Security Issues & Challenging Attributes in Mobile Ad-Hoc Networks (MANET)

S.Nithya[1], S.Prema[2], G.Sindhu[3]

[1] Asst.Professor, Department of ECE, KPR Institute of Engineering & Technology, Tamil Nadu, India
[2] Asst.Professor, Department of ECE, KPR Institute of Engineering & Technology, Tamil Nadu, India
[3] Asst.Professor, Department of CSE, Kalaivani College of Technology, Tamil Nadu, India

---***---

Abstract - A Mobile Ad-hoc Network otherwise called as MANET is a collection of wireless nodes that can dynamically be set up anywhere & anytime without having the preexisting network infrastructure. It is an anonymous system in which mobile hosts connected by wireless links are free to move randomly. Here the nodes sometime act as a host & also sometime acts as a router. It plays a major role in Household, industry, Study & Military applications, but the security plays a major role in ad-hoc networks. The attacks may be classified into two types. One is Active & other is Passive Attack. This paper deals with the security issues & the challenges in mobile Ad-hoc Networks.

Key Words: *Mobile ad-hoc Networks, Attacks, Security.*

1. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network. The mobile ad hoc network has the following typical features.

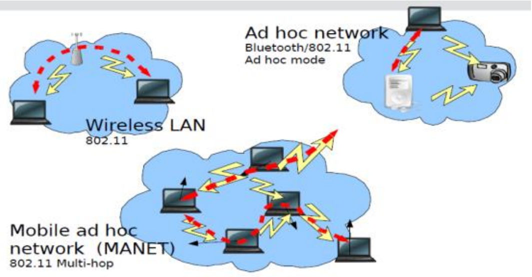

Fig -1: Mobile ad hoc network

In the recent scenario, the Routing protocols in MANET play a vital role. There come major protocols like AODV (Ad hoc *On* Demand Distance Vector protocol), DSR (Dynamic Source Routing protocol), WRP (Wireless Routing Protocol) etc., but none of the routing protocols specifies the security issues. The reality is the MANET is very vulnerable to malicious attacks compared to traditional Wired Networks. In MANET basically two types of attacks will take place. One will be Active Attack & other is Passive attack. In ***passive* attacks**, the attackers typically involve eavesdropping of data, thus disclose the information of the location and move patterns of mobile nodes. This kind of attack is very difficult to detect, because the attacker seldom exhibits abnormal activities. ***Active attacks***, on the other hand, involve actions performed by intruder. The target of the attack can be either data traffic or routing traffic [1].

The MANETS set new challenges for network security and the need of an hour is to pay more attention to the security threats posed on the network [2]. Following are the concerned issues in security of ad hoc networks:

i. In MANET, many nodes are participating in transferring the information's, so that any malicious nodes in the network can easily misuse the message traffic either by dropping the messages or by creating the duplicate or false messages.

ii. Due to the limitation of network resources in mobile ad hoc networks, the various cryptographic solutions applicable to wired networks are not directly applicable. Therefore there is a need for new security solutions which can find their application in this challenging domain.

iii. Dynamically changing network topology results in more opportunities for the malicious nodes to attack.

iv. Since Ad hoc networks are formed for a purpose, the deployment environment may not be very security sensitive. For Example, the nodes deployed in the battlefield or in the forests for tracking wild animals etc. may invite many security threats and attacks.

v. Interoperability is very easy in a wireless medium. Therefore, there is a lack of privacy and the important messages can be eavesdropped and modified easily.

vi. MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad hoc network. Lack of centralized management will impede trust management for nodes [3].

vii. Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to Development of various security schemes and architectures. Collaborative ad hoc environments also allow implementation of self organized security mechanism

viii. Due to mobility of nodes, scale of ad hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones

ix. Routing algorithm for MANETs usually assume that nodes are cooperative and non malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications

