A Study on Various Security Attacks In Mobile Adhoc Network (MANET)

Tajinder Kaur
Dept of Computer Science
Guru Nanak Khalsa Girls College
Baba Sang Dhesian Goraya , Punjab

Abstract- *Security in Mobile Adhoc network (MANET) is a challenging issue as it has no fixed infrastructure in which every node works likes a router that stores and forwards the packet to final destination, limited resources, dynamic topology means MANET is anywhere and anytime. Mobile Ad-hoc Network (MANET) is a mobile wireless network where the groups of mobile devices form a temporary network without any kind or fixed an infrastructure. It is very useful due to its self maintenance, self organizing and by reason of mobility of wireless communication. MANETs vulnerable to various security attacks that are not so common in a wired network due to the feature of decentralization and dynamic configuration of the nodes. This paper, mainly focus on all prominent attacks in MANET's.*

Keywords- Ad-hoc Network, Security attacks in MANET.

I. INTRODUCTION

MANET certainly is the new growing technologies which has been in use since 1980's. There are currently two types of mobile wireless networks, i.e. infrastructure networks and infrastructure less mobile network, which is commonly known as a Mobile ad-hoc network (MANET). In infrastructure networks means the mobile devices communicated with access point like base station, connected to the fixed infrastructure, but in Mobile nodes in MANET are dynamically located and communicated at anywhere & any time without using preexisting network infrastructure[3].

Mobile ad-hoc network is a way of communication, among different portable devices, without offering a centralized device. There is no need of any access point in mobile ad-hoc network. It is the beauty of mobile ad hoc network that mobile nodes communicate with different nodes in the absence of any fixed or central infrastructure, this infrastructure-less property of MANET makes it different and unique among all other networks [1]. The expansion of inexpensive, smaller than average more substantial devices transforms MANET a fast growing network. An Ad-hoc network is self coordinating as well as transformative.

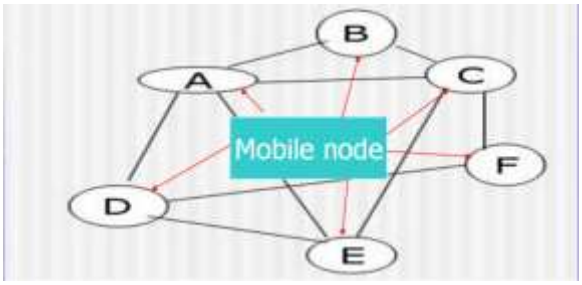

Fig 1: Mobile ad-hoc network architecture

In mobile communication topologies are dynamically created due to the ad hoc nature of the network infrastructure and mobility. MANET architecture shown as in Figure 1. Each mobile node can work either as a host or as a router. There is no necessity of fixed infrastructure and these mobile nodes organize themselves in an arbitrary fashion to form a temporary network with dynamically changing topology. Nodes within each other's wireless transmission ranges can communicate directly, but nodes outside each other's range have to depend on neighboring nodes to relay messages[2]. Nodes of these networks function as routers which discover and maintain routes to other nodes in the network. Applications of Mobile Ad-hoc networks are:

- Disaster recovery environments
- Emergency search and rescue operations where a network connection is urgently required
- Personal area networking(cell phone, laptop, ear phone, wrist watch)
- In military environments (soldiers, tanks, plane)
- Civilian environment(taxi cab network,meeting rooms,sports stadiums,boats, small aircraft)

II. CHARACTERISTICS

There are some characteristics of Mobile ad-hoc network (MANET) which are followed:

- Each node can act as a host and router, which shows its autonomous behavior
- Operating without a central coordinator

- No infrastructure
- Unreliability of wireless links between nodes
- The mobile nodes dynamically establish routing among themselves i.e Dynamic network topology
- Limited energy and computing resources
- Limited Security: Wireless network is more prone to security threats
- Mobile nodes are characterized with less memory, power and light weight features
- Wireless links usually have lower reliability, efficiency, stability and capacity as compared to wired networks
- Adhoc networks require the support of multi-hop communications

III. TYPES OF SECURITY GOALS

There are Six major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. They are mainly:

