ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology(IJRASET)

Security Threats in MANETS

Ms Mamta Sachdeva[1], Aarti Sharma[2]

[1]Associate Professor in CSE Department, [2]M.Tech Student(CSE)
South Point Institute Of Technology and Management, Sonipat , Haryana ,India

Abstract: Mobile ad hoc networks (MANETs) are one of the fastest growing areas of research. They are an attractive technology for many applications such as rescue and tactical operation. due to the flexibility provided by the dynamic infrastructure. Security in mobile adhoc network is quite challenging as there is no centralized authority which can supervise the individual nodes operating in the network. The attacks can come from both inside and outside the network. Further many security solution used for wired networks are ineffective and inefficient for the highly dynamic and resource constrained environments where Manet use might be expected. So we consider most common types of attacks on mobile ad hoc network and on access point through which MANET is connected to the internet. Specifically we study how different attacks affect the performance of the network.
Keywords: PDA,RREQ,MANET, DOS, IP

I. INTRODUCTION

A mobile ad hoc network is a self configuring network of mobile nodes .It lacks any fixed infrastructure such as access points or base station. It lacks centralized environment and administration and is connected by wireless links or cables. Wireless ad hoc network can be built up where there is no support of wireless access or wired backbone is not feasible.
This is obvious that with the lack of infrastructural support and susceptible wireless link attacks security in adhoc network become inherent weak.Secure communication among nodes require secure communication link to communicate.
Characteristics of Ad hoc networks include:

1)Lack of fixed infrastructure: ad-hoc network is a collection of nodes that do not rely on pre-existing infrastructure for their connectivity. So these types of networks are flexible and easily reconfigurable.

2)Limited resources: lack of infrastructures, these networks have limited resources for their use. Resources like battery power, bandwidth, computation power, memory etc have to be used judiciously for the survival and proper functioning of the network.

3) Dynamic Topology: Nodes in the ad hoc networks are often mobile and wireless devices like laptops, PDAs, smart phones etc resulting in frequent change of their location, resulting in a
dynamic topology.

4) Autonomous Networks i.e. standalone self-organized system: Due to their decentralized nature, these networks eliminate the complexities of infrastructure setup, enabling devices to create and join networks "on the fly" anywhere, anytime, for any application. A node in the networks can communicate with all other nodes which are in its transmission range. Nodes in the network are self sufficient for the purposes like routing application messages, assuring security of the network and so on.

II. SECURITY GOALS

Security in MANET is involving set of investments that are inadequately funded .As all the networking function in a network from data transmission to data reception is performed by node which are highly mobile. So it is quite difficult to identify where network goes wrong or insecure.
If the network is meeting following goals than it is ensured the network is secure. The goals are as follows:

2.1 Availability: Availability means the assets are accessible to authorized parties appropriately Availability applies both to data and to services. It ensures the survivability of network service despite of denial of service attack.

2.2 Confidentiality: Confidentiality ensures that computer-related assets are accessed only by the authorized parties. only those who should have access to something will actually get that access. To maintain confidentiality of some confidential information, we need to keep them secret from all entities that do not have privilege to access them. Confidentiality is sometimes called secrecy or privacy.

2.3 Integrity: Integrity means 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 corrupted.

2.4 Authentication: Authentication enables a node to ensure the identity of peer node it is communicating with. communication are auth- enticated . Authenticity is ensured because only the legitimate sender can produce a message that will decrypt properly with the shared key.

2.5 Non repudiation: Non repudiation ensures that sender and receiver of message cannot disavow that they have ever sent or received such a message. This is helpful when we need to discriminate if a node with some undesired function is compromised or not.

2.6 Anonymity: Anonymity means 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.

2.7 Authorization: This property assigns differ- ent access rights to different types of users. For-
e.g. a network management can be performed by
the network administrator. This right guarantees
that the network operation should be performed by an authorized member.
This right also ensure trust worth of node
.

III. VULNERABILITIES IN MANET

In Manet security system plays a vital role. vulnerable system is a weakness in system security. Before allowing data access the system does not identify the user's identity that is the only reason why system is vulnerable to unauthorized access.

3.1Availability of Resource: It is an issue in mobile ad-hoc network. Providing secure communication as well as protection against various threats is too tedious.