x. 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

2. SECURITY ATTACKS

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

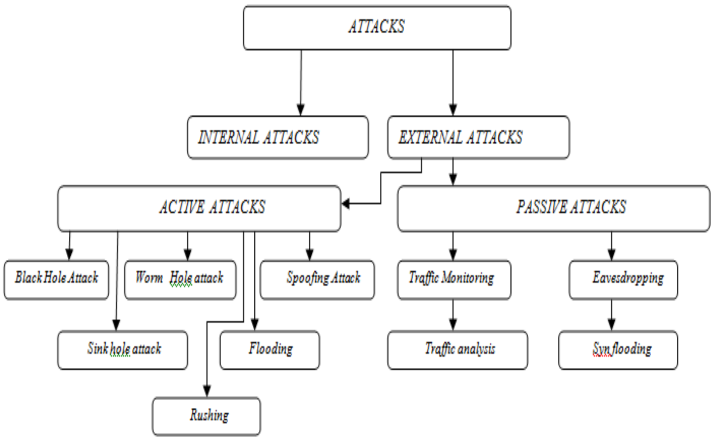

Fig -2: Types of Attacks

Internal Attacks-Attacks may be classified basically as Internal & External Attacks. Internal attacks are sometimes more difficult to handle as compare to external attacks, because internal attacks occurs due more reliable nodes. The inaccurate routing information generated by malicious nodes is difficult to identify. It will attack the nodes in the networks & interface between them.

It wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.

External Attacks- These are the attacks in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services. External Attacks causes' congestion & Denial of services & it Provide wrong routing information .This Prevents the network from normal communication & it produces additional overhead. External Attacks are classified into two types of Attacks namely, Active & Passive Congestion.

Active Attacks-Active Attacks plays a major role in MANET. It causes serious effects over the network. These attacks are very severe attacks on the network that prevent message flow between the nodes. Active attacks can be internal or external. Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks.

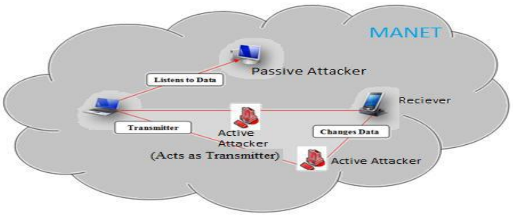

Fig -3: Active & Passive Attacks

Black Hole Attack-In this attack, a malicious node acts drops all data packets passing through it as like matter and energy disappears from our universe in a black hole. If the attacking node is in connection between nodes of two connecting components of that network, then it effectively separates the network in to two disconnected components. Then Black-Hole node separates the network into two parts.

The Fake Node sends fake or wrong routing information, insisting that it has an optimum route and causes other good nodes to route data packets through the fake one. A fake node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.

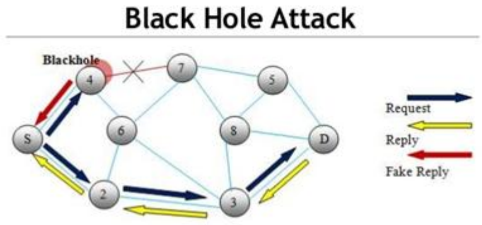

Fig -4: Black Hole Attack

Wormhole Attack-This type of attacks involves in receiving data packets at particular point & invokes them to some other fake node. The Channel or tunnel exist between the two nodes are referred as wormhole attack. These type of attacks are mainly seen in the routing protocols like DSR,AODV etc., If there is no defense mechanism are introduced in the network along with routing protocols, than existing routing protocols are not suitable to discover valid routes.

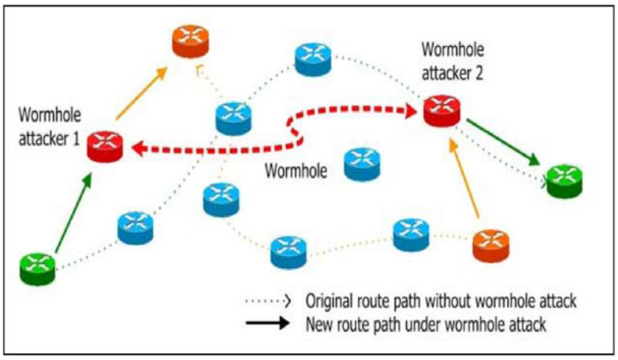
Wormhole attacker 2
Wormhole attacker 1
Wormhole
Original route path without wormhole attack
New route path under wormhole attack

Fig -5: Wormhole Attack

Spoofing Attack-In spoofing attack, the attacker assumes the identity of another node in the network; hence it receives the messages that are meant for that node. Usually, this type of attack is launched in order to gain access to the network so that further attacks can be launched, which could seriously cripple the network.

