IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 58-63

Network Security and Types of Attacks in Network Security

Ms.M.Aruna[1], Ms.K.Gayathri[2], Dr. M.Inbavalli[3]
[1](III MCA, Perumal Manimekalai College of Engineering, Hosur, Anna University, Tamilnadu)
[2](II MCA, Perumal Manimekalai College of Engineering, Hosur, Anna University, Tamilnadu)
[3](Associate Professor MCA, Perumal Manimekalai College of Engineering, Hosur, Anna University Tamilnadu)

Abstract: *The network technology is developing fast, and the development of internet technology is more quickly, people more aware of the importance of the network and its security. This Network security is main issue of computing because many types of attacks and problems are increasing day to day. In the mobile ad-hoc network the nodes are autonomous. Shielding computer and the network security are the critical issues. The malicious codes create a problem in the network and damages the network. This malicious codes acts as selfishness, It can use the resources of other nodes and preserve the resources of its own. After analyzing the network information and its security elements privacy, integrity and availability, this paper describes the network security privacy vector, network security integrity vector and network security availability vector; also we present the major type of attacks in MANET and the another MANET issues.*
Keywords: *Network, Security, MANET, Integrity, Privacy.*

I. Introduction

The Network security starts with authorization and authentication commonly with a usernames and a password with encrypted key. This Network security consists of the provisions and some policies adopted to a network administrators to prevent and monitor unauthorized access, modifications in system and misuse, or denial of an computer networks and network-accessible resourceses. Basically this network security involves the authorization of access to a data in a network, which is controlled by the network admins. It has become more important to personal computer users, and association. If this approved, a firewall forces to access policies such as what services are allowed to be accessed for network users. So that to prevent illegal access to system, this component may fail to check potentially harmful satisfied such as computer worms or Trojans being transmit over the set of connections. Anti-virus software or an intrusion detection system (IDS) help detect the malware[7]. Today abnormality may also monitor the network like wire shark traffic and may be logged for assessment purposes and for later on high-level analysis in system. Communication between two hosts using a network may be uses encryption to maintain privacy policy.The world is becoming more interconnected of the Internet and new network technology. There is a so large amount of not public, military, business, and government information on networking infrastructures worldwide available. Network security is becoming of great importance because of thinker property that can be easily acquired through the internet.The network security is analyzed by researching the following:

- History of network security
- Internet architecture and security aspects of the Internet
- Types of network attacks and security methods
- Security for internet access in networks
- Current improvement in the network security hardware and software

II. Network Security

System and the Network Technology is a key technology for a wide variety of applications. It is a critical requirement in the current situation networks.

There is a significant lack of security methods that can be easily implemented.There exists a "communication gaps" between the developer of the security technology and developers of each networks. Network design is a developed process that can depend on the Open Systems Interface (OSI) models[1]. The OSI models has several advantages when designing network security. It offers modularity, ease of uses, flexibility, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allows the modular development. In contrast to secure network design is not a well developed proces. There is a methodology to manage the complexity of the security requirements. When considering about the network security, it should be emphasized that the complete network is secured. It does not only concerned with the security in the computers at each end of the communication chains[3]. When transferring from one node to another node the communication channel should be vulnerable to attacker. All the hackers will target the

communication channel, get all the data, and decrypts it and insert a duplicate message. Though securing the network is just as important as the securing computers and encrypting the message. While developing the secure network, the following needs to be considered.

2.1 Confidentiality
It means that the non-authenticated party does not examine all the data.

2.2 Integrity
It is an assurance that the data which is received by the receiver has not been change or adapted after the send by the sender.

III. Types of Threats

Here we are present some basic class of attacks which can be a cause for slow network performance, uncontrolled traffic, viruses etc. Attacks to network from malicious nodes. Attacks can be categories in two:

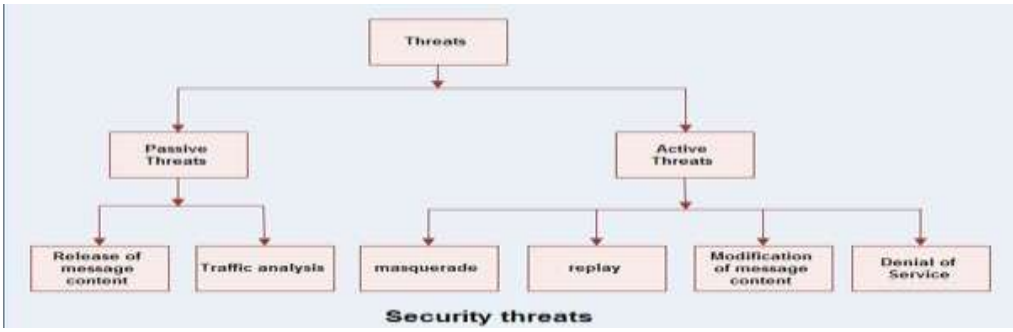

Fig 1 Security Threats

3.1 Active attack
Some active attack are spoofing attack, Wormhole attack, Modification, Denial of services, Sinkhole, and Sybil attack.

