Ministry of higher education
and scientific research
University of Diyala
College of science
Department of computer science

Network Security

Research submitted to Diyala University / College of Science / Department of Computer Science
As one of the requirements for obtaining a Bachelor's degree in Computer Science

By :
Alwaleed Khalid shalaan
Akram Ahmed Nassif

Supervised by

Dr. Muntadher Khamees

2019-2020 **1440-1441**

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة ديالى/كلية العلوم
قسم علوم الحاسوب

حماية الشبكات

بحث مقدم الى جامعة ديالى/كلية العلوم/قسم علوم الحاسوب

كأحدى متطلبات لنيل شهادة البكالوريوس في اختصاص علوم الحاسوب

أعداد

الوليد خالد شعلان

اكرم احمد

بأشراف

اسم المشرف

د. منتظر خميس

٢٠٢٠

بسم الله الرحمن الرحيم

{ وقل ربي زدني علما } طه (١١٤)

{ وما اوتيتم من العلم الا قليلا } الاسراء (٨٥)

وقل اعملوا فسيرى الله عملكم ورسوله و }
{ المؤمنون
التوبة (١٠٥)

الأهداء

الى رمز الحب والحنان والوفاء والتضحية...

والقلب الناصع بالبياض (والدتي العزيزة)....

والى من فنا عمره .... والقلب الكبير

وصاحب البسمة الدائمة الذي ضحى كثيرا

ولازال يضحي من اجلنا (الوالد العزيز).....

والى الاساتذة والمعلمين الذين مهدو لنا

الطريق دائما وزرعوا اجمل الذكريات فينا

والى كل من له دور في حياتنا شكرا جزيلا

وعسى الله ان يوفقنا جميعا.....

الشكر والتقدير

بسم الله الرحمن الرحيم، الحمد لله الذى علم
الإنسان ما لم يعلم، والصلاة والسلام على من
بعثه الله للمسلمين، وخاتم النبيين وسيد ولد
آدم، في البداية اتقدم بالشكر الى الاساتذة
والمعلمين الذين مهدو لنا الطريق وتقدير شكر
خاص لأستاذ (منتظر خميس)الذي يسر لي
وساهم في هذا البحث ونسال الله ان يوفقنا
لخدمت عراقنا الحبيب وخدمة الوطن .
أما بعد فإن ما نتناوله
اليوم بين أيدينا هو بحث علمي في
مجال(الشبكات)تخصص“الحماية”
ولهذا البحث أهمية كبيرة للفرد والمجتمع،
ونظرا لأهميته فسوف نعرض لكم أهم النقاط
المتعلقة به وأهم الدراسات التي تمت عليه
والنتائج التي تم الحصول عليها.

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.

الخلاصة :

تتطور تكنولوجيا شبكة الكمبيوتر بشكل سريع ، كما أن تطوير تكنولوجيا الإنترنت أسرع ، ويدرك الناس أهمية أمان الشبكة .أمن الشبكات هو القضية الرئيسية للحوسبة لأن العديد من أنواع الهجمات تتزايد يومًا بعد يوم .في شبكة الأقران المتنقلة ، تكون العقد مستقلة .حماية الكمبيوتر وأمن الشبكات هي قضايا حرجة . العقد الخبيثة تخلق مشكلة في الشبكة .تعمل هذه العقد الخبيثة كأنانية ، يمكنها استخدام موارد العقد الأخرى والحفاظ على الموارد الخاصة بها .بعد تحليل وقياس سرية عناصر أمن معلومات الشبكة وسلامتها وتوافرها ، تصف هذه الورقة ناقل سرية أمان الشبكة ، ومتجه تكامل أمان الشبكة ، ومتجه توفر أمان الشبكة ؛ كما نقدم بعض أنواع الهجمات الرئيسية.

Context

Chapter 1 (network type and some important concept)

Chapter 2 (Network security)

Chapter 2 (Type Of Network Attack And Some Concepts)

Chapter 4

Table of figures

Chapter One

(network type and some important concept)

1- Introduction

Many periods in the history of mankind have been named after significant technological discoveries that occurred within them or after the dominant technology of the time. The stone age, the bronze age and the iron age constitute early examples of such periods that were named after the dominant material for building tools and the respective technology. More recently, one may distinguish the steam age, the electricity age and the silicon age. Our times might, in the future, be named the "information age". If this happens, the name will be due to the realization of the Information Society, that affects all human activities and influences the way in which we live, work, entertain ourselves, engage in entrepreneurial activities, perform transactions, care for our health, communicate with each other etc. In this environment, networks have permeated almost all aspects of our everyday life, changing it, improving it and making it easier, while at the same time increasing its dependence upon Information and Communication Technologies (ICT). This is the main reason why the security of networks is the most frequently cited reason that influences the further expansion of e-services. Indeed, the more our society depends upon ICT, the more significance will be attributed to securing these technologies. In this scene, where almost all organizations base their operation on processing information, new dependencies, new vulnerabilities and new risks appear.

