, modify data content, replay, or flood data packets. They can also inject false packets in to the ongoing communication.

Some special attacks

- *Blackhole Attack*

This attack capitalizes on route discovery mechanism of reactive routing protocols. In this the malicious node presents itself to the victim node as a fresh and shortest route to destination. It does so by replying positively to the route requests made by victim node(s).It claims the freshness by replying with the highest sequence number and minimum hop count. After this, route is established and then victim node starts sending packets to attacker node. At this point its attacker's wish what to do with the packets and as the name suggests its drops all the packets and so called as blackhole node.Fig.4 shows the blackhole attack.

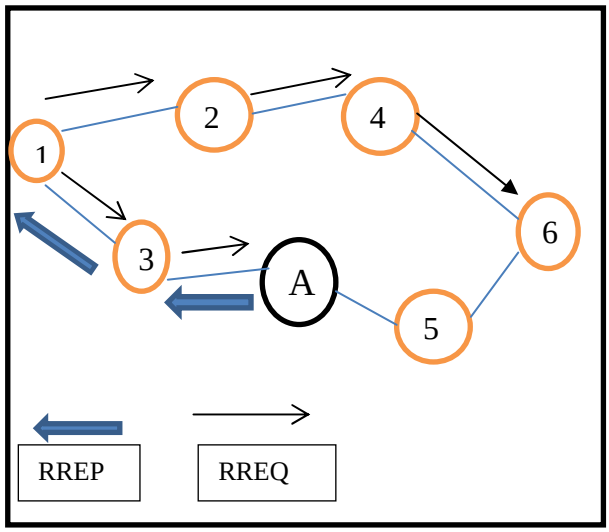

Fig.4 Blackhole Attack

Here node 1 wants to send packets to node 6 and A is an attacker. When 1 broadcasts RREQ to all neighbor nodes for route to node 6, then A sends fake RREP to 1 with hop count set to minimum and sequence number set to maximum, making A the most optimal route to destination node. So 1 starts sending packets to A which then starts dropping all packets executing the blackhole attack.

- *Grayhole Attack*

It is just modification of blackhole attack. In this attacker performs the step of fake RREP same as in blackhole attack but in the next step it does not drop all the data packets. It drops selectively some packets and forward rest of the packets. This makes it more difficult to detect Grayhole attack as dropping some packets and passing rest makes it looks like congestion in network or some other valid reason.

- *Wormhole Attack*

It is particularly challenging to defend against wormhole attack [12]. Wormhole attack is one of the most serious and well planned attacks. In this, two or more malicious nodes collude together by establishing a tunnel using an efficient communication medium (i.e., wired connection or high-speed wireless connection etc.)[6]. It is also called tunneling attack. Fig.5 shows the wormhole attack.

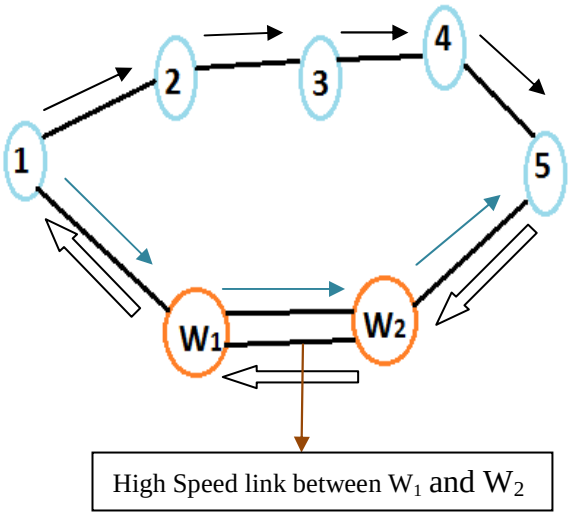

Fig.5 Wormhole Attack

In this, two attackers W1 and W2 form a tunnel. During the route discovery phase node1 send RREQ messages to neighbor nodes. When the first attacker W1 receives RREQ from node1 it sends it through high speed link to second attacker W2 which forwards it to destination node5. Now the RREQ from W1 and W2 reaches destination earlier than any other node so other RREQs are discarded and the malicious nodes are added in the path from the source to the destination. Once the malicious nodes are included in the routing path, the malicious nodes either drop all the packets or drop the packets selectively to avoid detection.

- *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 [10].

- *Resource consumption attack*

As the name suggests the target of this attack is mainly the resources of nodes. The resources that can be targeted are battery power, bandwidth, and computational power, which are only limitedly available in ad hoc wireless networks. The attacks could be executed through unnecessary requests for routes, very frequent generation of beacon packets, or forwarding of stale packets to nodes. One example of resource consumption is sleep deprivation attack. In Sleep deprivation attack, attacker interacts with the node in a manner that appears to be legitimate, but where the purpose of the interaction is to keep the victim node out of its power conserving sleep mode [1].