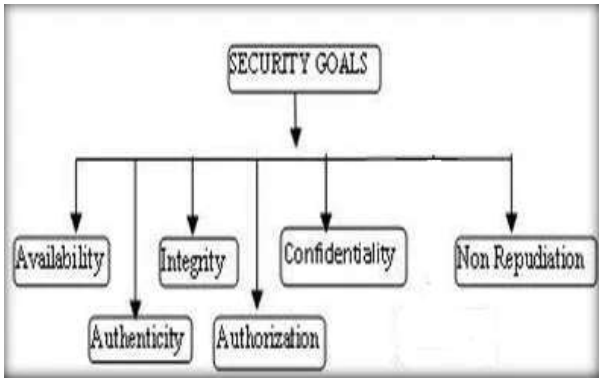

Fig. 2 Security goals

1. **Availability:** The main goal of availability is to node will be available to its users when expected, i.e. survivability of network services despite denial of service attack[4]. For example, on the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channel while on network layer it could disrupt the routing protocol and continuity of services of the network.
2. **Confidentiality:** The goal of confidentiality is to keep information secret from unauthorized user or nodes. The standard approach for keeping information confidential is to encrypt the data with a secret key that only intended receivers posses, hence achieving confidentiality.
3. **Integrity:** The goal of integrity is to guarantee the message being transmitted is never corrupted or altered. Integrity guarantees the identity of the messages when they are transmitted. Ethics guarantees that a information currently being transmitted has never been corrupted[5].
4. **Authentication:** The goal of authentication is too able to identify a node with which it is communicating. In infrastructure-based wireless network, it is possible to implement a central authority at a point such as a base station or access point. But in MANETs, no central administration so it is difficult to authenticate an entity.
5. **Non repudiation:**The main goal of non repudiation is sender of a message cannot deny having sent the message. This is useful when for detection and isolation of compromised nodes.
6. **Authorization:**Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority.

IV. TYPE OF SECURITY ATTACKS ON MANET

Protecting wireless ad-hoc computer networks is a major concern. Security support safe and healthy communication among MANET is prominent for secured transmission of data in an unfriendly environment. There is no Infrastructure among communicating nodes in ad hoc network, instead MANET organizes themselves dynamically which results in the emergence of new challenges for the basic security in applied architecture. Due to this sensitive infrastructure MANET can be directly attacked by digital/cyber assaults compared to wired networks. There is really a wide variety of attacks that influence MANET[6].These types of attacks are generally categorized into two types:

Active Attack: An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network. The attacker can modify, inject, alter or drop data by disturbing the whole network operation. The severity of this assault is high as they can bring down the entire network. They are easy to detect as they degrade the network performance significantly.

Active attacks can be classified further into two categories, i.e. *external* and *internal* attacks.

External attacks: They are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls.

Internal attacks: They are from compromised nodes that are actually part of the network. Since the adversaries are already part of the network as authorized nodes, internal attacks are

more severe and difficult to detect when compared to external attacks.

Dropping assault: The communication between two nodes outside the transmission range depends on intermediate nodes to forward the packets. But formerly these intermediate nodes does not work as expected, i.e. they start to drop the packets during the communication in order to save their limited sources such as bandwidth, energy, etc. Such kinds of nodes are called misbehaving nodes or non cooperative nodes. Due to this, it might also reduce the network performance by causing data packets to be retransmitted and also new routes to the destination to be discovered [10].

Modification attacks: The attacker makes some changes to the routing message. Due to movability of nodes in the network, the malicious node participates in the packet forwarding process and later on launch the message modification attacks. The example of message modification attacks is impersonation attacks and packet mis-routing.

Passive attacks: A passive attack does not disrupt the operation of the network; the adversary snoops the data exchanged in the network without altering it. Here, the requirement of confidentiality can be violated if an adversary is also able to interpret the data gathered through snooping. Detection of passive attacks is very difficult for the operation of the network itself does not get affected. One way of overcoming such problems is to use powerful encryption mechanisms to encrypt the data being transmitted, thereby making it impossible for eavesdroppers to obtain any useful information from the data overheard[7]. The types of passive attacks are eavesdropping and traffic analysis & monitoring:

Eavesdropping: It aims to obtain any confidential information that should be kept secret during the communication[8]. In this the attacker listens all the information that is being transmitted between the two parties in order to find some useful data like passwords, secret codes, confidential information etc.

Traffic analysis and monitoring: In this the attacker keeps track of the traffic flow so that he is able to detect the location of the source, destination, and source-destination pair. Its aim is to engage in a protocol or to provoke transmission between nodes.

V. ATTACKS CORRESPONDING TO DIFFERENT LAYERSIN MANET

Layer	Attacks
Physical layer	Jamming, interceptions, eavesdropping
Data link layer	Traffic analysis, monitoring
Network layer	Wormhole, Black hole, Gray hole, message tempering, Byzantine, Flooding, resource consumption, location disclosure attacks
Transport layer	Session hijacking, SYN Flooding
Application layer	Repudiation, Data corruption
Multiple layer	Denial of Service (DoS), man-in-the-middle attack

Fig. 3 Security attacks in various layers

Denial of Service: In this type of attack, an adversary attempts to prevent legitimate and authorized users of the services offered by the network from accessing those services. A denial of service (DOS) attack can be carried out in many ways. The classic way is to flood packets to any centralized resource (*e.g.*, an access point) used in the network so that the resource is no longer available to nodes in the network, resulting in the network no longer operating in the manner it was designed to operate. This may lead to a failure in the delivery of guaranteed services to the end users. Due to the unique characteristics of adhoc wireless networks, there exist many more ways to launch a DOS attack in such a network, which would not be possible in wired networks. DOS attacks can be launched against any layer in the network protocol stack [12].