2- Types and benefits

Forms of networks The forms of computer networks differ in terms of the engineering arrangement in which they are installed, including:

1. Ring Topology.
2. Hybrid Topology.
3. Mesh Topology.
4. Of the Star Topology network.
5. Tree Topology.
6. Bus Topology

Benefits of networks There are many benefits of networks, including the following:
1. Reduce the cost of resources; When computers are connected through the network, they can share various resources such as printers, operating systems, software, and others.
2. Increase the storage space; Where data is stored in a huge shared space, such as a central server.
3. The flexibility to access data anywhere, and through any device connected to the network.

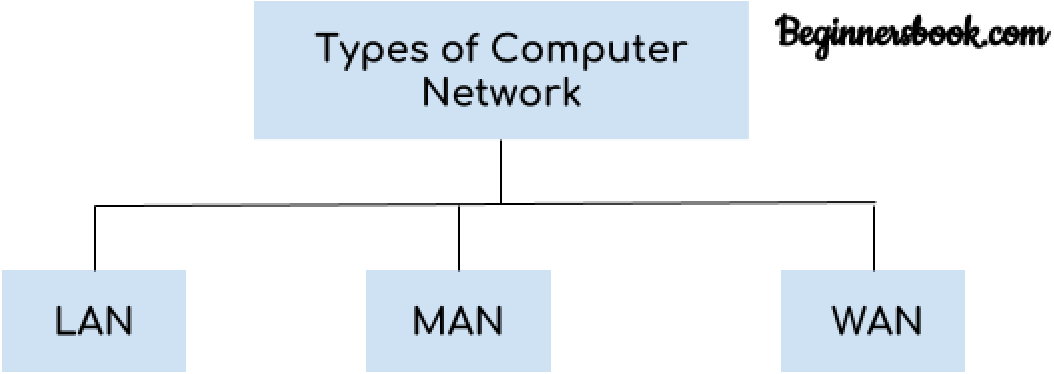
4. Simplifying the communication process; You can send and receive messages and files easily, simply by connecting to the network.

3- Types of Computer Network: LAN, MAN and WAN

By Chaitanya Singh | Filed Under: Computer Network

A computer network is a group of computers connected with each other through a transmission medium such as cable, wire etc. In this guide, we will discuss the types of computer networks in detail.

Types of Computer Network

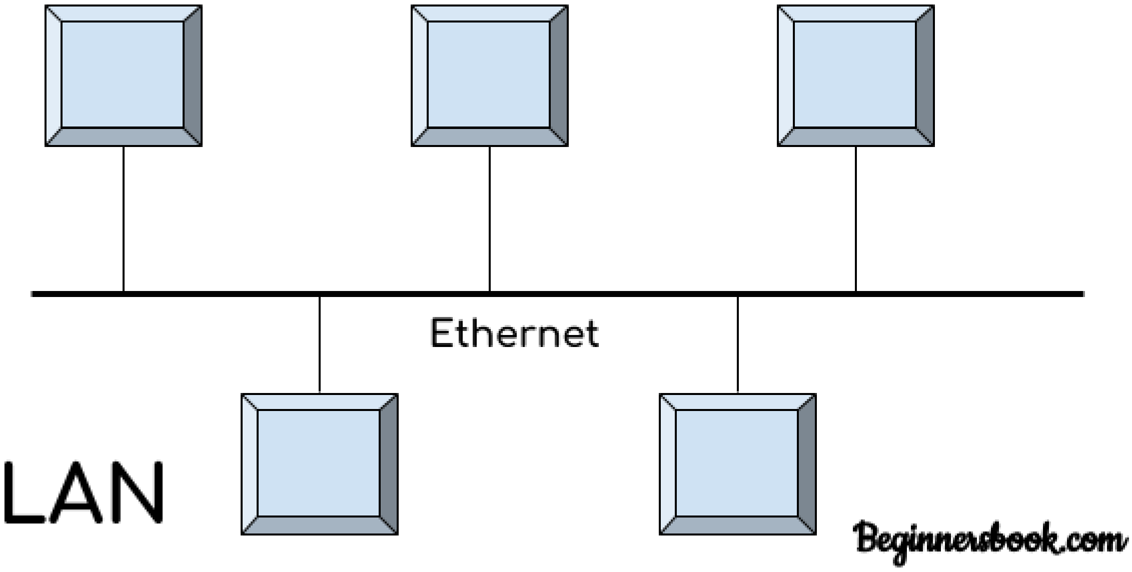


1.1 fig 1 (type of network)

There are mainly three types of computer networks based on their size:

1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide area network (WAN)