This type of attack can be launched by any malicious node that has enough information of the network to forge a false ID of one its member nodes and utilizing that ID and a lucrative incentive, the node can misguide other nodes to establish routes towards itself rather than towards the original node.

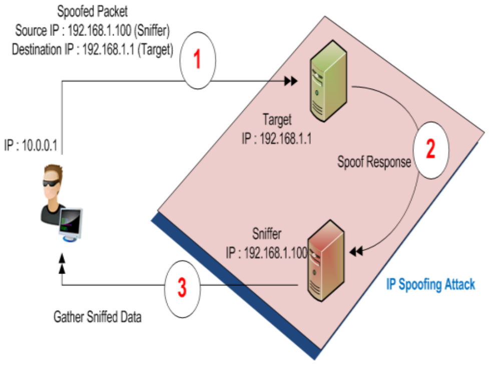

Fig -6: Spoofing Attack

Flooding -It is the basic form of Denial of Service (DoS). This type of attack is to paralyze the whole network by exhausting network resources like bandwidth of the network, battery of nodes. Radio jamming and battery exhaustion methods are the tools to conduct this attack in the network. Attackers may initiate massive bogus route request (RREQ) packets that will definitely be rebroadcast on and on by other nodes. Bogus may be in the sense that the destination address does not exist in the network. As there will not be any reply for these RREQs, network will be flooded leading to the consumption of battery power and bandwidth of all nodes.

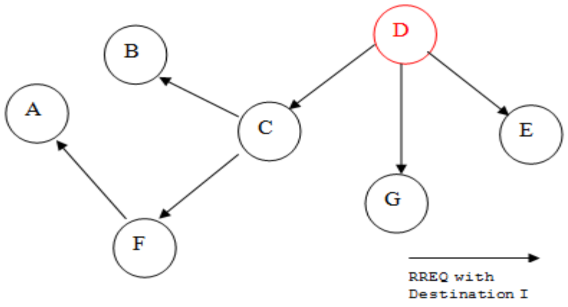

Fig -7: Flooding Attack

Rushing-The term "rushing" suggests that the attacker will speed up to become a hop of the path to a targeted node. This is done by forwarding RREQ quickly than the authorized nodes to increase the probability that routes discovered will be the ones including attacker. It can thus tamper the message traffic passing through it.

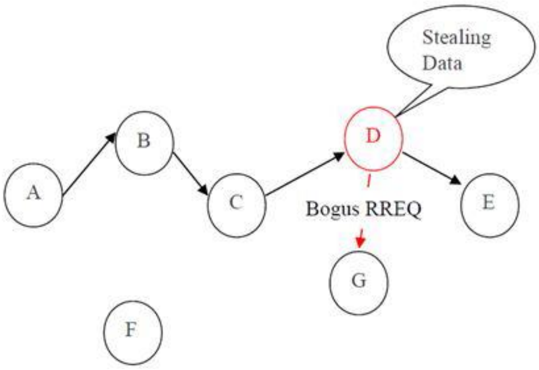

Fig -8: Rushing Attack

Passive Attacks-The passive attackers are to steal the valuable information from the targeted networks. Attackers do not disturb the normal network functioning like inducing false packets or dropping packets. They simply become a part of the network but continuously keep an eye on the network traffic thus in turn violating the message confidentiality constraint.

Since they do not initiate any malicious activity to disrupt the normal functioning of the network, it becomes very difficult to identify such attacks.

Examples of such types of attacks are traffic analysis, traffic monitoring and eavesdropping. Eavesdropping is one kind of passive attack that usually happens in MANET.

Its main aim is to obtain some confidential information that should be kept secret during the communication. The confidential information may include the location, public key, private key or even passwords of the nodes.

Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access.