a. Spoofing
When a malicious node miss-present his independence, so that the sender change the topology

b. Modification
When malicious node performs some modification in the routing route, so that sender sends the message during the long route. This difficulty cause communication delay occurred between sender and receiver.

c. Wormhole
This attack is also called the tunnelling attack. In this attack an attacker receives a packet at one point and tunnels it to another hateful node in the network. So that a beginner assume that he found the direct path in the network [1].

d. Fabrication
A malicious node generate the false routing message. This means it create the incorrect information about the route between devices [2].

e. Denial of services
In disagreement of services attack, malicious node sending the message to the node and consume the bandwidth of the network. The main aim of the malicious node is to be busy with the network node. If a message from unauthenticated node will come, then receiver will not receive that message because he is demanding and beginner has to wait for the receiver reply.

f. Sinkhole
Sinkhole is a service attack that prevents the base station from obtain complete and correct information. In this attack, a node tries to exert a pull on the data to it from his all bordering node. Selective modification, forwarding or dropping of data can be done by using this assault [1]

g. Sybil

This attack related to the multiple copies of malicious codes. The Sybil attack can be happen due to malicious node share its secret key with other malicious codes. In this way the number of malicious code is increased in the network and the probability of the attack is also increased. If we used the multipath routing, then the possibility of selecting a path malicious code will be increased in the network [1].

3.2 Passive attack

The names of some passive attacks are traffic analysis, eavesdrop, and Monitoring [8].

a. Traffic analysis

In the traffic analyser attack, an attacker tries to sense the communication path between the sender and receiver. An attacker can found the amount of data which is travel from the direct of sender and receiver. There is no adaptation in data by the traffic analysis.

b. Eavesdropping

This is a passive attack, which occur in the mobile ad-hoc networks. The main aim of this attack is to find out some secret or private information from communication. This secrete information may be private or public key of sender or receiver or any hide data.

c. Monitoring

In this attack in which attacker can read the private data, but he cannot edit the data or cannot modify the data.

3.3 Advance attacks

a. Black hole attack

Black hole attack is one of the advance attacking which attacker uses the routing protocol to announce itself as having the best path to the node whose packets it want to cut off. An hacker use the flooding based protocol for listing the request for a route from the originator, then hacker create a reply message he has the shortest path to the receiver . As this message from the hacker reached to the maker before the reply from the actual node, then inventor wills consider that, it is the shortest path to the receivers. So that a hateful false route is create.

Fig 2 Threats in Network

b. Rushing attack

In rushing attack, when sender send packet to the receivers end, then attacker change the packet and forward to receiver. Attacker perform duplicate sends the duplicate to the receivers again and another time. Receiver assumes that packets come from sender so the receiver becomes busy endlessly.

c. Replay attack

It this attack a the malicious code may repeat the data or delayed by the data. This can be done by inventor who intercept the data and retransmits it. At that time, an attacker can intercepts the passwords and encrypt the passwords.

d. Byzantine attack

A set of intermediate code works between the sender and receivers and performs the some changes such as creating routing loops, sending packet through optimal path or selectively dropping the packet, which result in disturbance or degradation of map-reading services.

e. Location disclosure attack

Malicious code collects the informations about the node and about the route by computing and monitoring all the traffices.So malicious code may perform more attacks on the networks.

IV. Different Types of Attacks

If you do not have any security plan in place then your network and the data are vulnerable to any of the following types of attacks because without security controls and measure in place, your data might be subjected to an attacker. Attacks will be passive or active, passive meaning information is monitor and others are active meaning the information is altered with intent to alter or destroy some data or the networks itself.In general we send the data in plain texts that is an unsecured way, which allows an attacker(want to access our information) who has gained access to data paths in your networks to "listen in" or takes (read) the traffices. When an attacker is eavesdropping on your communications, it is referred to as sniffing (Data modification) or intrusive (IP Address snooping).

There are many types of attacks:

- Insider Attack.
- Close in Attack.
- Phishing Attack
- Denial of Service Attack.

4.1 Insider Attack

An insider attack involves someone from the inside, such as an authorize employes, attacking the networks Insider attacks can be malicious or no malicious. An insider attack is a malicious attacker perpetrated on a network or computer system by a person with authorized system access. Insiders that perform attacks (insider's attacks) have a distinct advantages over a external attackers because they have authentications to a system access and also may be familiar with an network architecture and system policies and procedures. In addition, there may be less security against the insiders (that perform attack) because many organizations focuses on protection from external attacks and can't focus on insider attackers.An insider attack is also known as an insider threates.

4.2 Close in Attack

A close-in attack involves someone can attempting to get physically closed to network data, components, and systems inorder to learn more about a network Close-in attacks consists of regular individuals attaining close physical immediacy to networks, systems, or facilities for the purpose of gathering and modifying or denying access to informations. Close physical proximity can be achieved through underhand entry into the network, open access, or both. In other word into Close in attack a attackers are physically closed to the target system and take advantages with physically closed by retrieved the useful information's like password and security code etc.

