Review of different types of Security Attacks in Mobile Ad hoc network (MANET)

Gurpreet Kaur
Computer Science and Engineering, Lovely Professional University Phagwara, Punjab (India)
Email - gdaljit.93gmail.com,

Abstract: *Mobile ad hoc network (MANET) is an infrastructure less network (no pre fixed infrastructures),dynamic network is a collection of wireless nodes (mobile ,laptop) that communicate with each other without using the any centralized authority. Mobile ad hoc networks are self-configure network mean automatically establishment network of mobile nodes connected via a wireless link(used wi -fi connection).The nature and structure of such kind of network make it attractive to various types of attackers. Security is the main concern for protected communication between mobile nodes .MANET is a vulnerable (weakness in security system) to various kind of security attack. In this paper telling whole security attack come under in mobile ad hoc network.*

Key Words: *Mobile ad hoc network (MANET), Security Attacks.*

1. INTRODUCTION:

A mobile ad hoc network (MANET) is the self-configuring network of mobile nodes that can communication to each other via radio waves. The mobiles nodes that are in radio range of each other can directly communicate. Nodes in MANETs can join and leaves the network dynamically .There is no-fixed set of infrastructures and centralized administration in this types of network. The dynamic nature of such type's network makes it highly susceptible to various link attacks. As the transmissions takes places in open medium makes the MANETs more vulnerable to security attacks. Vulnerability is a weakness in security system. Security is a major concern for protected communication between mobile node in a hostile environment (unfriendly environment).

2. MANET characteristics : There are some characteristics in following:-

- Distributed operations: There is no central control in network operations, the control of the network is distributed among the nodes.
- Multi-hop routing: When a node tries to send the information to other nodes which is out of communication ranges, the packet should be forwarded via one or more intermediate nodes
- Autonomous-terminal: In MANET,each node is an independent node which could function as both such as host and a routers.
- Dynamic topology: Nodes are free to move with differently speed. Thus the topology may change randomly. Nodes are free to connect to any nodes. The topology between the nodes are changing continuously.
- Light weight terminals are less cpu capability, low power ,storage and small memory.
- Shared physical medium use the wireless media. The communication medium is broadcast nature and connection of different nodes is wireless.

3. Application of MANET

- Military Battlefield(communication)
- Medical services
- Personal area network
- Local levels
- Disaster recovery managements

4. Security Attacks:-

Securing the wireless ad-hoc network is a highly challenging issues. Understanding the possible form of attacks is always the first step towards developing the good security solution. Security of the communication in MANET is very important for secure transmission of information. Absence of any central co-ordination mechanism and use shared wireless medium make MANET more vulnerable to digital / cyber attacks than wired network .Mobile ad hoc networks are vulnerable to various attack not only from outside but also from within the network itself .Ad hoc network are mainly subjected to two different levels of attacks.

The first level of attack occurs on the basic mechanism of the ad hoc network such as routing The second level of attack s tries to damage the security mechanisms employed in the network.

5. The attacks in MANETs are divided into two major types:

Internal Attack

The internal attack are directly leads to the attack on nodes present (within) in network.

External Attack

These types of attack try to cause congestion In the network ,denial of services(dos).External attack prevent the network from normal communication and producing additional overhead to the network .

External attacks can be classify into two categories:

1 . Active attack

2 . Passive attack

Active Attack :

Active attacks can be carried out by outside source that do not belong to the network . These attack generate unauthorized access to network that helps the attacker to make changes (alter) such as modification of packet. Active attack are very severe attack on the network that prevent (stop) message flow between the nodes .

Passive Attack:

A Passive attack does not alter the data transmitted within the network .In which attacker or unauthorized "listening " to the network traffic or accumulates data from it . The attacker only steal the useful information from the targeted network .