On the physical and *MAC* layers, an adversary could employ jamming signals which disrupt the on-going transmissions on the wireless channel. On the network layer, an adversary could take part in the routing process and exploit the routing protocol to disrupt the normal functioning of the network. For example, an adversary node could participate in a session, but simply drop a certain number of packets, which may lead to degradation in the QoS being offered by the network. On the higher layers, an adversary could bring down critical services such as the key management service. Some of the DOS attacks are described below:

Jamming: In this form of attack, the adversary initially keeps monitoring the wireless medium in order to determine the frequency at which the receiver node is receiving signals from the sender. It then transmits signals on that frequency so that error-free reception of the receiver is hindered. Frequency hopping spread spectrum (*FHSS*) and direct sequence spread

spectrum (*DSSS*) (described in detail in the first chapter of this book) are two commonly used techniques that overcome jamming attacks[13].

SYN flooding: Here, an adversary sends a large number of SYN packets to a victim node, spoofing the return addresses of the SYN packets. On receiving the SYN packets, the victim node sends back an acknowledgment (SYN-ACK) packets to nodes whose addresses have been specified in the received SYN packets. However, the victim node would not receive any ACK packet in return. In effect, a half-open connection gets created. The victim node builds up a table/data structure for holding information regarding all pending connections. Since the maximum possible size of the table is limited, the increasing number of half-open connections results in an overflow in the table[15]. Hence, even if a connection request comes from a legitimate node at a later point of time, because of the table overflow, the victim node would be forced to reject the call request.

Distributed DoS attack: A more severe form of the DOS attack is the distributed DOS (DDOS) attack. In this attack, several adversaries that are distributed throughout the network collude and prevent legitimate users from accessing the services offered by the network.

VI. CONCLUSION

MANET is prone to various security attacks which degrades the security and overall performance. In this paper discussed about Mobile Adhoc networks, their security goals, their characteristics, and the issues and various assaults that are posed by Mobile adhoc networks and discussed how the attack has been occurring in the different layer. To conclude, the security is mobile adhoc network is a complex and challenging topic. So improve the security method which protects the MANET from all kinds of security threats.

REFERENCES

[1] Muhammad Kashif Nazir, Rameez U. Rehman, Atif Nazir, A Novel Review on Security and Routing Protocols in MANET,SCIRP,2016.

[2] Saritha Reddy Venna1 , Ramesh Babu Inampudi2, “A Survey on Security Attacks in Mobile Ad Hoc Networks”, IJCSIT Vol. 7 (1) , 2016, 135-140.

[3] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks ,”.

[4] HaoYang, Haiyun & Fan Ye ― Security in mobile adhoc networks : Challenges and solutions,‖, Pg. 38-47, Vol11, issue 1, Feb 2004.

[5] M. Frodigh, P. Johansson, and P. Larsson.―Wireless ad hoc networking: the art of networking without a network,‖ Ericsson Review,No.4, 2000, pp. 248-263.

[6] Pradip M. Jawandhiya, Mangesh M. Ghonge, Dr. M.S.Ali, Prof. J.S. Deshpande, “A Survey of Mobile Ad Hoc Network Attacks ”, International Journal of Engineering Science and Technology, Vol. 2(9), 2010, 4063-4071

[7] Lidong Zhou, Zygmunt J. Haas:,” Securing Ad hoc Networks”,IEEE Network Magzine, 13, 6, Pages 24-30, 1999.

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

[9] Gagandeep, Aashima, Pawan Kumar, Analysis of Different Security Attacks in MANETs on Protocol Stack AReview ,International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[10] Amitabh Misgra and Ketan M. Nadkarni, “Security in Wireless Ad hoc Networks”, in Book The Handbook of Ad hoc Wireless Networks(Chapter 30),CRC Press LLC, 2003.

[11] P. Papadimitratos and Z.J.Haas, “Securing the Routing Infrastructure”, IEEE Communications, vol. 10, no. 40. October 2002, pp. 60-68. [17] Amitabh Misgra and Ketan

[12] R. Chadha and L. Kant. Policy-driven mobile ad hoc network management. Wiley- IEEE Press, 2007.

[13] D. Djenouri, L. Khelladi, and N. Badache. A survey of security issues in mobile ad hoc Networks. IEEE communications surveys, 7 (4), 2005.

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

[15] Hoang Lan and Uyen Trang Nguyen, “Study of Different Types of Attacks on Multicast in Mobile Ad hoc Networks”, Proceedings of ICNICONSMCL’06, 0-7695-2552-0/06@ 2006 IEEE.

[16] Goyal, Priyanka, Vinti Parmar, and Rahul Rishi. "Manet: vulnerabilities, challenges, attacks, application." IJCEM International Journal of Computational Engineering & Management, pp.32-37, 2011

[17] I. Noman and Z. A. Shaikh, “Security Issues in Mobile Ad Hoc Network,” Wireless Networks and Security, Springer Berlin Heidelberg, pp. 49-80, 2013

[18] Imrich Chlamtac a, Marco Conti b, Jennifer J.-N. Liu c, “Mobile ad hoc networking: Imperatives and Challenges”, ELSEVIER, 2003, 13-64