Network Security and Types of Attacks in Network

DINESHKUMAR B [1]

PG Scholar, Dept of MCA, DSCE

Bangalore, India

SAMITHA KHAIYUM [2]

Assistant Professor, Dept. of MCA, DSCE

Bangalore, India

---***---

Abstract

The network technology is developing quickly, and the development of web technology is more quickly, individuals a lot of tuned in to the importance of the network security. Network security is that the main problems with computing due to many sorts of attacks are increasing day by day. Within the mobile ad-hoc network the nodes are freelance. The malicious nodes produce a retardant within the network and damages the network. After analyzing and quantifying the network info and its security parts privacy, integrity and availability this paper describes the network security confidentiality vector and network security are availability vector, also we tend to present the main kind of attacks in Manet and also the problems.

Keywords: Network, Security, MANET, Integrity, Privacy.

1 Introduction

Network security starts with authorization usually with a user identification and a password. This Network security is purpose to stop the unauthorized access, modifications in system and misuse or denial of a network and network accessible resources .Basically this network security involves the authorization of access to a data in a very network, that is controlled by the network admins. It's become a lot of vital to private pc users, and association. If this approved, a firewall forces to access policies like what services square measure allowed to be accessed for network users. in order that to stop illegal access to system, this part could fail to ascertain probably harmful glad like pc worms or Trojans being transmit over the set of connections. Anti-virus software or an intrusion find ion system (IDS) facilitate detect the malware. Communication between 2 hosts using a network is also uses encoding to keep up privacy policy. The world is turning into a lot of interconnected to the web and new network technology.

2. Body

I. Network Security

Network security is a key technology for a large kind of applications. It's a critical requirement within the current state of affairs networks. There is critical of security strategies that can be simply enforced. The “communication gaps” between the developer of the protection technology and developers of every networks. Network style may be a developed process depend on the Open Systems Interface (OSI) models. The OSI models has many professionals once designing network security. It offers modularity, easy uses, flexibility, and user friendly of protocols. The protocols of different layers may be simply combined to create stacks that allows the standard development. To secure network design isn't a well-developed process. There isn’t a strategy to manage the quality of security necessities. Once considering about the network security, Network ought to be complete secured. Once transferring from one node to a different node the communicating ought to be at risk of wrongdoer. All the hackers can target the communicating, get all the info, and decode it and insert a replica message. Securing the network is simply as vital because the securing computers and encrypting the message. Whereas developing the secure network, the following must be considered.

1. Confidentiality – It means that unauthenticated party does not read the info.

2. Integrity – it suggests that once data is received by the receiver has not been modification or changed after the send by the sender.

II. Types of Threats (Attacks)

Here we are presenting some basic category of attacks which may be a cause for slow network performance, uncontrolled traffic, viruses etc. Attacks to network from malicious nodes. Attacks may be categories in 2. "Passive" once a network intruder intercepts data traveling through the network, and "Active" during which an normal initiates commands to disrupt the network's traditional operation.

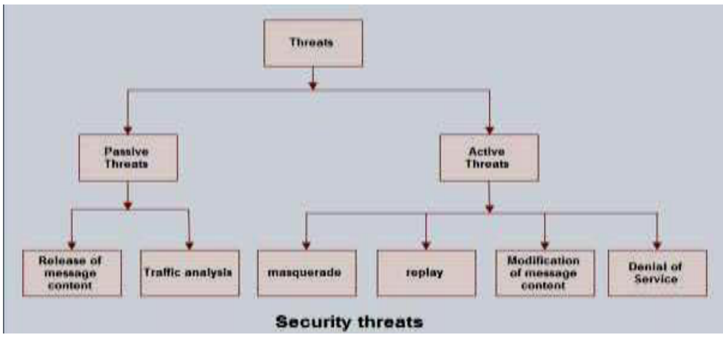

Fig 1 Security Threats

- **Active attack**

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

1. Spoofing

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

2. 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.

3. 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

4. Denial of services

In disagreement of services attack, malicious node causation the message to the node and consume the information measure of the network. the most aim of the malicious node is to be busy with the network node. If a message from unauthenticated node can come back, then receiver won't receive that message as a result of he's exigent and beginner should look ahead to the receiver reply.

5. Sinkhole

Sinkhole may be a service attack that forestalls the bottom station from get complete and proper info. During this attack, a node tries to exert a pull on the information thereto from his all bordering node. Selective modification, forwarding or dropping of knowledge may be done by exploitation this assault.

6. Sybil

This attack associated with the multiple copies of malicious codes. The Sybil attack may be happen because of malicious node share its secret key with alternative malicious codes..

III. Passive attack

The names of some passive attacks area unit traffic analysis, eavesdrop, and watching.

1. Traffic analysis

An attacker tries to sense the communication path between the sender and receiver. Associate in nursing attacker will found the number of data that is travel from the direct of sender and receiver. There's no modification in data by the traffic analysis.

2. Eavesdropping

The main aim of this attack is to seek out out some secret or personal info from communication. This secrete info is also personal or public key of sender or receiver or any hide knowledge.

3. Monitoring

Monitoring during this attack during which attacker will scan the personal knowledge, however he cannot edit the information or cannot modify the information.

IV. Advance attacks

1. Black hole attack

black hole attack Black hole attack is one among the advance offensive that wrongdoer uses the routing protocol to announce itself as having the simplest path to the node whose packets it wish to chop off. Associate in nursing hacker use the flooding primarily based protocol for listing the request for a route from the conceiver, then hacker produce 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 particular node, then discoverer wills contemplate that, it's the shortest path to the receivers. in order that a hateful wrong route is produce.

Fig 2 Threats in network

2. Rushing attack

In rushing attack, once sender send packet to the receivers finish, then wrongdoer amendment the packet and forward to receiver. Attacker perform duplicate sends the duplicate to the receivers once more and once more. Receiver assumes that packets come back from sender that the receiver becomes busy endlessly.

3. Replay attack

It this reply attack the malicious code could repeat the information or delayed by the information. This will be done by inventor UN agency intercept an and retransmits it. At that point, Associate in nursing wrongdoer will intercepts the passwords and inscribe the passwords.

4. Byzantine attack

A set of intermediate code works between the sender and receivers and performs the some changes like making routing loops, causation packet through optimum path or by selection dropping the packet, that lead to disturbance or degradation of map-reading services.

5. Location disclosure attack

Malicious code collects the informations regarding the node and regarding the route by computing and monitoring all the traffics. So malicious code could perform a lot of attacks on the networks.

3. 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.

4. References

[1].Advanced Research and Technology in Industry Applications (WARTIA), 2017 IEEE Workshop on in Canada.

[2] Robiah, Y., Siti Rahayu, "Time Based Intrusion Detection on Fast Attack for Network Intrusion Detection System", Second International Conference on Network Applications, Protocols and Services, IEEE, 2010.

[3].Kartalopoulos, S. V, "Differentiating Data Security and Network Security," Communications, 2008. ICC' 08. IEEE International Conference on, pp.1469-1473, 1923 May 2008.

[4].Dowd, P.W.; McHenry, J.T., "Network security: its time to take it seriously," Computer, vol.31, no.9, pp.2 428, Sep 1998

[5].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.

[6]. Siddharth Ghansela "Network Security: Attacks, June 2013.

[6]. Neha Khandelwal, Prabhakar.M. Kuldeep Sharma, "An Overview Of security Problems in MANET".

[7].Anupam Joshi and Wenjia Li. "Security Issues in Mobile Ad Hoc Networks-A Survey".