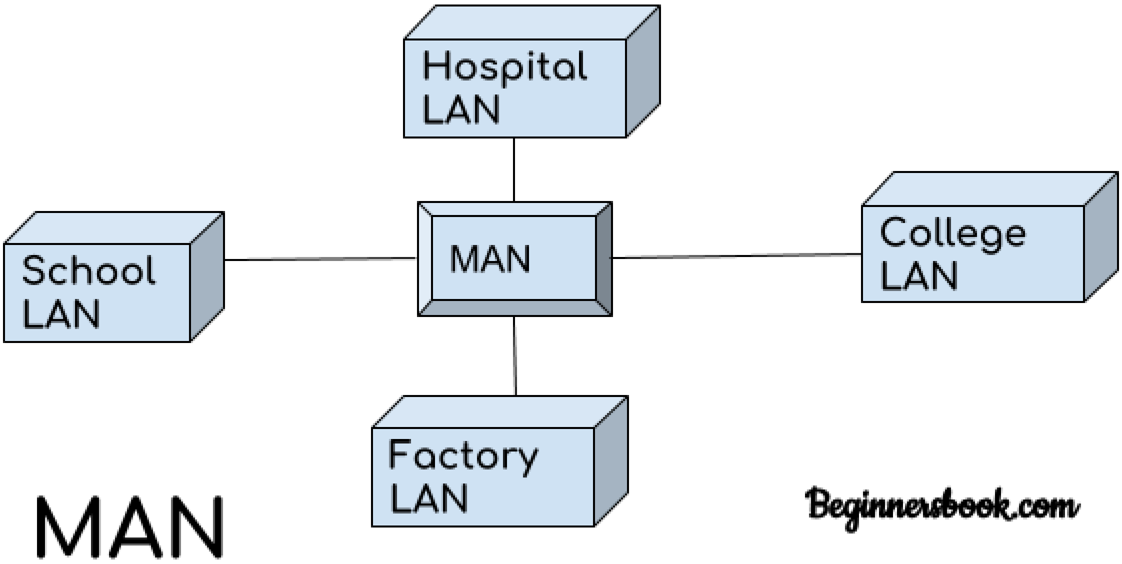
1. Local Area Network (LAN)



1.2 fig 2(LAN network)

1. **Local area network** is a group of computers connected with each other in a small places such as school, hospital, apartment etc.
   2. LAN is secure because there is no outside connection with the local area network thus the data which is shared is safe on the local area network and can't be accessed outside.
   3. LAN due to their small size are considerably faster, their speed can range anywhere from 100 to 100Mbps.
   4. LANs are not limited to wire connection, there is a new evolution to the LANs that allows local area network to work on a wireless connection.

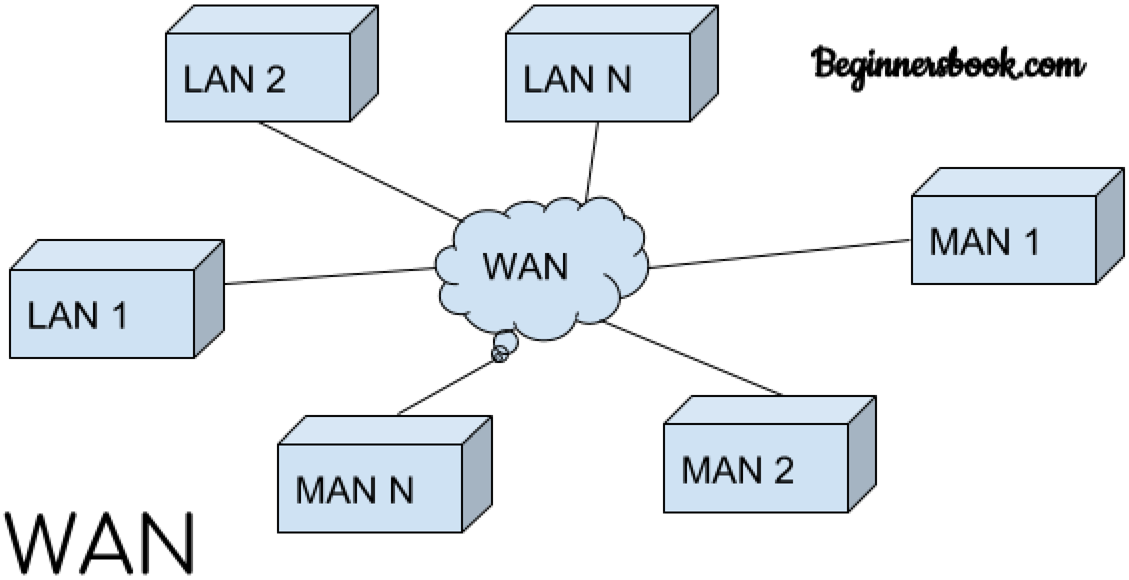
2. Metropolitan Area Network (MAN)



1.3 fig 3(MAN network)

MAN network covers larger area by connections LANs to a larger network of computers. In Metropolitan area network various Local area networks are connected with each other through telephone lines. The size of the Metropolitan area network is larger than LANs and smaller than WANs(wide area networks), a MANs covers the larger area of a city or town.