ACTIVE ATTACK:

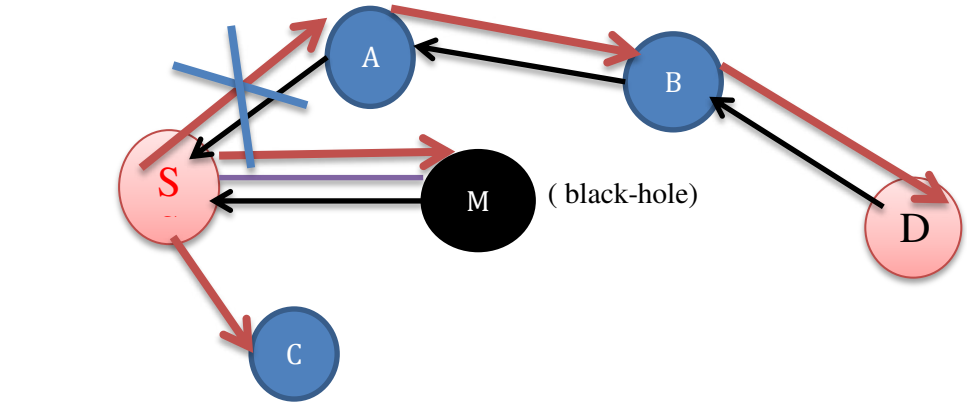
Some attacks under in the active attack are following :

- Black- hole attack
- Worm-hole attack
- Gray-hole attack
- Sink-hole attack
- Denial of service(Dos)
- Sybil attack
- Byzantine attack
- Man -in –the- middle attack
- Fabrication
- Spoofing
- Modification
- Replay attack
- Rushing attack etc.

a. **Black hole attack**:

In black-hole attack the malicious node present itself as the shortest and network route to the destination node and attracts the routing packets. In this types of attack malicious node claims having an feasible or optimum route to the node whenever it receive a RREQ packet and send the RREP with highest destination sequence number and minimum hop count value to originator node. A malicious node acts like a black –hole, dropping all the data packet passing through it . It is a network layer attack. For example in the figure 1 When a node "S" want to send the data to the destination node "D", it initiates the route discovery process. The malicious node "M" when a receives the routes request it immediately sends responses to source. If reply from node "M" reaches first to the source than the source node "S" ignores all other reply messages and begin to send packet via route node "M".As a result all data packet are consumed or lost at malicious node. The black hole attack drop the packet every time.