One popular forms of close in attackes is social engineering in a social engineering attack, the attacker compromises the network or system through a social interaction with person, through an e-mail message or phones. Various tricks can be used by all the individual to revealing the information about the security of company. The information that the victim reveals to the hacker would be most likely be used in a subsequent attacker to gain the unauthorized access to the system or a network.

Fig 3 Session Hijacking

4.3 Phishing Attack

A phishing attack is an popular at the time in this attacks of the hacker whom creates a fake web site (to communicate all the people) that looks exactly like a popular sites such as the SBI bank, Pay TM or PayPal. The phishing part of the attacker is that the hacker then sends an e-mail message trying to trick the user into clicking a link that leads to an fake site[4]. When the user attempts to sign up with their Personal information and account informations, the hacker can records the username/user_id and password and then tries that information on the real site.When you access internet on that time you get some messages its say for clicking on

a particular links and then ask for your email id and password onces you entered your password and id then it is automatically saves your information and then use it on yours behalf.

4.4 Exploit attack

Meaning of exploit is "Using something to ones own advantages", An Exploit is an piece of software that can be used to sequence of some command or chunks of data[9] .In this type of attacks, the attacker can knows of actually security problems within an operating system or an piece of softwares and leverages that knowledge by exploiting the vulnerability in orders to occures on computer hardware and the software or something electronics that is usually computerized. Some things are frequently included into it like gaining control on computer system and allowing privileges escalation and then denial of service related attacks.

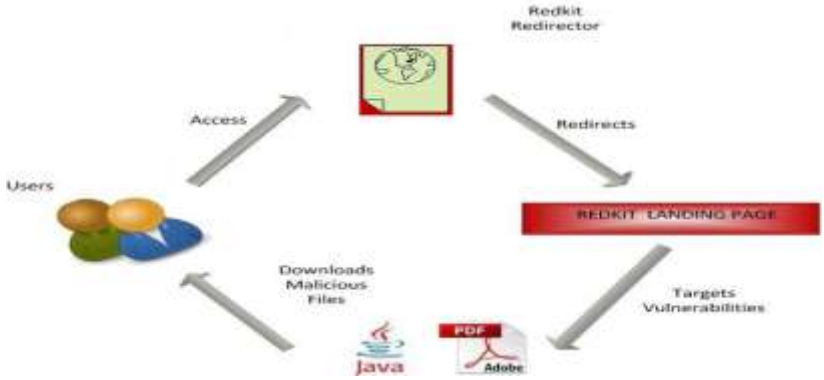

Fig 4 Exploit Attack

4.5 Denial of Service Attack

Denial of service (DOS)attack, it is an type of attack on the network that can be designed to bring the network to its knees by flooding it with useless traffics. In computing networks denial of services attacker is an attempt to make an machine or networks resource whis is unavailable to its intended users, such as to temporarily or indefinitely interrupts or suspends the services of an host connected to the internet connection. DOS Attack can be initiated in many ways:

1)transmission failures
2)trafficredirections
3)DNS attacker
4)Connection floodings.

V. Buffer Overflow

Buffer overflow are same as stackes overflow, an buffer overflow attack accrues when the attacker sends more data to an application that can be is expected. A buffer overflow attacker usually results in the attacker gaining administrative access to the systems in a command prompt or shell.

Fig 5 DDoS Attack

VI. Conclusion

The security is the main problem in the mobile ad-hoc networks. In the MANNET the node looks like selfishness. A node can use the resources of other node and preserve the resources of its own. This type of node creates the problem in MANET there are a number of ways, which guarantees for the safety and security of your networks. Perform the following to avoid security loophole. Must have an updated antivirus program. Don't provide more or unwanted access to any network users. Operating system should be regularly updated.

References

[1]. Neha Khandelwal, Prabhakar.M. Kuldeep Sharma, "An Overview Of security Problems in MANET".
[2]. Anupam Joshi and Wenjia Li. "Security Issues in Mobile Ad Hoc Networks- A Survey".
[3]. Ali Ghaffari, "Vulnerability and Security of Mobile Ad hoc Networks".
[4]. Shobha Arya1 And Chandrakala Arya2, "Malicious Nodes Detection In Mobile Ad Hoc Networks", Journal of Information and Operations Management, ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, 2012, pp-210-212.
[5]. Siddharth Ghansela "Network Security: Attacks, Tools and Techniques" , ijarcsse Volume 3, Issue 6, June 2013.
[6]. Faizal, M.A., Mohd Zaki M., Shahrin Sahib, Robiah, Y., Siti Rahayu, S., and Asrul Hadi, Y. "Time Based Intrusion Detection on Fast Attack for Network Intrusion Detection System", Second International Conference on Network Applications, Protocols and Services, IEEE, 2010.
[7]. Kim J., Lee K., Lee C.," Design and Implementation of Integrated Security Engine for Secure Networking," In Proceedings International Conference on Advnaced Communication Technology,
[8]. "Communication Systems and Network Technologies (CSNT)", 2014 , ISBN:978-1-4799-3069-2,7-9 April 2014.
[9]. "Advanced Research and Technology in Industry Applications" (WARTIA), 2014 IEEE Workshop on in Canada.