IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

SECURITY ISSUES IN MANETS

Pimal Khanpara

ABSTRACT

A Mobile Ad Hoc network is a cluster of communication devices that wish to interact within themselves without any fixed infrastructure. The majority of applications of MANET are in areas where no wired connection is required and rapid deployment and dynamic reconfiguration is required. Earlier studies on ad hoc networks aimed to propose solutions to some fundamental problems, such as routing, copying with the new challenges caused by network's and nodes features without taking the security issues into account. This paper talks about the problems existing in MANET.security issues into account. This paper talks about the problems existing in MANET.

Keywords: MANET, Ad-hoc, Eavesdropping, Jamming, DoS, Active interference, Malicious, Black hole attack, Sinkhole attack, Wormhole attack, Spoofing, Session hijacking.

I. INTRODUCTION

MANET- Mobile Ad-hoc network."Ad-hoc" means "for that particular purpose" [1].It does not contain any infrastructure and every devices are connected without wires. All devices in MANET are self-configured. Every node in this network are mobile and can change to other devices frequently. Every devices can act as a router as well as hosts. Ad-hoc networks are different from other networks because they have flat infrastructure, work on shared medium (example: - radio), have dynamic topology. In this network every computer device acts like a router as well as end hosts.

I. APPLICATIONS

- In wireless communication there is primary requirement of MANET which provides effective communication, even where efforts in group is required..
- At the time of disaster, there is need of wireless network. The places where wired network may be affected by the disasters, MANET can be implemented [2].
- Military battlefield: - Ad hoc networking would allow the military to maintain an information network between the soldiers, vehicles and military information headquarters.
- Economic and commercial: - Ad hoc can be used in emergency or rescue operations such as emergency in earthquake, in floods etc. Other commercial scenarios include ship-to-ship ad hoc mobile communication,etc

II. ATTACKS IN MANETS

A. ATTACKS AT PHYSICAL LAYER

1. **Eavesdropping [3]:-** This is a passive attack. Eavesdropping refers to unauthorized monitoring of other people's communication. Since eavesdropping do not affect normal transmission of data in networks, sender or receiver hardly notice that the data is stolen, intercepted or defaced. It obtains confidential information like private key, location and routing information, passwords of the nodes which should restricted during communication.
2. **Jamming**:- It is one of the specific types of DoS attack. The objective of this attack is to prevent the legitimate sender and receiver from transmitting and sending packets on the network i.e. to interfere between two communicating authentic nodes. It will interfere with live communication by injecting dummy packets into the shared medium. In some cases it also abuses the MAC layer of other nodes.
3. **Active Interference**:- This is type of DoS attack. In this attack it interrupts the wireless communication channel. In active interception the messages transmitted can be overheard by the intruder, and afterwards may push duplicate messages into network on the user's behalf where as in passive interception the network traffic is routinely monitored to collect qualitative information, or other information not explicitly communicated via a data stream. In order to replay old messages attacker changes the message sequence. Old messages can be played again or canreintroduced out of date information.

B. ATTACKS AT DATA LINK/MAC ADDRESS

1. Selfish misbehaviour of nodes [4]: - These are the nodes where it wants to preserve its own resources while using the services of others and consuming their resources. The node uses its resource when there is need in the network and after using it turn tranquil, not visible to network. When there is need of resources for packets it will show disinterest in packets and will drop them. Selfish nodes can perform below actions in ad-hoc network:

*a)*Being quite when not having any communication with other nodes.

*b)*On receiving RREQ messages it does not broadcast these messages in network.

*c)*Re-broadcast RREQ, forward RREP on reverse path but does not forward data packets.

*d)*In order to fight with existing mechanism it drop data packets selectively.

Based on above threats we can see how damaging are these nodes can be in MANET, particularly in terms of reducing delivery rates by dropping packets.

2. Malicious behaviour of nodes[5]: - When a node breaches any of the security principles and is therefore under any attack it acts maliciously in the network. Such node exhibit the following behaviour: **-**

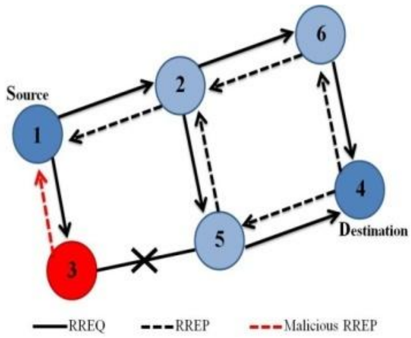
- Packet dropped
- Battery drained
- Stale packets
- Delay
- Link break
- Node not available

- Stealing information
- Delay

3. Traffic analysis: - process of collecting information on the way to keep track of essential information in communication, or in other words gathers all the information of the network. Traffic analysis may leak information such as location of nodes, network topology used for communication; roles played by nodes, available source and destination nodes.