3.2 Scalability: The growth of ad-hoc network changes with time as more and more nodes added to the system the scalability of system varies. Security mechanism should be in such a way that it can handle large as well as small networks.

3.3 Lack of centralized management: There is no central authority and administration. Detection of security attack is almost to impossible. It will impede trust management for nodes. It is not easy to monitor the nodes as environment is too large comprising million of nodes.

3.4 Mutual cooperation among nodes: nodes in network highly cooperate each other so it is difficult to identify malicious node .malicious node can act as a routing agent as a result of this and disrupt the whole communication process as well as disobey protocol specifications.

3.5 Bandwidth constraint: The communication links are variable having low capacity are more susceptible to external interference , disturbance and attenuation as compared to the wireless links.
3.6 Limited power supply: Manet power supply is limited to some extent and nodes can behave in a selfish manner due to this when they find that power supply is limited.

3.7 Adversary in the network: nodes in Manet
is free to join and leave the network. The nodes within the network can behave maliciously and is not identified easily. These nodes are called as compromised nodes.In real terms they are more dangerous than internal nodes.These nodes perform a part of adversary in the network .

3.8 No predefined Boundary: In mobile adhoc networks we cannot precisely define a physical boundary of the network. The nodes work in a nomadic environment where they are allowed to join and leave the wireless network. As soon as an adversary comes in the radio range of a node. It will be able to communicate with that
node. The attacks include Eavesdropping and impersonation.

IV. CATEGORIZING ATTACKS

In ad-hoc network the attacks can be classified in two categories: Active Attacks and Passive attacks. Although there are a number of attacks that affect manet. These attacks can be classified into two types:

4.1 Passive attacks: This type of attack is normally performed by a passive attacker. Attacker does not disturb the normal functioning of the network but tries to steal the valuable information of the network. They also try to generate wrong packets and drop packets. They keep an eye on the network so that they do alterations wherever needed to affect the normal functioning of the network.
Due to their nature the analysis of such type of attack is difficult.eg of this type of attack is Eavesdropping.

4.2 Active Attacks: Active Attacker is responsible for this type of attack to happen. Active attackers interfere with the normal functioning of the network and tamper with the network traffic like cause congestion and propagation of false information. Due to their active participation in causing an attack prevention algorithms are being applied to prevent it as attackers can cause incorrections in routing information.

Attacks on the basis of position of the attacker

4.3 External Attack: This attack is caused by the nodes which do not belong to the network and are from outside the network. These outsider nodes can cause congestion or relay false information and cause unavailability of service.

4.4 Internal Attack: This type of attack is performed by the compromised nodes who belong to the network and gain access to the confidential information of the network and impersonates itself as genuine node.

V. TYPES OF ATTACKS

Layers	Attacks
PHYSICAL	• Jamming • Eavesdropping • Active interference
DATALINK	• Selfish misbehavior of nodes. • Malicious behavior of nodes • DOS • Misdirecting traffic.
NETWORK	• Worm hole attack • Black hole attack • Byzantine attack • Information disclosure • Gray hole attack • Replay attack • Jamming
TRANSPORT	• Session hijacking
APPLICATION	• Impersonation • Man in middle attack

Table1:This table gives an illustration of different types of attacks on different layers

5.1 Jamming: In jamming, attacker initially keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered.

5.2 Eavesdropping: This is a passive attack. The node simply observes the confidential information. This information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper.

5.3 Active Interference: The active nodes create interference in the network by hindering the normal activities of the network.

5.4 Denial of Service attack: This attack aims to attack the availability of a node or the entire network. If the attack is successful the services will not be available. The attacker generally uses radio signal jamming and the battery exhaustion method to cause such type of attack.

5.5 Misdirecting Traffic: Sometimes the traffic misdirects from its original route the reason for this misdirection is the presence of malicious nodes in the MANET environment.

5.6 Wormhole attack: In a wormhole attack, an attacker receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole.

5.7Blackhole attack: In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.

5.8Byzantineattack:Attacks were the adversary has full control of an authenticated device and can perform arbitrary behaviour to disrupt the system are referred to as Byzantine attacks.
Many Byzantine attacks share features with the "selfish" node problem for e.g. not forwarding the data packets to others, but the intentions under these two are different. Goal of the selfish node is to reap the benefits of participating in the ad hoc network without having to expend its own resources in exchange.

