

Wireless Network Security

JOCELYN O. PADALLAN

ARCLER PRESS

WIRELESS NETWORK SECURITY

Wireless Network Security

JOCELYN O. PADALLAN

ARCLER PRESS

www.arclerpress.com

Wireless Network Security

JOCELYN O. PADALLAN

Arcler Press
2010 Winston Park Drive,
2nd Floor
Oakville, ON L6H 5R7
Canada
www.arclerpress.com
Tel: 001-289-291-7705
001-905-616-2116
Fax: 001-289-291-7601
Email: orders@arclereducation.com

© 2018 Arcler Press

ISBN: 978-1-77361-305-5 (Hardcover)

This book contains information obtained from highly regarded resources. Reprinted material sources are indicated and copyright remains with the original owners. Copyright for images and other graphics remains with the original owners as indicated. A Wide variety of references are listed. Reasonable efforts have been made to publish reliable data. Authors or Editors or Publishers are not responsible for the accuracy of the information in the published chapters or consequences of their use. The publisher assumes no responsibility for any damage or grievance to the persons or property arising out of the use of any materials, instructions, methods or thoughts in the book. The authors or editors and the publisher have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission has not been obtained. If any copyright holder has not been acknowledged, please write to us so we may rectify.

Notice: Registered trademark of products or corporate names are used only for explanation and identification without intent of infringement.

Arcler Press publishes wide variety of books and eBooks. For more information about Arcler Press and its products, visit our website at www.arclerpress.com

About the Author



JOCELYN O. PADALLAN

Jocelyn O. Padallan is currently pursuing her Master of Science in Information Technology from Laguna State Polytechnic University, Philippines and has Master of Arts in Educational Management from the same University. She has passion for teaching and has been an Instructor at Laguna State Polytechnic, Los Banos Campus, Philippines.

Contents

List of Figures ..... *xi*

Preface ..... *xv*

Chapter 1 Wireless Network Security **1**

- Learning Objectives 1
- Introduction 2
- Types Of Wireless Networks 10
- Wireless Ad Hoc Network 14
- Case Study One: General Campus Wireless Network 29
- Case Study Two: Hall Of Residence 30
- Review Questions 31

Chapter 2 Problems in Wireless Communication **33**

- Learning Objectives 33
- Introduction 33
- Different Types Of Problems In Wireless Communication 34
- Performance Fundamentals of WirelessNetworks 39
- Measuring Real-World Wireless Performance 43
- Wireless Technology Standards 46
- Wireless Speed & Range 47
- Wireless Interference 48
- Review Questions 49

Chapter 3 Types of Wireless Network **51**

- Learning Objectives 51
- Introduction 52
- Types of Wireless Networks 56
- Types of Communication Technologies 58
- Types of Wireless Data Transmission 63
- Types of Wireless Devices 68
- Review Questions 76

Chapter 4 Security Measures In Wireless Networking 77

- Learning Objectives 77
- Wireless Network Security Keys 78
- Wi Fi Protected Access (Wpa And Wpa2) 79
- Wired Equivalent Privacy (Wep) 80
- Why Does The Little Acronym Matter? 82
- Wep, Wpa, And Wpa2: Wi-Fi Security Over The Era 82
- Wi-Fi Protected Access Ii (Wpa2) 88
- Wireless Network Security Technologies 90
- WPA and WPA2 Standards Based Security Certifications 94
- Review Question 101

Chapter 5 Challenges In Wireless Security 103

- Learning Objectives 103
- Introduction 104
- Problems Of Wi-Fi Security 104
- Recommendations For Wireless Security Architecture 107
- Risk In Wireless Networks 109
- Security Anywhere Access From Many Environments 114
- Ease And Control Of Administration 115
- Review Question 118

Chapter 6 Architecture Of Wireless Network 119

- Learning Objectives 119
- Introduction 119
- Security Associated With Each Layer Of The Osi Model 134
- Review Question 140

Chapter 7 Threat To Wireless Network- Active And Passive Attack 141

- Learning Objectives 141
- Introduction 141
- Session Replay Attack 144
- Types of Dos Attacks 147
- Methods OfPassive Attacks 150
- Review Question 156