FIGURE 1: Black hole attack



RREQ

RREP

DATA PACKET

S -- SOURCE NODE

D -- DESTINATION NODE

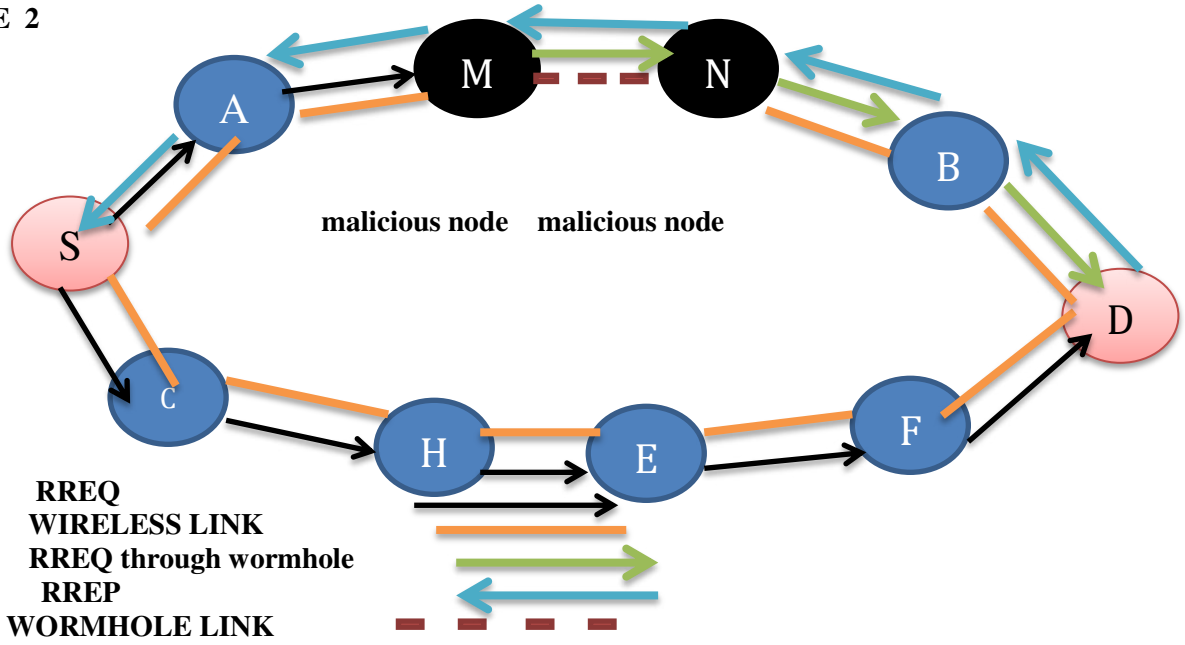
M -- MALICIOUS NODE

A, B and C is INTERMEDIATE (HOPs) NODES

b. Worm- hole attack:

In the worm hole attack , malicious node or attacker node receive data packet at one point in the network and tunnels them to another malicious node. The tunnel exist between two malicious node is referred to as a worm hole . Routing can be disrupted when routing control messages are tunneled . In which mainly concept disrupting flow of the packet. For example figure 2 the nodes M and N are malicious node that form the tunnel in network. The originating node of "S" when initiate the RREQ message to find out the route to node "D" destination node .The immediate neighbor node of originating node of "S" namely "A" and "C" forward the RREQ message to their respectives neighbor node so on. When a M malicious node receive the RREQ it immediately shares with it N (malicious) node and later it initiate RREQ to its neighbor node through which the RREQ is delivered to the destination node "D".Due to high speed link it force the source node to select route <S-A--B-D> for destination. It result in "D" ignore RREQ that arrives at a later time.

FIGURE 2



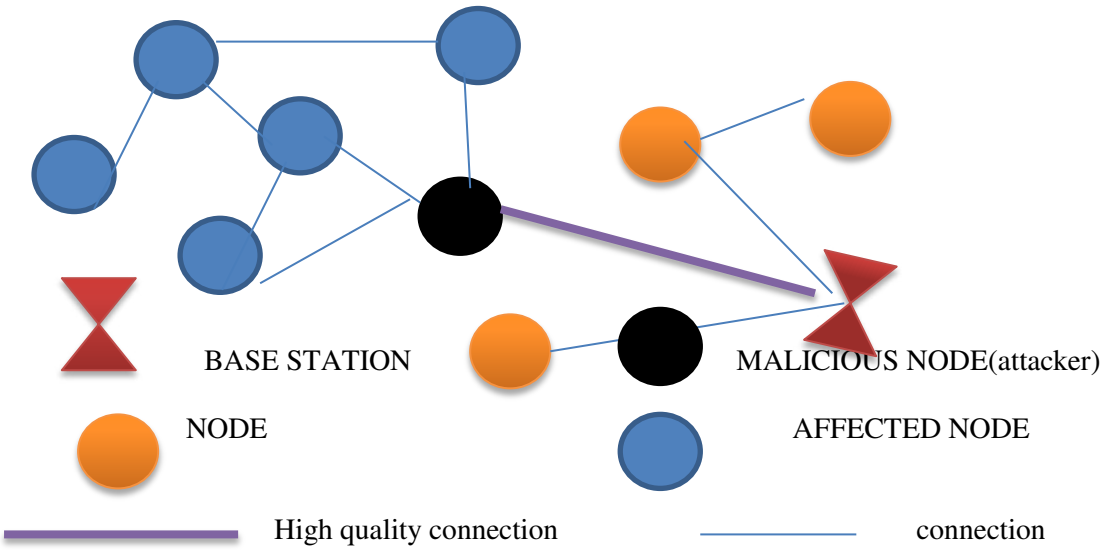
RREQ
WIRELESS LINK
RREQ through wormhole
RREP
WORMHOLE LINK