- *Rushing Attack*

This attack forces entire network traffic to pass through an attacker. The source node is unable to find any secure route without the attacker. Malicious node after receiving RREQ packet from initiating node reacts immediately and floods the network quickly with these packets before other nodes receiving the same RREQ can respond. This is the reason it is called rushing attack as malicious nodes rushes packets. Nodes receiving legitimate RREQ packets treat them as duplicates and discard them. So every route established has attacker as one of the intermediate nodes [9].

- *Link withholding attacks*

In this attack, a malicious node does not advertise the information about the links to specific nodes or group of nodes. It holds the information itself. This may result in losing the links to these nodes. This type of attack is particularly serious in the OLSR protocol.

- *Link spoofing attack*

In a link spoofing attack, an attacker node broadcasts spoofed links with non-neighbors to disrupt the 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 multipoint relay [10].

- *Partitioning Attack*

An attacker may try to partition the network by injecting forged routing packets to prevent one set of nodes from reaching another [8].

- *Location disclosure attack*

In this, attacker node after acting as a part of network leaks out information. Such information may include knowledge regarding the network topology, geographic location of nodes, or optimal routes to authorized nodes. This information is then used by other nodes for further attacks. The leakage of such information is devastating in security-sensitive scenarios.

- *Replay attack*

It is known that nodes in MANET are mobile in nature and the topology changes randomly. Due to this the routes that are valid in past may have become dead now. Attacker takes the advantage of this as it records valid control messages in the past and resends them later. This causes nodes to add dead and invalid routes in their routing table which disrupts the whole routing operation.

- *Colluding misrelay attack*

In this attack, two or more adversaries work in collusion to drop or modify packets. This attack is difficult to detect by using the conventional methods such as watchdog and pathrater [4].Fig.6 shows colluding misrelay attack.

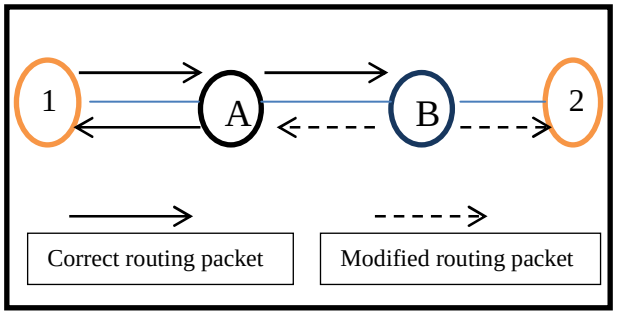

Fig.6 Colluding misrelay Attack

In this A and B are two attackers. Attacker A forwards packets from node 1 without any modification so as to prevent itself from detection but attacker B modifies or drops packets. It is hard to detect as one of the attackers is performing normally and other is playing active role.

- *Jellyfish Attack*

It is a selective blackhole attack in which malicious node attacks the network by changing order of packets, dropping selective packets or increasing jitter of the packets that pass through it in order to prevent it from being detected and it seems to the network that loss or delay is due to environmental reasons [9].

4.3.4 *Transport Layer Attacks*

The objectives transport layer protocols in MANET include setting up of end-to-end connection, end-to-end Reliable delivery of packets, 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**.**

4.3.4.1 *SYN flooding attack*

The SYN flood attack sends TCP connections requests faster than a machine can process them. For two nodes to communicate using TCP, they must first establish a TCP connection using a three-way handshake. A normal three step handshake process and a handshake process of an attacker are shown in fig.7 and fig.8. In normal process one of the node ask for establishing a connection by sending a SYN request. Then the requested node responds by sending SYN ACK (Synchronization acknowledgement).Final step is completed by initiator node by sending ACK to SYN ACK.

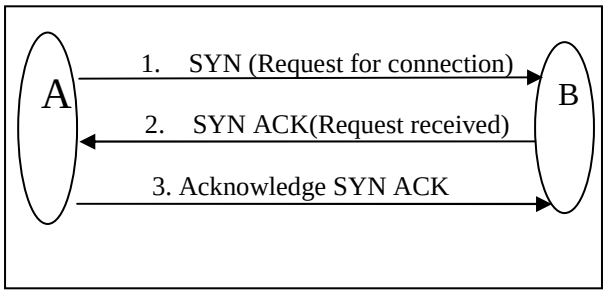

Fig.7 Normal Handshake Process

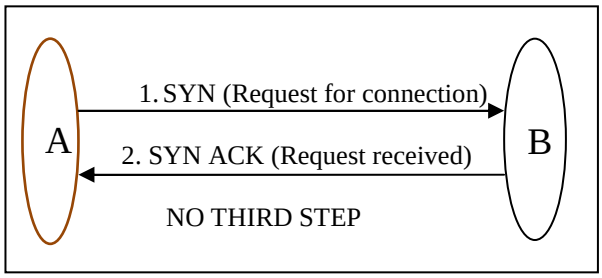

Fig.8 Handshake Process with Attacker

In case of attacker, first two steps are followed normally but the third step is never done. This creates half open connections. Without receiving the ACK packets, the half-open data structure remains in the victim node. Attacker, in this way sends a large amount of SYN packets to a victim node. So a large number of half open connection are created and if the victim node stores these half-opened connections in a fixed-size table while it awaits the acknowledgement of the three-way handshake, all of these pending connections could overflow the buffer, and the victim node may come to a halt even. Another way of launching this attack is spoofing the return address of SYN packets with non-existent node so SYN+ACK packets never reach any node fooling the victim node.