Chapter 8 Measures To Prevent Active Attacks And Passive Attack 157

- Learning Objectives 157
- Introduction 157
- Types Of Passive Defences 158

- Patching Known Vulnerabilities 160
- Effects Of Positive Pre-Emptive Or Counterattacks 165
- Review Question 168

Chapter 9 Security Measures For Routing Protocols And Ieee Standards 169

- Learning Objectives 169
- Protecting Against Attacks On Routing Protocols 169
- Defending Against The Sybil Attack 171
- Defending On The Attacks In Privacy Sensor 173
- Basic Ieee Standards And Their Concepts 176
- Review Questions 181

Chapter 10 Security Goals In Wireless Communication And Issues 183

- Learning Objectives 183
- Introduction 184
- Security Goals/Elements 186
- Service Reliability And Availability 188
- Wired Equivalent Privacy (Wep) 189
- Wireless Protected Access (Wpa) And Wireless Protected Access 2 (Wpa2) 191
- Wireless Connectivity Security Challenges 193
- Case Study: Interference In French Universities Computer System 197
- Case Study: A Pupil Hacked His University Network 197
- Review Questions 197

References 199

Index 201

List of Figures

Figure 1.1: Wireless device
Figure 1.2: LAN cable
Figure 1.3 Telecommunication through wireless networking
Figure 1.4: suitability of wireless networking
Figure 1.5: social media
Figure 1.6: advantages of wireless networking
Figure 1.7: mobility as an advantage of wireless networking
Figure 1.8: WIMAX technology
Figure 1.9: wireless PAN
Figure 1.10: connecting different devices using wireless networking
Figure 1.11: different types of cables
Figure 1.12: wireless AD-Hoc network
Figure 1.13: wireless MAN
Figure 1.14: Wireless WAN
Figure 1.15: tower of a cellular network
Figure 1.16: transfer of data
Figure 1.17: types of cellular network
Figure 1.18: transfer of data using cable
Figure 1.19: Digital advanced mobile phone service
Figure 1.20: GAN
Figure 1.21: Satellite over space
Figure 1.22: Bluetooth technology
Figure 1.23: properties of wireless network
Figure 1.24: Mobile switching center
Figure 1.25: encryption

Figure 1.26: encrypted security to wireless security
Figure 1.27: Password security
Figure 2.1: Different types of problems
Figure 2.2: multipath diminishing
Figure 2.3: Network bandwidth
Figure 2.4: security to wireless network
Figure 2.5: Cyber security
Figure 2.6: radio communication from one place to another
Figure 2.7: cell breathing
Figure 2.8: communication through cell breathing
Figure 2.9: wireless networking
Figure 2.10: standards of wireless technology
Figure 2.11: Wi-Fi gadget range
Figure 2.11: signal strength
Figure 3.1: wireless mesh network
Figure 3.2: types of wireless network
Figure 3.3: storage area network
Figure 3.4: IEEE logo
Figure 3.5: wireless connection of different devices
Figure 3.6: connected to home through wireless network
Figure 3.7: home technology
Figure 3.8: mobile phone
Figure 3.9: types of wireless technology
Figure 3.10: connecting different devices through Bluetooth
Figure 3.11: ZIGBEE protocol
Figure 3.12: wireless network hub
Figure 3.13: types of wireless devices
Figure 3.14: wireless router
Figure 3.15: adapter
Figure 3.16: broadband router
Figure 3.17: wi-fi repeater
Figure 3.18: wireless repeater
Figure 3.19: microwave transmitter

Figure 3.20: infrared waves
Figure 3.21: infrared transmission
Figure 3.22: old style radio
Figure 3.23: wireless mobile phones
Figure 3.24: cellular mobile
Figure 3.25: video games
Figure 3.26: walkie talkie
Figure 4.1: security circle to wireless network
Figure 4.2: Security
Figure 4.3: wireless network security keys
Figure 4.4: coded security
Figure 4.2: wireless IP cameras
Figure 4.3: wireless network security device
Figure 4.4: security networking device
Figure 4.5: security settings
Figure 4.6: encryption of security device
Figure 4.7: digital authentication
Figure 4.8: security levels breach impact
Figure 4.9: towers of wireless network
Figure 4.10: cipher encryption
Figure 4.11: virtual private network
Figure 4.12: icon issues
Figure 4.13: two-way security
Figure 4.14: proxy server
Figure 4.15: Wi-Fi signal
Figure 5.1: wireless network transmitter
Figure 5.2 firewall security
Figure 5.3: wireless device security
Figure 5.4: SDH and ethernet ring aggregation
Figure 5.5: measures to security
Figure 5.6: access control
Figure 5.7: no signal
Figure 5.8: security to AD-hoc network