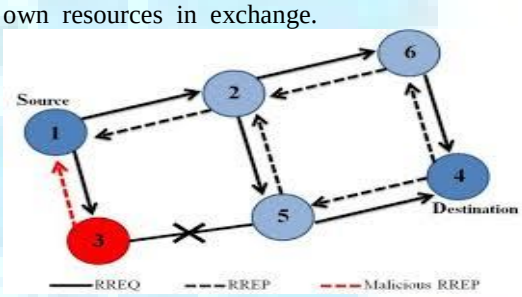

Figure 1: This figure shows the presence of malicious node which cause an obstruction in the smooth flow of information.

5.9 Information Disclosure: This type of attack cause the disclosure of the confidential information present in the network which results in the leakage of private data present in the network.

5.10 Gray hole attack: This attack is also known as routing misbehavior attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.

5.11 Replay Attack: An attacker that performs a replay attack are retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

5.12Session Hijacking: The attacker in a session hijacking scenario exploits the unprotected session following to its initial setup. The attacker forges the IP address of the victim node, computes the sequence number expected by the target, and then launches a DoS attack against the victim. By so doing, the attacker pretends to impersonate the victim node and maintain communicating with the target over the already established.

5.13 Man in middle attack: An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender.

VI. ROUTING ATTACKS IN MANET

Generally there are four different types of MANET routing protocol attacks which is divided in to two main types which are given below
1. Routing disruption attacks
2. Resource consumption attacks
In case of routing disruption attacks, the main task of attacker is to disrupt routing process by routing packets in order to introduce wrong paths. In case of resource consumption attacks are concerned the main task of the attacker is to introduce some non-cooperative or selfish nodes that can be used to inject false packets due to this way load on the network increases and it will become a cause of consuming network bandwidth.
Mainly both of these attacks in MANET routing protocols are the best examples of Denial of Service (DoS) attacks. In Figure 2, there is a broader classification attacks in MANET routing protocols which are given below

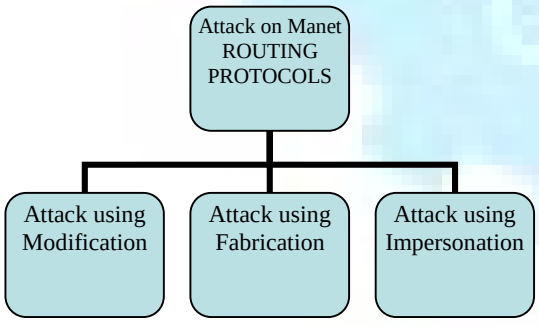

Figure 2:This figure shows the classification of attacks on Manet routing Protocols.

6.1 Attack using Modification
6.1.1Route sequence numbers modification :In this type of attack which frequent in ad-hoc n/w an attacker (i.e. malicious node) used to modify the sequence number in the route request packets.

6.1.2Hop count modification attack :In this type of attacks an attacker mostly change hope count value and due to this way it will become the cause of attract traffic. They are mainly used to include new routes in order to reset the value of hop count field to a lower value of a RREQ packet or sometime even it is used to set to zero.

6.1.3 Source route modification attack :In this type of attack the original route to the destination from the source is being modified by an attacker
By causing alterations in source address.

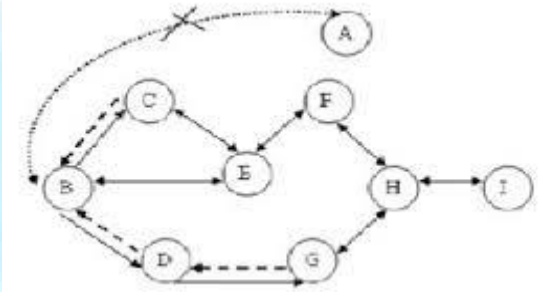

Figure 3:This figure shows how the route from the origin is altered.

6.2 Attack using Fabrication: In this type of attacks, where an attacker as a malicious node try to inject wrong messages or fake routing packets in order to disrupt the routing process. The fabrication attacks are very much difficult to detect in the mobile ad hoc network.