3. Wide area network (WAN)



1.4 fig 4(WAN network)

Wide area network provides long distance transmission of data. The size of the WAN is larger than LAN and MAN. A WAN can cover country, continent or even a whole world. Internet connection is an example of WAN. Other examples of WAN are mobile broadband connections such as 3G, 4G etc.

Advantages of WAN:

Centralized infrastructure: One of the main advantage of WAN is the that we do not need to maintain the backup and store data on local system as everything is stored online on a data centre, from where we can access the data through WAN.

Privacy: We can setup the WAN in such a way that it encrypts the data that we share online that way the data is secure and minimises the risk of unauthorized access.

Increased Bandwidth: With the WAN we get to choose the bandwidth based on the need, a large organization can have larger bandwidth that can carry large amount of data faster and efficiently.

Area: A WAN can cover a large area or even a whole world though internet connection thus we can connect with the person in another country through WAN which is not possible is other type of computer networks.

Disadvantages of WAN:

Antivirus: Since our systems are connected with the large amount of systems, there is possibility that we may unknowingly download the virus that can affect our system and become threat to our privacy and may lead to data loss.

Expensive: Cost of installation is very high.

Issue resolution: Issue resolution takes time as the WAN covers large area, it is really difficult to pin point the exact location where the issues raised and causing the problem.

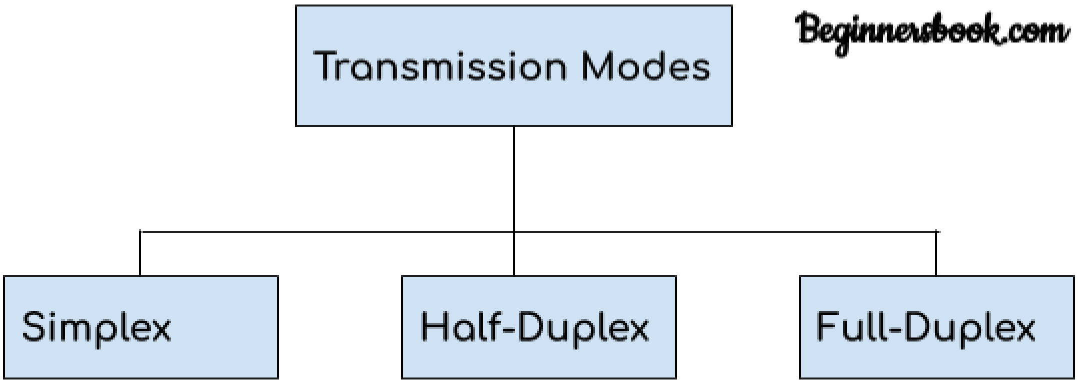
Interconnection of Networks:
We have read LAN, MAN and WAN above, we also talked about internet. You can say that an internet is a combination of LAN, MAN and WAN.

4- Computer Network Transmission Modes

By Chaitanya Singh | Filed Under: Computer Network

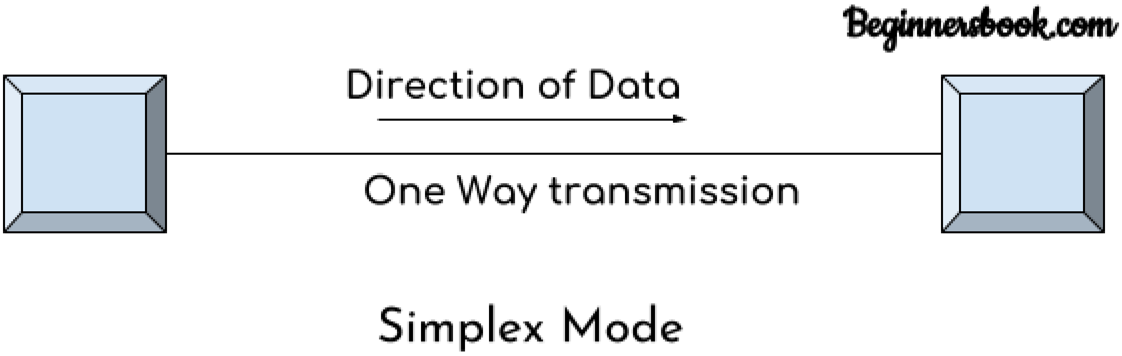
The data is transmitted from one device to another device through a **transmission mode**. The transmission mode decides the direction of data in which the data needs to travel to reach the receiver system or node. The transmission mode is divided in **three** categories:

1. Simplex
2. Half-Duplex
3. Full-Duplex



1.5 Fig 5 (Transmission mode)

4-1 Simplex Mode



1.6 fig 6 (Simplex mode)

1. In simplex mode the data transmits in one direction only, from one system to another system.
2. The sender device that sends data can only send data and cannot receive it. On the other hand the receiver device can only receive the data and cannot send it.
3. Television is an example of simplex mode transmission as the broadcast sends

signals to our TV but never receives signals back from our TV. This is a unidirectional transmission.