Figure 6.1: architecture of connectivity
Figure 6.2: touch security
Figure 6.3: multilevel OSI model
Figure 6.4: Eavesdropper to transmitter to intended receiver
Figure 6.5: OSI 7-layer model
Figure 6.6: applications to wireless sensor networks
Figure 7.1: different types of active attacks
Figure 7.2: structure of an attack
Figure 7.3: type of DOS attack
Figure 7.4: architecture of a DOS attack
Figure 7.5: methods of passive attacks
Figure 7.6: types of passive attack
Figure 7.7: tree structure of wireless network
Figure 7.8: unsuccessful eavesdropping by encryption
Figure 8.1: weapons to active attacks
Figure 9.1: Non-overlapping channels
Figure 10.1: Classic cryptosystem with media access control (MAC) layer encryption as an example. The grey blocks represent the encrypted data.
Figure 10.2: security elements/goals
Figure 10.3: Wired Equivalent Privacy (WEP)

Preface

This book systematically focuses on the field of wireless security in network. All the important areas of wireless communication have been covered in this book. This topic is interdisciplinary in nature. Hence, the related topics covering wireless network and security have been discussed at various points in the book. The books also describe the key issues which are being faced in the wireless communication system as well as in the security system to protect it.

The book starts with an introduction to the field of wireless network and security and explains the basic terms as well as the concepts related to it. Subsequently, the history of wireless network and how it has evolved over all the years has been discussed in this book. Various problems related to wireless network communication and security have been explained. Chapter two describes the real-time problems which are already being faced in the wireless network along with the types of wireless devices. How these devices can be used as a medium in the theft of data has also been explained.

Later the security measures in wireless network have been elaborated and challenges in the field of wireless security has been shown. In chapter six, the architecture of wireless network in the terms of OSI model have been elaborated. The next chapter focuses on the attacks to wireless network which are active attack and passive attack and the chapter next to it deals with the measures to prevent these attacks. With the rapid advancement in technology, security measures have also been arranged in the advanced way. In chapter nine, the securing of data through routing protocol has been discussed along with the IEEE standards. In last chapter of the book, the security goals along with the issues related to the wireless communication are discussed.

Author

CHAPTER 1

WIRELESS NETWORK SECURITY

LEARNING OBJECTIVES

- Evolution of Wireless Technology
- How Data is secured in the wireless network
- What are the types of wireless network?
- Types of network in cellular data
- Personal mode of wireless communication such as Bluetooth, Infrared, LAN etc.
- Standards in wireless communication
- How secured are we in a wireless network



Figure 1.1: Wireless device

INTRODUCTION

DID YOU KNOW

Previous names for Wi-Fi were WaveLan, Flank-Speed, DragonFly, WECA and IEEE 802.11b Direct Sequence, before the more consumer friendly name of Wi-Fi was adopted

A system of flexible data communications is known as a wireless network. This makes use of wireless media, for example, radio frequency technology to transfer and receive data over air. This, in turn, minimizes the necessity for wired connection.

Wireless networks are used to expand instead of replacing the existing wired networks.

They are most commonly used to make available last few points of connectivity between a mobile user and a wired network.



Figure 1.2: LAN cable

A computer network which uses wireless data between the nodes of network is known as wireless network.

In other words, a wireless network is a computer network that uses wireless data connections between network nodes.

In recent years we have seen that the telecommunication industry has encountered a tremendous innovation in technology.

Some of these technological developments are a result of breakthrough of science. The other innovations have been derived from the well-known principles of demand, which see an inherent gap, and thus aim at fulfilling the needs of customers.