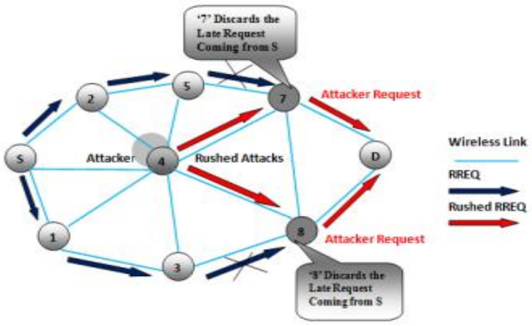
C. ATTACKS AT NETWORK LAYER

1. Black hole attack: - Here the malicious node publicize itself as having best path in route discovery process. As soon as it receives the RREQ packets it will send fake RREP packet to source node [6][7][8].



In the above figure we see that node 3 act as malicious node. When node 1 (SN) will send RREQ packets to all nodes, node 3 will reply as having shortest path in this network. It will take all the packets from the source node and will drop all packets instead of forwarding to the node 4 (DN).

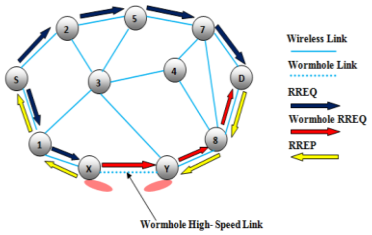
2. Rushing attack: - Rushing attacks are used against all on-demand routing protocol[9].



When a source node sends route request packet in a network the malicious node (node 4 in above figure) will accept the RR packet and will send it with high transmission speed as compared to another nodes present in the network [10]. The destination node will receive this packet and will discard the other actual data packets which it will return later. Receiver will found this route as valid route and attacker will successfully gain access in communication.

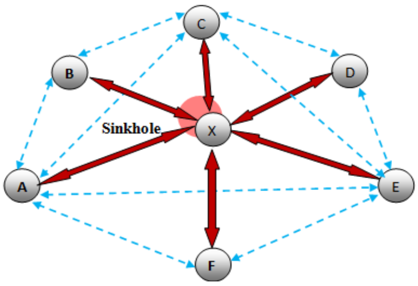
3. Wormhole attack: - In this attack the malicious node receives data packet from source node and will forward it to another node in a network making it as a malicious. This route between two malicious nodes forms a tunnel called wormhole. These are extreme threats to routing protocols.

In the given figure nodes “X” and “Y” are two malicious nodes which forms tunnel. The source node “S” sends RREQ message to node “D” destination node to find path. The neighbour node of “1” and “2” of source node forward it to their respective neighbours “X” and “5”.



When node “X” receives RREQ packet it immediately forward it to “Y” and initializes RREQ later to node “8”. It results in “D” ignores the packet that arrives late and selects the path <S-1-X-Y-8-D>.

4. Sinkhole attack [11]:- In sinkhole attack, malicious node itself broadcast as a fixed node and draws all traffic of the network to itself. It modifies the confidential information after receiving and makes network complicated this attacks are difficult to counter because the node which had supplied the routing information becomes difficult to verify.



5. Replay attack: - this attack keeps the note of control messages of all other nodes and again sends them later. This results in other nodes to record their routing table with stale routes. These replay attacks are later used wrongly to disturb the routing operation in a MANETs.

6. Link withholding and link spoofing attacks: - In link withholding attack, malicious node ignores the requirement to publicize to group of nodes which results in loss to these networks. It results in losing the links between the nodes.

Spoof means to hoax, trick. In link spoofing attack, malicious node impersonates another device in a network in order to launch attacks.

7. Resource consumption attack: - These are typically known as sleep deprivation attack and it occurs mostly in front of devices that does not offer any services to network. It attempts to consume battery life by passing unnecessary data to victims.