4.3.4.2 *Session Hijacking*

One weak point is that most authentications processes are only carried out once when a session starts. An adversary could try to appear as an authentic node and hijack the session. An attacker gets access to the session state of a particular user by stealing session ID which is used to get into a system and then finks the data. At first attacker predicts the correct sequence number and then spoofs victim‘s IP address. The attacker executes a DoS attack on the victim, aiming to continue the session with the target.

4.3.5 *Application Layer Attacks*

The application layer contains user data, and it supports many protocols such as HTTP, SMTP, TELNET, and FTP, which provide many vulnerabilities and access points for attackers. The application layer attacks are attractive to attackers because the information they seek ultimately resides within the application and it is direct for them to make an impact and reach their goals [10]. The various attacks are discussed below:

4.3.5.1. *Viruses & Worms*

These are malicious code or programs that could damage operating system or whole network. They replicate themselves and can transmit to all other systems. They could possibly leaks out information from the victim node and transfers it to other attackers for further attacks.

4.3.5.2. *Repudiation attacks*

In the network layer, firewalls can be installed to check incoming and outgoing packets. In the transport layer, end-to-end encryption to connections can be provided. But these solutions do not solve the authentication or non-repudiation problems in general. In Repudiation an attacker refuses to participate in all or part of the communication. For example a selfish node can deny processing an online bank transaction. These attacks are detected by sophisticated techniques.

4.3.6 *Multi-layer attacks*

A multi-layer attack is an attack which can be executed from more than one layer within a network. Examples of multi-layer attacks are denial of service attacks, impersonation attacks and man-in-the-middle attack.

4.3.6.1 *Denial of service (DoS) attack*

The basic purpose of DoS attack is simply to flood/overhaul network so as to deny authentic user services of the network. It can be launched at different layers. At the physical layer, through signal jamming attack normal communication is disturbed. At the link layer, malicious nodes can capture channel and prevent other nodes from channel access. At the network layer, DoS attacks are mounted on routing protocols and disrupt the network performance through flooding various types of routing packets. At the transport and application layers, SYN flooding, session hijacking, and malicious programs can cause DoS attacks.

4.3.6.2 *Impersonation attacks*

Impersonation attacks are launched by using other node’s identity, such as MAC or IP address. Each node in a MANET requires a unique address to participate in routing, through which nodes are identified. However, in a MANET there is no central authority for this identity verification. An adversary can exploit this property and send control packets, for example RREQ or RREP, using different identities; this is known as a Sybil attack. This is an impersonation attack where the intruder could use either random identities or the identity of another node to create confusion in the routing process, or to establish bases for some other severe attack [4].

5. CONCLUSION

MANETs can be applied in various situations ranging from emergency operations and disaster relief to military service and task forces. Providing security in such scenarios is critical. The paper gave state-of-the-art analysis of attacks discovered by researchers in MANET and also discusses challenges in security. Confidence in MANETs is mainly constrained by its security. The survey presented in this paper will be a helpful instrument in studying attacks and then developing secure protocols.

REFERENCES

[1] Adnan Nadeem and Michael P. Howarth, "A survey of MANET Intrusion Detection & Prevention Approaches for Network layer Attacks", IEEE Communication Surveys & Tutorials, pp.1-19, 2012.

[2] Azzedine Boukerche, Begumhan Turgut, Nevin Aydin, Mohammad Z. Ahmad, Ladislu Boloni, Damla Turgut, "Routing protocols in Adhoc network: A survey", Elsevier, Computer Network 55(2011) 3-32-3080.

[3] 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.

[4] 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

[5] C. Perkins, Ad Hoc Networks, Addison-Wesley, 2001 .

[6] 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.

[7] Kamanshis Biswas & Md. Liakat Ali, "Security threats in Mobile Ad-hoc Network", Master thesis, Department of Interaction & System Design, Blekinge Institute of Technology, Sweden 22nd of March 2007.

[8] 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.

[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] http://www.ietf.org/rfc/rfc3561.txt

[12] Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks," *IEEE JSAC*, vol. 24, no. 2, Feb. 2006.

[13] Zubair Muhammad Fadlullah, Tarik Taleb, and Marcus Schöller, "Combating against Security Attacks against Mobile Ad Hoc Networks (MANETs),"Security of self-organizing networks: MANET, WSN, WMN, VANET, AS. K.Pathan pp173-194, CRC Press, Taylor & Francis Group 2011.