As the inception of wireless network has rapidly increased, its demand in consumption has led to an increase in connectivity across networks.

This topic will let us know about the idea of how far have we come in this field as well as the future perspective of wireless communications.

Clearly, we can see that apart from today's technology, the actual definition of telecommunication can get us all the way back in the time pigeons were used to transfer message from one place to another.

This is the simplest example of wireless communication. In the modern approach there were many innovations year after year.

The wireless as we see today is a result of centuries of innovation. In year 1684, Robert Hooke, a British scientist, invented panels in mobile which was even coded in letters of the alphabets.

This was the earliest example to show the existence of our modern telecommunication. This theory was further elaborated in the 18th century which appeared in the inventions of optical telegraph.

This was created by Claude Chappe, who was a French scientist. This device used to transmit coded words of data from one place to another and carried it a long way without wire.

Tracking this large-scale tower with signals which were developed and installed in a city of France, were also assisted by the nearby countries.

These are considered as precursors to radio communications. With the help of these technologies, it was possible for generations to learn the basic sciences in the field of telecommunications.

The developments were a result of issues faced in these communication systems, which demonstrated how this modern fixed wireless system like millimeter wave and microware are linked by infrared.

Post this, Radio Communication came into existence which was the use of radio waves in transmitting the coded

information. This was developed by the hard work of Maxwell and Hertz, who experimented with their innovative thoughts using electromagnetic waves.

This experiment also used the first paper detailing of radio communication system. This radio communication system was first described by Tesla in late 1800.

Somewhere near the same time a scientist named Marconi who patented the telegraph, showed the use of mobile communication in the crossing of war ships with the English Channel.

Then, these technologies continued to develop and after several years' people started to understand the complexities associated with telecommunications.



Figure 1.3: Telecommunication through wireless networking

The major change was seen in the field of telecommunication was during the second world war, when the research of military was done with the help of radar and with the help of remote sensing.

This is the place when a lot of controversies came in the telecommunication which included the strong encryption and giving a proper security to the data which is being transferred. Then the companies started to focus more on the encryption of data and preventing it from getting stolen.

A huge number of subsequent firms emerged with this technology which also included the broadcasting of Television.

Now, in the year 1970, AT&T Bell Labs started a cellular system and continued to bring advance technology to the people who were using it, the results of which can be seen now.

This also included the standards and spectral efficiencies and lowering down the price of the products due to competition and increase in competitors.

This made it led in the commercial market and people had their acceptance.

From that time till now, customers have risen to a most modern device possible which is wireless mobile with a lot of services.

With the increase in telecommunication services the risk of theft is also increased which is a high risk for the people and the enterprise.

This is taken care of by encrypting data and making sure about the key and acknowledging the data which is being transferred from one place to another.

Wireless networking is a means by making use of which homes, telecommunications networks and corporate fittings evade the expensive procedure of installing cables into a building, or as a connection between numerous gear locations.

Wireless telecommunications networks are usually executed and managed using radio communication. The execution of wireless communications happens at the physical level of the OSI model network structure.

Some of the examples of wireless networks comprise cell phone networks, wireless local area networks (WLANs), wireless sensor networks, satellite communication networks, and terrestrial microwave network.

Electromagnetic waves or radio waves are used in wireless networks to transmit information from point to another. This does not rely on the wired connection i.e. physical connections.

Often, the radio waves are known as radio carriers. These are referred to as radio carriers only due to the reason that they basically accomplish the function of transporting energy to a remote receiver. The transmitted data is overlaid on the radio carrier. It is done as, so that data which is being transmitted can be precisely pulled out at the receiving end.

The signal of the radio dwell in more than a single frequency after the superimposing of data.

The signal occupies single frequency as the frequency of the controlling information augments to the carrier.

When the radio waves are transmitted on different radio frequencies, then various radio carriers can co-exist in the same space at the same time without any interference among anyone.

A radio receiver tunes into single radio frequency to pull out data, while at the same time declining all other frequencies.

The received signal i.e. moderated signal is then demodulated and the data is pulled out from the signal.

There are three different elements involved in transferring data through a wireless network. It comprises of involves the radio signals, the data format, and the network structure.