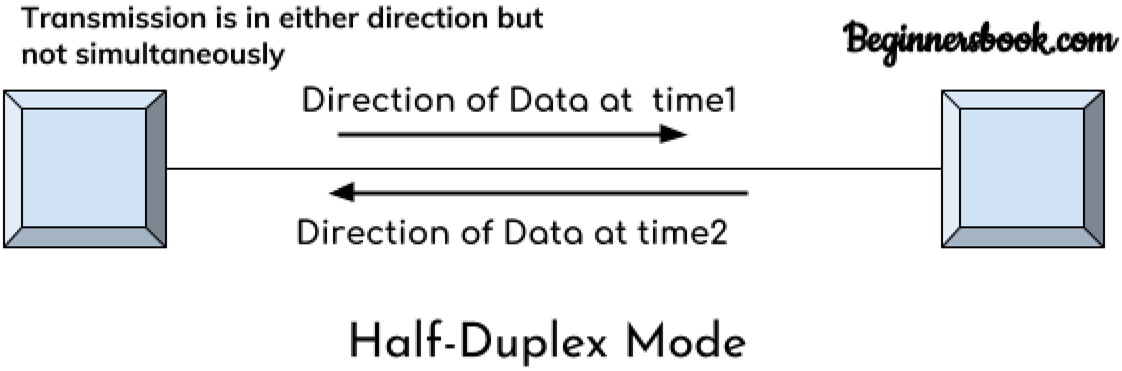
4.1.1 - Advantages of Simplex Mode:

The full capacity of the transmission medium is utilised as the transmission is one way and cannot have traffic issues.

4.1.2 - Disadvantages of Simplex Mode:

No bidirectional communication is possible. Two devices cannot communicate with each other using simplex mode of transmission.

4.2- Half-Duplex Mode


Transmission is in either direction but not simultaneously
Beginnersbook.com
Direction of Data at time1
Direction of Data at time2
Half-Duplex Mode

1.7 fig 7 (Half-Duplex mode)

1. In half duplex mode transmission can be done both ways which means if two systems are connected with half-duplex mode of transmission, they both can send and receive data but not at the same time.
2. If one device is sending data then other device cannot send data until it receives the data which is already in transmission. You can say that the communication is not simultaneous.
3. The radio communication device that our soldiers use at the battle fields are the examples of half duplex mode transmission as they send message and then say over and then the person on other hand send his message and this way they communicate but not simultaneously like we used to do on mobile.

4.2.1- Advantages of Half-Duplex mode:

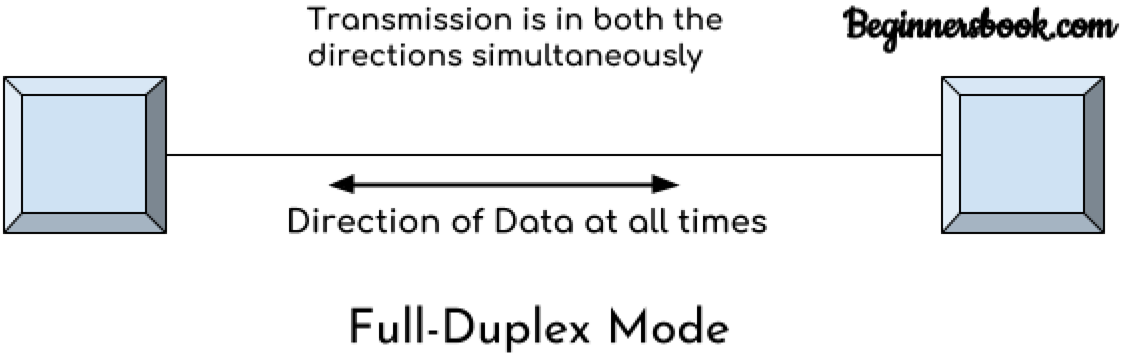
Both devices can send and receive data.

Whole bandwidth can be utilised as at a time only one signal transmits.

4.2.1- Disadvantages of Half-Duplex mode:

The disadvantage in half duplex mode is that the other device cannot send data until it receives the data which is already in transmission, this can cause delays to the communication.

4.3- Full Duplex Mode:


Transmission is in both the directions simultaneously
Beginnersbook.com
Direction of Data at all times
Full-Duplex Mode

1.8 fig 8 (Full-Duplex mode)

1. In full duplex mode both the connected devices can send and receive data simultaneously. The mobile phone we use is an example of full duplex mode where we can communicate simultaneously.
2. Both the devices can send and receive the data at the same time.

4.3.1- Advantages of Full Duplex mode:

No delays in communication as both can send and receive data simultaneously.

4.3.2- Disadvantages of Full Duplex mode:

No proper bandwidth utilization as the same line is used for sending and receiving data at the same time.