8. Sybil attack:- It generates fake identity of nodes. In this the malicioud node itself produces number of fake identities instead of generating a single node. The additional identities that the node requires are called Sybil attack. Various effects due to Sybil nodes are:-

a) Prevents fair resource allocation amongst the nodes in the network.

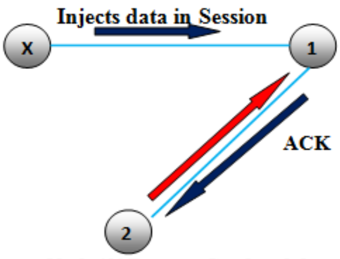
b) It becomes difficult to identify affected node in presence of Sybil node as it generates fake identities.

c) Due to these duplicate identities the outcome may vary.

d) Sybil node appears at various location, hence affecting the normal operation.

D. ATTACKS AT TRANSPORT LAYER

1. Session hijacking: - Session hijacking is also known as address attack which make affect on OLSR protocol. In this attack, the attacker spoofs the victim's IP address and then launches various DoS attacks. In this attack malicious node tries to collect all secret information such as private key, public key, data and all other information from the nodes in network.



Node '2' Become Confused & SEND lost ACK to Resynchronize

In above figure node X injects the data in session to node 1 and then sends acknowledgement to node 2. Node 2 receive the packet and tries to synchronize again with the TCP session with node "1". This process is repeated over and over which leads to ACK storm.

2. SYN flooding: - In this attack the attacker sends SYN request to target system in order to consume enough server resources to make system unresponsive. This attack involves having a client repeatedly sending synchronization packets to every port on the server using fake IP address. When attack begins the server sees multiple attempts to establish communication. The server responds to each attempt with acknowledgement packet from each port. This is one type of DoS attack where attacker creates a large number of half opened TCP connection with victim node. These half opened connection never handshake to fully open the connection.

E. ATTACKS AT APPLICATION LAYER

1. **Malicious code attack: -** This type of attack includes viruses, worms, and Trojan horses, spywares that can attack both user application and operating system.

2. **Repudiation attack: -** This attack can be used to change information of actions executed by malicious users in order to log wrong data to wrong files. Attacker passes this from transport layer to network layer. It denies participation coming from system in order to communicate with network Commercial system is example of this attack. Network and Transport layer are not enough to prevent this attack.

REFERENCES

[1] Pimal Khanpara and BhushanTrivedi, “Security in ad hoc networks”, Proceedings of International Conference on Communication and Networks,Springer, pp. 501-511, 2017.

[2] Dr. SS Tyagi and Aarti, MANET-characteristics, challenges, applications, vol.3.

[3] Abhay Kumar Rai, Rajiv RanjanTewari&Saurabh Kant Upadhyay “Different Types Of Attacks on Integrated MANET-Internet Communiaction” International Journal of Computer Science and Security(IJCSS) Volume(4): Issue (3).

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

[5] Jangra1,A. Goel,N. Priyanka and Bhati,K.-Security aspects in Mobile Ad Hoc Networks (MANETs): A Big Picture, International Journal of Electronics Engineering, pp. 189-196, 2010.

[6] GauravSandhu&MoitreyeeDasgupta, (2010) “Impact of blackhole attack in MANET”, International Journal of Recent Trends in Engineering and Technology, Vol. 3, No. 2.

[7] Hongmei Deng & Wei Li, Dharma P. Agarwal (2002) “Routing security in wireless ad hoc networks”, University of Cincinnati, IEEE Communications magazine, Vol. 40, No. 10.

[8] Ochola EO &Eloff MM, “A review of black hole attack on AODV routing in MANET”.

[9] S. Albert Rabara1 and S.Vijayalakshmi2, “Rushing Attack Mitigation In Multicast MANET (RAM3)”, International Journal of Research and Reviews in Computer Science (IJRRCS), Vol. 1, No. 4, December 2010.

[10] R. Chandra, V. Rama subramanian, and K. Birman, “Anonymous Gossip: Improving Multicast Reliability in Mobile Ad-Hoc Networks,”Proc. 21st Int’l Conf. Distributed Computing Systems (ICDCS ’01), 2001.

[11] Benjamin J. Culpepper and H. Chris Tseng, “Sinkhole Attack Detection in DSR MANETs: A Fuzzy Logic Approach,” Technical Report No.200303, Computational Intelligence Lab., SJSU, 2003.