S SOURCE NODE **D DESTINATION NODE**

c. Gray hole attack: This attack is also known as routing misbehavior attack which lead to dropping of message . It is a network layer attack. Gray hole attack has two phases. In the first phase the advertise itself as having a valid route to destination while in second phase , nodes drops intercepted packet with a certain probability.This attack is also known selective forwarding attack. In which the malicious nodes try to stop the packet in the network by refusing to forward or drop the message passing through them. In this attacks tends to drops the packets while the routing process.

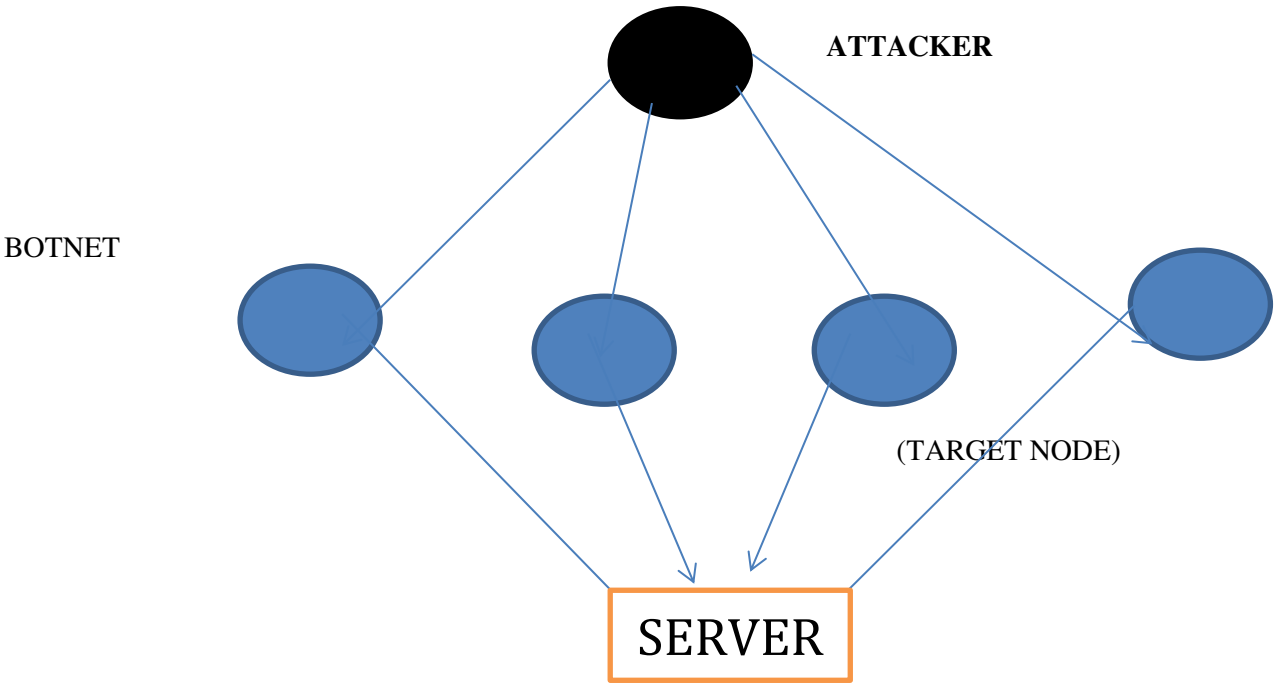
d. **Sinkhole attack**: The attacking node tries to offer a very attractive link e. g to a gateway (which whole traffic going). Therefore a lot of traffic bypasses this node. The compromised node advertises itself in such a way that it has shortest path to the destination. Sinkhole is a service attack that prevents the base station from obtaining complete and correct information.

