Network Security and Types of Attacks in Network

Conference Paper *in* Procedia Computer Science · May 2015

DOI: 10.1016/j.procs.2015.04.126

2 authors:

Mohandas Pawar
VIT University
14 PUBLICATIONS **33** CITATIONS

SEE PROFILE

J. Anuradha
VIT University
37 PUBLICATIONS **211** CITATIONS

SEE PROFILE

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 48 (2015) 503 – 506

Procedia
Computer Science

International Conference on Intelligent Computing, Communication & Convergence

(ICCC-2015)

Conference Organized by Interscience Institute of Management and Technology,

Bhubaneswar, Odisha, India

Network Security and Types of Attacks in Network

Mohan V. Pawar[1], Anuradha J[2]

[1]*Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, Maharashtra, India*
[2]*School of Computing Science and Engineering, VIT University, Vellore, Tamil Nadu, India*
mohanpawar2006@gmail.com[1] , januradha@vit.ac.in[2]

Abstract

The computer network technology is developing rapidly, and the development of internet technology is more quickly, people more aware of the importance of the network security. Network security is main issue of computing because many types of attacks are increasing day by day. In mobile ad-hoc network the nodes are independent. Protecting computer and network security are critical issues. The malicious nodes create a problem in the network. This malicious nodes acts as selfishness, It can use the resources of other nodes and preserve the resources of its own. After analyzing and quantifying the network information security elements confidentiality, integrity and availability, this paper describes the network security confidentiality vector, network security integrity vector and network security availability vector; also we present some major type of attacks in MANET.

Peer-review under responsibility of scientific committee of International Conference on Computer, Communication
and Convergence (ICCC 2015)

Keywords: Network Security, Attacks, IDS,OSI.

Peer-review under responsibility of scientific committee of International Conference on Computer, Communication and Convergence (ICCC 2015)
doi:10.1016/j.procs.2015.04.126

1. Introduction

Network security starts with authorization, commonly with a username and a password. Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, modification in system, misuse, or denial of a computer network and network-accessible resources. Basically network security involves the authorization of access to data in a network, which is controlled by the network admin. It has become more important to personal computer users, and organizations. If this authorized, a firewall forces to access policies such as what services are allowed to be accessed for network users. So that to prevent unauthorized access to system, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion detection system (IDS) help detect the malware. Today anomaly may also monitor the network like wire shark traffic and may be logged for audit 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 networking technology. There is a so large amount of personal, military, commercial, and government information on networking infrastructures worldwide available. Network security is becoming of great importance because of intellectual 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 development in the network security hardware and software

2. Network Security

System and Network Technology is a key technology for a wide variety of applications. It is a critical requirement in current situation networks, there is a significant lack of security methods that can be easily implemented. There exists a “communication gap” between the developers of security technology and developers of networks. Network design is a developed process that is depends on the Open Systems Interface (OSI) model. The OSI model has several advantages when designing network security. It offers modularity, ease-of-use, flexibility, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allow modular development. In contrast to secure network design is not a well- developed process. There isn’t a methodology to manage the complexity of security requirements. When considering about network security, it should be emphasized that the complete network is secure. It does not only concern with the security in the computers at each end of the communication chain. When transferring from one node to another node data the communication channel should not be vulnerable to attack. A hacker will target the communication channel, get the data, and decrypt it and re-insert a duplicate message. Though securing the network is just as important as securing the computers and encrypting the message. While developing a secure network, the following needs to be considered.

2.1 Confidentiality

It means that the non-authenticated party does not examine the data

2.2 Integrity

It is an guarantee that the data which is received by the receiver has not been change or
Modified after the send by the sender.

3. Types of Attacks

Here we are presenting 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:

"Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation.

3.1. Active attack

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

a. *Spoofing*

When a malicious node miss-present his identity, 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 through the long route. This attack 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 malicious node in the network. So that a beginner assumes that he found the shortest path in the network [1].

d. *Fabrication*

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

e. Denial of services

In denial 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 the network node. If a message from unauthenticated node will come, then receiver will not receive that message because he is busy and beginner has to wait for the receiver response.

f. Sinkhole

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

g. Sybil

This attack related to the multiple copies of malicious nodes. The Sybil attack can be happen due to malicious node shares its secret key with other malicious nodes. In this way the number of malicious node is increased in the network and the probability of the attack is also increases. If we used the multipath routing, then the possibility of selecting a path malicious node will be increased in the network [1, 2, and 3].

3.2. Passive attack

The names of some passive attacks are traffic analysis, Eavesdropping, and Monitoring [1, 2, and 3].

a. *Traffic analysis*

In the traffic analysis 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 route of sender and receiver. There is no modification in data by the traffic analysis.

b. *Eavesdropping*

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

c. *Monitoring*

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

3.3Advance attacks

a. Black hole attack

Black hole attack is one of the advance attacking which attacker uses the routing protocol to advertise itself as having the best path to the node whose packets it want to intercept. An hacker use the flooding based protocol for listing the request for a route from the initiator, then hacker create a reply message he has the shortest path to the receiver . As this message from the hacker reached to the initiator before the reply from the actual node, then initiator wills consider that, it is the shortest path to the receiver. So that a malicious fake route is create.

b. Rushing attack

In rushing attack, when sender send packet to the receiver, then attacker alter the packet and forward to receiver. Attacker performs duplicate sends the duplicate to the receiver again and again. Receiver assumes that packets come from sender so the receiver becomes busy continuously.

c. Replay attack

It this attack a malicious node may repeat the data or delayed the data. This can be done by originator who intercept the data and retransmit it. At that time, an attacker an intercept the password.

d. Byzantine attack

A set of intermediate node works between the sender and receiver and perform some changes such as creating routing loops, sending packet through non optimal path or selectively dropping packet, which result in disruption or degradation of routing services.

e. Location disclosure attack

Malicious node collects the information about the node and about the route by computing and monitoring the traffic. So malicious node may perform more attack on the network.

4. Conclusion

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

5. 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.