5- Computer Network Models

(By Chaitanya Singh | Filed Under: Computer Network)

A computer network consists software and hardware that is used to send and receive data from one device to another. The role of hardware is to prove the physical equipment that are required in order to send and receive data while software defines the set of instructions that uses the hardware equipments for data transmission. A simple transmission of data consists several steps at various layers of computer network. In computer network models we will discuss the models in detail to understand how the data is actually transferred and received at a computer level.

Before we discuss the computer network models, lets have a discussion on the layers that a computer model consists. Lets have a basic idea of layers involved in data communication.

5.1- Layers of a computer network models

1. The main purpose of having several layers in a computer network model is to divide a process of sending and receiving data into small small tasks.
2. These layers are connected with each other, each layer provide certain data to its immediate higher and immediate lower layer and receives certain data from the same.
3. Dividing a model is layers makes the structure quite simple that makes it easy to identify the issue if it occurs. There are three main components of a computer network model. Sender, receiver and carrier.

At sender Side:

Higher layer: Higher layer serves the middle layer, directs the message (or data) to middle layer
Middle layer: Middle layer picks up the data from higher layer and transfer it to the lower layer
lower layer: The data is transmitted to the lower layer of the receiver side.

At receiver Side:

lower layer: Receives the data from the lower layer of sender side and transfer it to middle layer.
Middle layer: Middle layer picks up the data from lower layer and transfer to higher layer.
Higher layer: Higher layer transfers the data to the receiver.
4. We will discuss more than one computer models here, each model has different set and design of layers.
The most important computer network models are:
1. OSI Model
2. TCP/IP Model

Chapter Two

(Network security And Network Type)

1.1 Introduction

Definition of networks Networks are defined as a group of devices that communicate with each other through physical or wireless communication media, allowing computers and individuals to share information, through chat rooms, e-mail, or sharing data and information using shared storage devices, Or printers, as well as sharing programs by running applications on remote computers, and the size of networks varies; It may consist of two computers connected to peripheral devices, or large data centers (in English: Data centers) may be connected to each other, and it may also be a group of networks connected to each other such as the Internet located around the world.

1.2 Network security basics

Definitions are fine as top-level statements of intent. But how do you lay out a plan for implementing that vision? Stephen Northcutt wrote a primer on the basics of network security for CSOonline over a decade ago, but we feel strongly that his vision of the three phases of network security is still relevant and should be the underlying framework for your strategy. In his telling, network security consists of:

- **Protection**: You should configure your systems and networks as correctly as possible
- **Detection**: You must be able to identify when the configuration has changed or when some network traffic indicates a problem
- **Reaction:** After identifying problems quickly, you must respond to them and return to a safe state as rapidly as possible

This, in short, is a *defense in depth* strategy. If there's one common theme among security experts, it's that relying on one single line of defense is dangerous, because any single defensive tool can be defeated by a determined adversary. Your network isn't a line or a point: it's a territory, and even if an attacker has invaded part of it, you still have the resources to regroup and expel them, if you've organized your defense properly.

1.3 Network security methods

To implement this kind of defense in depth, there are a variety of specialized techniques and types of network security you will want to roll out. Cisco, a networking infrastructure company, uses the following schema to break down the different types of network security, and while some of it is informed by their product categories, it's a useful way to think about the different ways to secure a network.

1.3.1 Access control:
You should be able to block unauthorized users and devices from accessing your network. Users that are permitted network access should only be able to work with the limited set of resources for which they've been authorized.

1.3.2 Anti-malware:
Viruses, worms, and trojans by definition attempt to spread across a network, and can lurk dormant on infected machines for days or weeks. Your security effort should do its best to prevent initial infection and also root out malware that does make its way onto your network.

1.3.3 Application security:
Insecure applications are often the vectors by which attackers get access to your network. You need to employ hardware, software, and security processes to lock those apps down.

1.3.4 Behavioral analytics:
You should know what normal network behavior looks like so that you can spot anomalies or breaches as they happen.

1.3.5 Data loss prevention:
Human beings are inevitably the weakest security link. You need to implement technologies and processes to ensure that staffers don't deliberately or inadvertently send sensitive data outside the network.

1.3.6 Email security:
Phishing is one of the most common ways attackers gain access to a network. Email security tools can block both incoming attacks and outbound messages with sensitive data.

1.3.7 Firewalls:
Perhaps the granddaddy of the network security world, they follow the rules you define to permit or deny traffic at the border between your network and the internet, establishing a barrier between your trusted zone and the wild west outside. They don't preclude the need for a defense-in-depth strategy, but they're still a must-have.

1.3.8 Intrusion detection and prevention:
These systems scan network traffic to identify and block attacks, often by correlating network activity signatures with databases of known attack techniques.

1.3.9 Mobile device and wireless security: Wireless devices have all the potential security flaws of any other networked gadget — but also can connect to just about any wireless network anywhere, requiring extra scrutiny.