FIUGURE 4: SINKHOLE ATTACK



e..Denial of service(DoS): In this attack malicious node prevent other authorized nodes to access network data or services. Using this attack , a specific node or service will be inaccessible and packet delay and congestion increases .In this type of attack ,malicious node sending the message to the node and consume the bandwidth of the network. The aim of the malicious node is to be busy the network nodes.

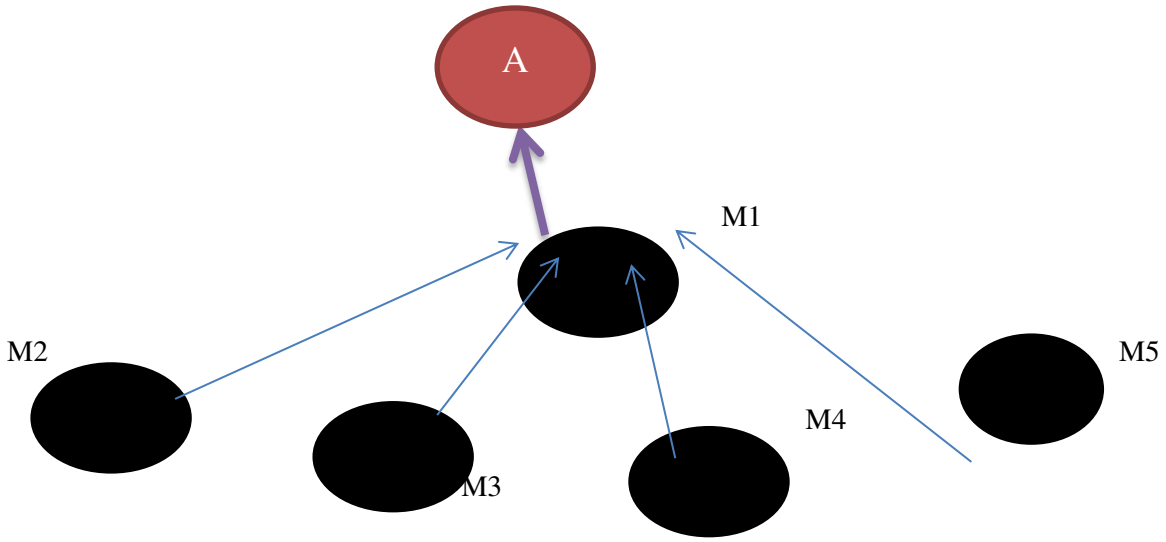
FIGURE 5: DOS ATTACK



In DOS Attacker send commands to botnet(automatically machine) ,botnet floods server with message

f . Sybil attack: The Sybil attack refer to the multiple copies of malicious nodes. In which the attacker tries to act as several different identities /node rather than one. The sybil attack manifest itself by faking multiple identities by pretending to be consisting of multiple nodes in the network .Due to this reason disruption can be quite high. M1 node assumes identities of M2,M3,M4 and M5 so to node A, M1 is equivalent to those nodes.