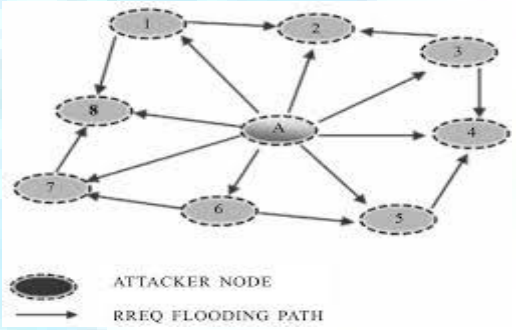

Figure 4:This figure shows flooding of wrong messages in the routing process.
6.3 Attack by Impersonation: :In this type of attacks where attacker is used to violates authenticity and confidentiality of a network. In this attack an attacker (i.e. malicious node) uses to impersonate the address of other user node in order to change the network topology.

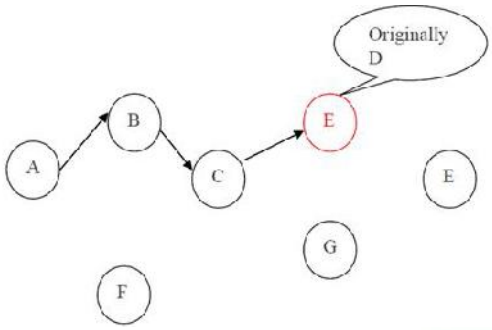

Figure 5:shows an example of impersonation attack.

VII. CONCLUSION

In recent time, mobile ad hoc networks have emerged as a promising technology and gained tremendous attention from researchers. Since these networks can be rapidly deployed without the need of any pre-defined infrastructure, they can be easily applied to various scenarios ranging from emergency operations and disaster relief to military services, vehicular networks, and other sensitive domains. However, their lack of infrastructure and/or central authoritative environment offers plenty of opportunities to malicious nodes for launching a wide array of attacks
some of the methods to attack a network model along with some of the .Various issues that need to be addressed keeping in view the security of MANETS have also been highlighted. The need of the hour is to detect and prevent these attacks in a timely fashion in time.

VIII. FUTURE WORK

The future of ad- hoc networks is really appealing, giving the vision of—anytime, anywhere and cheap communications.
In this review paper, we try to inspect the security issues in the mobile ad hoc networks, which may be a main disturbance to the operation of it. Due to the mobility and open media nature, the mobile ad hoc networks are much more prone to all kind of security risks, such as information disclosure, intrusion, or even denial of service. As a result, the security needs in the mobile ad hoc networks are much higher than those in the traditional wired networks.

REFERENCES

[1] A. Nadeem and M.P. Howarth, “A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks”,IEEE Communications Surveys & Tutorials, 2013.
[2] Gagandeep, Aashima and P. Kumar, “Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review”, International Journal of Engineering and Advanced Technology,2012.
[3] E.M. Shakshuki, N.Kang, and T. R. Shelt.ami,“EAACK-A Secure IDS for MANETs”,IEEE Trans.on Industrial Electronics,2013
[4] Y. Yoo And D. P. Agrawal, “Why Does It Pay To Be Selfish In A Manet”, IEEE Wireless Communications, Dec. 2006.
[5] H. L. Nguyen and U. T. Nguyen,“A study of different types of attacks on multicast in MANET”, Elsevier, AdHoc Networks, 2008.
[6] O. F. Gonzalez, G. Ansa, M. Howarth and G. Pavlou,“Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc networks”, Journal of Int. Engg, 2:1, 2008.
[7] X. Y. Zhang, Y. Sekiya and Y. Wakahara, “Proposal of a Method to Detect Black Hole Attack in MANETs”,Proc. IEEE International Symposium on Autonomous Decentralized System ISADS, 2009.
[8] Monika Arora, Deepak Goyal “Agent Based QoS Routing using DSR in Mobile Ad hoc Networks”, International Journal for Research in Applied Science and Engineering Technology (IJRASET), Volume 2 Issue VII, July 2014, Page No: 183-189
[9] Deepshikha, Dr.Savita Shiwani “A novel adaptive routing algorithm for Wireless adhoc network”, International Journal for Research in Applied Science and Engineering Technology (IJRASET), Volume 2 Issue VII, July 2014, Page No: 279-284