1.3.10 Network segmentation: Software-defined segmentation puts network traffic into different classifications and makes enforcing security policies easier.

1.3.11 Security information and event management (SIEM): These products aim to automatically pull together information from a variety of network tools to provide data you need to identify and respond to threats.

1.3.12 VPN: A tool (typically based on IPsec or SSL) that authenticates the communication between a device and a secure network, creating a secure, encrypted "tunnel" across the open internet.

1.3.13 Web security: You need to be able to control internal staff's web use in order to block web-based threats from using browsers as a vector to infect your network.

1.4 Network security software

To cover all those bases, you'll need a variety of software and hardware tools in your toolkit. Most venerable, as we've noted, is the firewall. The drumbeat has been to say that the days when a firewall was the sum total of your network security is long gone, with defense in depth needed to fight threats behind (and even in front of) the firewall. Indeed, it seems that one of the nicest things you can say about a firewall product in a review is that calling it a firewall is selling it short.

But firewalls can't be jettisoned entirely. They're properly one element in your hybrid defense-in-depth strategy. And as eSecurity Planet explains, there are a number of different firewall types, many of which map onto the different types of network security we covered earlier:

- Network firewalls
- Next-generation firewalls
- Web application firewalls

- Database firewalls
- Unified threat management
- Cloud firewalls
- Container firewalls
- Network segmentation firewalls

Beyond the firewall, a network security pro will deploy a number of tools to keep track of what's happening on their networks. Some of these tools are corporate products from big vendors, while others come in the form of free, open source utilities that sysadmins have been using since the early days of Unix. A great resource is SecTools.org, which maintains a charmingly Web 1.0 website that keeps constant track of the most popular network security tools, as voted on by users. Top categories include:

- Packet sniffers, which give deep insight into data traffic
- Vulnerability scanners like Nessus
- Intrusion detection and prevention software, like the legendary Snort
- Penetration testing software

That last category might raise some eyebrows — after all, what's penetration testing if not an attempt to hack into a network? But part of making sure you're locked down involves seeing how hard or easy it is to break in, and pros know it; ethical hacking is an important part of network security. That's why you'll see tools like Aircrack — which exists to sniff out wireless network security keys — alongside staid corporate offerings that cost tens of thousands of dollars on the SecTools.org list.

In an environment where you need to get many tools to work together, you might also want to deploy SIEM software, which we touched on above. SIEM products evolved from logging software, and analyze network data collected by a number of different tools to detect suspicious behavior on your network.

Chapter Three

(Type Of Network Attack And Some Concepts)

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

Mohan V. Pawar and J. Anuradha / Procedia Computer Science 48 (2015) 503 – 506

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

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 tunnel ling 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.

d. Fabrication

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

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].

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. Inthis 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]

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 the cannot edit the data or cannot modify the data.

3. Advance 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 Mohan V. Pawar and J. Anuradha / Procedia Computer Science 48 (2015) 503 – 506.

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 net ork. In MANNET node looks like selfishness. A nod 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. Some Concepts

a. Hacker Categories

1.Hacker- Cleaver programmer

2.Cracker - Illegal hacker

3.Script Kiddies- Starting hacker. May not target a specific system. Rely on tools written by others.

4.White Hat Hackers- Good guys. Very

knowledgeable. Hired to find a vulnerability in a

network. Write own software.

5.Black Hat Hackers- Bad guys. Desire to cause harm

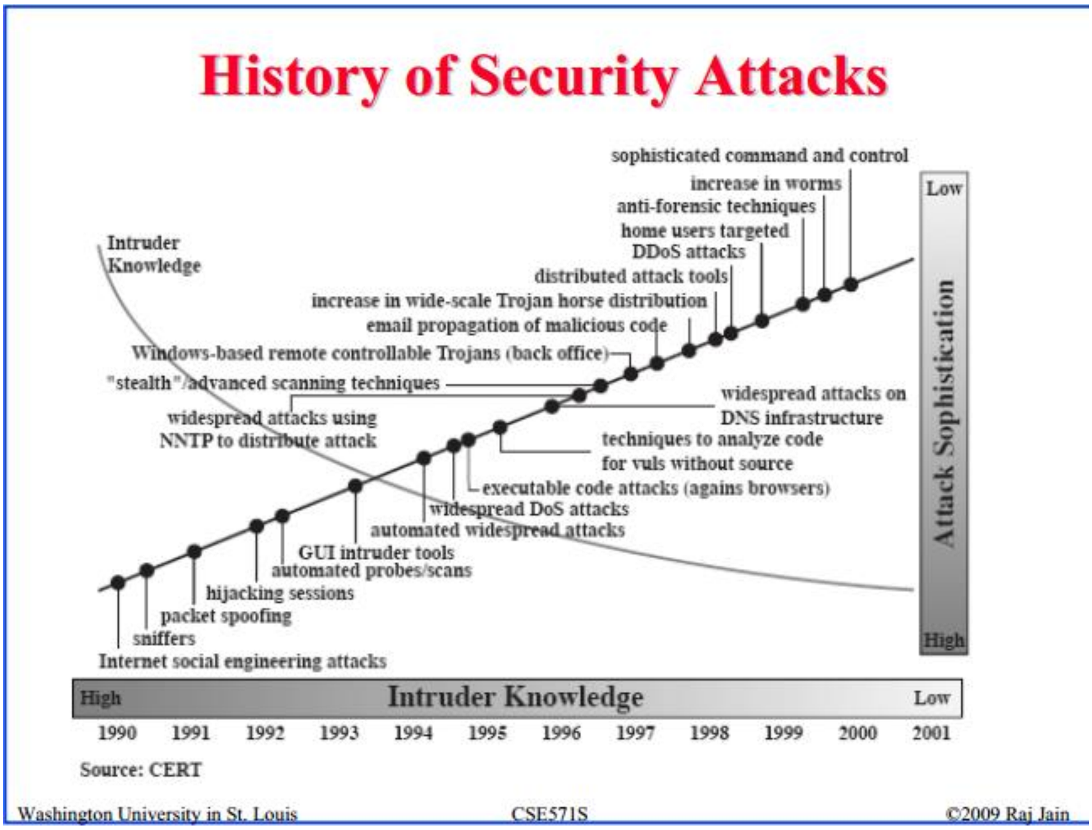
to a specific system. Write own software.