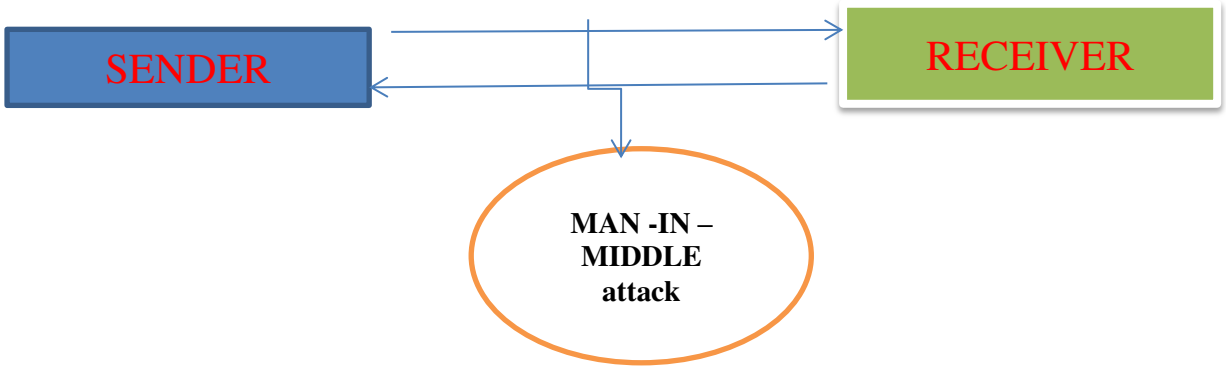
FIGURE 6: SYBIL ATTACK



g. Byzantine attack: In this attack , a set of intermediate or hop node work between the sender and receiver and perform some change such as creating routing loop , sending the packet through non optimal path or selectively dropping packet . which result in disruption of routing service

h. Man -In -the -Middle attack: The man in middle attack , the attacker sites between the sender and receiver and capture (sniffs) any information being sent between two nodes.

FIGURE:8



i. Fabrication attack : In the fabrication attack , malicious node destroys the routing table of the nodes by injecting the fault information .Attacker generating false routing message. This mean it generate the incorrect information about the route between devices.

j. Spoofing attack: In this attack, when a malicious node miss present his identity so that the sender change the topology. The Attacker assumes the identity of another node in network

Modification: The Malicious nodes performs some modification in the routing so that sender sends the message through the long route. This cause time delay and communication delay is occurred between sender and receiver.

k. Rushing attack: The rushing attack are mainly against the on demand routing protocol .These types of attack subvert the route discovery process. Two colluded attacker use the tunnel procedure to from a wormhole .If the fast transmission path (e.g dedicated channel shared by attacker) exist between the two end of the wormhole ,the tunneled packet can propagate faster than those through the normal multi – hop route.

6. CONCLUSION: Here we can map the attacks (active or passive) with the layers:

Attacks	Active attack	Passive attack	Layer
➢ Black- hole attack	✓		**Network layer**
➢ Worm-hole attack	✓		**Network layer**
➢ Gray-hole attack	✓		**Network layer**
➢ Sink-hole attack	✓		**Network layer**
➢ Denial of service(Dos)	✓		**Multi layers**
➢ Sybil attack			**Network layer**
➢ Byzantine attack	✓		**Network layer**
➢ Man -in –the-middle attack	✓		**Multi layers**
➢ Spoofing	✓		**network layer**
➢ Fabrication	✓		**Multi layers**
➢ Modification	✓		**Multi layers**
➢ Replay attack	✓		**Multi layers**
➢ Rushing attack	✓		**Multi layer**
➢ Traffic monitoring		✓	**Data link layer**
➢ Eavesdropping	✓	✓	**Physical layer**

REFERENCE:

1. Aarti and Dr.S.S. Tyagi (2013) ,"Study of MANET: characteristics , applications and security attack"
2. Satyam shrivastava et al./ (3 march 2013)" A brief introduction of different types of security attacks found in mobiles ad hoc network " International journal of computer science & engineering technology,.
3. Priyanka Goyal and Ajit singh (2010) ,"A literature review of security attacks in mobile Ad –hoc Network",.
4. Manjeet singh and Gaganpreet kaur (june 2013)."A surveys of attacks in MANET", volume 3 , issues 6.
5. Arnab Banejee and Debika Bhattachrjee ,"Different types of attacks in mobile adhoc network ".
6. Mohan V.Pawar (2015) ,"Network security and types of attacks in networks"..
7. Jyoti Thalor et al ," Detection and prevention technique in mobile adhoc network "(2014).
8. S.Mueller, R. P. Tsang, and D. Ghosal (2014), Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges,.
9. A. Boukerche, B. Turgut, N. Aydin, and M. Z. Ahmad (2011), Routing protocols in ad hoc networks: A survey,‖ Computer Networks, pp. 3032-3080,.