4. SECURITY THREATS AS PER OSI LAYER

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

Physical Layer

1. Jamming
2. Active Interference

Data Link Layer

1. Selfish Misbehavior
2. Traffic Analysis

Network Layer

1. Black hole attack
2. Wormhole attack
3. Spoofing
4. Sinkhole attack

Transport Layer

1. Flooding Attack
2. Hijacking

Application Layer

1. Malicious node Attack
2. Worms & Virus

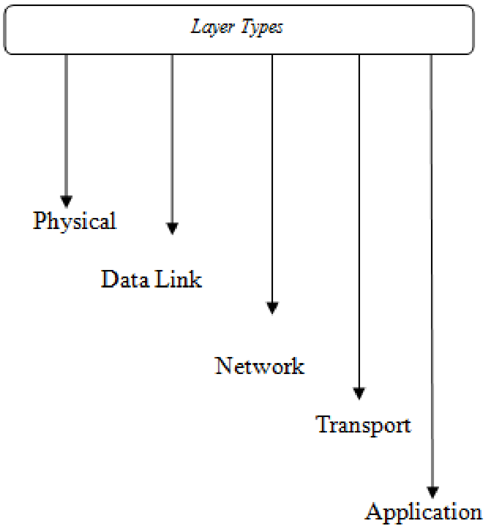

Fig -9: Attacks on OSI Layer

5. SECURITY CHALLENGES

Ad hoc networks are intranets and they remain as intranets unless there is connectivity to the internet. Information sent in ad hoc route can be protected in some way but since multiple nodes are involved, the relaying of packets has to be authenticated by recognizing the originator of the packet and the flow ID or label.

6. CONCLUSION

MANET is used in different types of applications like military, disaster management etc., Hence the reliability, delay & Security becomes main concern in MANET. This paper presents the survey on security issues & Challenging attributes in every wireless networks. Security defenses must be strong enough to avoid adversary to affect the networks.

It is mandatory to handle the data with full confidentiality & with high level of security, but due to its small battery capacity , lack of security & limited memory for processing the information's restrict against the heavy hacking algorithm but it still needs the some efficient algorithms & techniques to secure its data communication over wireless channels.

REFERENCES

1. *Detecting of Black hole Attack in Mobile Ad Hoc Networks, Bo Sun* ***Yong*** *Guan Jian Chen Udo* ***W.*** *Pooch*
2. *Security Threats in MANET,A Review by Shikha jain, International Journal on Information Theory (IJIT), Vol.3, No.2, April 2014*
3. *A Literature Review of Security Attacks in Mobile Ad hoc Networks by Priyanka Goyal,Sahil Batra,Ajit Singh, International Journal of Computer Applications*
4. *A Review on security issues & attacks in wireless sensor netwoks, Lovepreet kumar& jyoteesh malhotra. International Journal of Future Generation Communication and Networking Vol. 8, No. 4 (2015), pp. 81-88*
5. *Detecting of Black hole Attack in Mobile Ad Hoc Networks, Bo Sun* ***Yong*** *Guan Jian Chen Udo* ***W.*** *Pooch*
6. *Security Threats in MANET,A Review by Shikha jain, International Journal on Information Theory (IJIT), Vol.3, No.2, April 2014*
7. *A Literature Review of Security Attacks in Mobile Ad hoc Networks by Priyanka Goyal,Sahil Batra,Ajit Singh, International Journal of Computer Applications*
8. *A Review on security issues & attacks in wireless sensor netwoks, Lovepreet kumar& jyoteesh malhotra. International Journal of Future Generation Communication and Networking Vol. 8, No. 4 (2015), pp. 81-88*
9. *A Review on security attacks in mobile adhoc networks, by Amandeep karuri, Dr.Amardeep singh, International journal of science & research*
10. *Security issues in mobile adhoc networks- A Survey, Wenjia Li and Anupam Joshi*
11. *A Survey of black hole attacks in wireless mobile adhoc networks by Fan-Hsun Tseng, Li-Der Chou1 and Han-Chieh Chao.*
12. *Scurity in wireless sensor networks, issues & challenges, Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong.*
13. *Dai, S, Jing, X, and Li, L, "Research and analysis on routing protocols forwireless sensor networks", Proc. International Conference on Communication*
14. *Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J., "Security for Sensor Networks", CADIP Research Symposium, 2002, available at, http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf*
15. *Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L., "Security in Mobile AdHoc Networks: Challenges and Solutions", IEEE Wireless Communications, Volume 11, Issue 1, February 2004, pp. 38 – 47.*
16. *Security issues in wireless sensor networks: Attacks & Counter measures,*
 Kahina CHELLI