6.Cyber terrorists- Motivated by political, religious ،

or philosophical agenda.

b. Types of Malware

1. Viruses: Code that attaches itself to programs, disks, or memory to propagate itself.
2. Worms: Installs copies of itself on other machines on a network, e.g., by finding user names and passwords
3. Trojan horses: Pretend to be a utility. Convince users to install on PC.
4. Spyware: Collect personal information
5. Hoax: Use emotion to propagate, e.g., child's last wish.
6. !Trap Door: Undocumented entry point for debugging purposes
7. Logic Bomb: Instructions that trigger on some event in the future
8. Zombie: Malicious instructions that can be triggered remotely. The attacks seem to come from other victims.



History of Security Attacks

Source: CERT

Fig 3.1(history of security attack)

Chapter Four

(Suggestions and Reference)

4.1- Suggestions :

1- **Use strong authentication methods**
2- **Upgrade your software with latest security patch**
3- **Physically secure equipment and ports**
4- **Establish cyber security rules for your employees and make them aware of the important role they play in security**
5- **Encrypt your data and require users to enable bios passwords**
6- **Protect devices against viruses, spyware, and other malicious code**
7- **Protect and secure external network access**
8- **Perform regular internal security audits and plan for improvements**
9- **Define strong security rules for administrator accounts**
10- **Don’t forget about mobile and BYOD**

4.2- Reference :

1- "Network", www.techopedia.com, Retrieved 28-3-2019. Edited.

2- Computer Hope (13-11-2018), "Network" ،www.computerhope.com, Retrieved 28-3-2019. Edited.

3- Vangie Beal, "network" ،www.webopedia.com, Retrieved 28-3-2019. Edited.

4- Carmen Steele (29-1-2019), "Why is Computer Networking Important?" ، www.digitaldividecouncil.com, Retrieved 8-4-2019. Edited.

5- Neal Krawetz . Introduction to Network Security. Charles River Media. Boston, Massachusetts 02210. 2007.

6- William R. Cheswick and Steven M. Bellovin. Firewalls and Internet Security. AddisonWesley , Reading, Massachusetts, USA, 1994.

7- Raj Jain .Network Security Concepts . Washington University in Saint Louis. MO 63130. 2009. Page 2-9,2-10.

8- Siddharth Ghansela "Network Security: Attacks, Tools and Techniques" , ijarcsse Volume 3, Issue 6, June 2013.

9- Mohan V. Pawar , Anuradha J[2.] . Network Security and Types of Attacks in Network . Interscience Institute of Management andTechnology,Bhubaneswar, Odisha, India. (ICCC-2014)

10- ."Communication Systems and Network Technologies (CSNT)", 2014 , ISBN:978-1-4799-3069-2,7-9 April 2014.

11- Cisco Systems, Inc. and Internet Security Systems, Inc. versus Michael

12- Lynn and Blackhat, Inc. U.S. District Court, Northern District of California,

13- San Francisco Division. Case number 05-CV-0343, Judge Hon. Jeffrey White. July 28, 2005

. المراجع

1 "Network", www.techopedia.com, Retrieved 28-3-2019. Edited.

2 Computer Hope (13-11-2018), "Network" ‹www.computerhope.com, Retrieved 28-3-2019. Edited.

3 Vangie Beal, "network" ‹www.webopedia.com, Retrieved 28-3-2019. Edited.

4. Carmen Steele (29-1-2019), "Why is Computer Networking Important?" ‹ www.digitaldividecouncil.com, Retrieved 8-4-2019. Edited