All these elements are independent of each other; thus, all of these should be defined while giving introduction to wireless networks. Radio signal works at the physical level while referring to the terms of OSI model and the several other higher levels are controlled by the data format.

The structure of the network comprises of the wireless network interface adapters and base stations. The work of these adapters and base stations is to transmit and receive the radio signals.

The interface adapters of network in each computer convert digital data to radio signals in a wireless network. Base stations work in the same manner. They also convert the digital data to radio signals.

These radio signals are then transmitted to other devices on the equivalent network. In addition, their job is to receive and change incoming radio signals from other network elements back to digital data.

All of these wireless data services of broadband make use of dissimilar grouping of radio signals, data formats, and network structure.

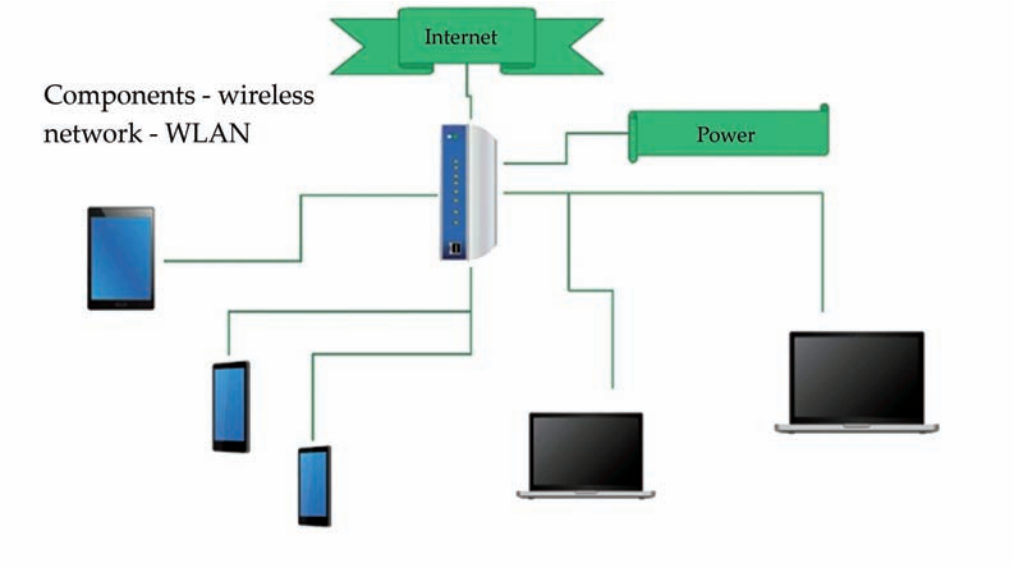


Figure 1.4: suitability of wireless networking

Wireless networks provide below given benefits. It offers various efficiency, suitability, and cost advantages over outdated wired networks:



Figure 1.5: social media

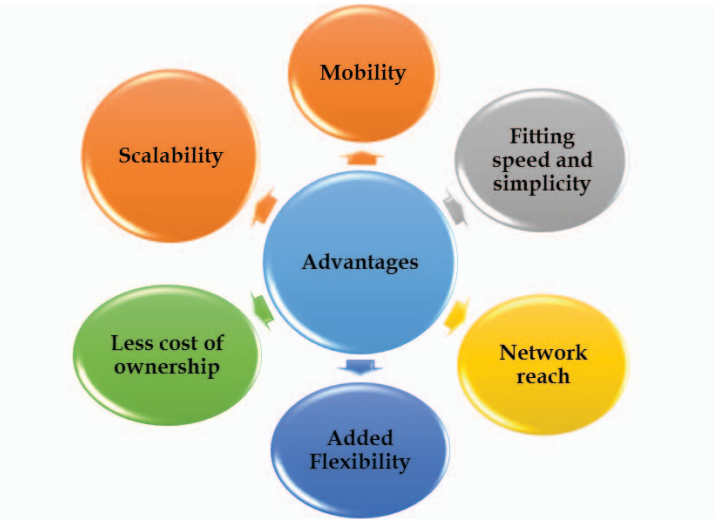


Figure 1.6: advantages of wireless networking

Mobility

Wireless networks enable mobile users access to actual information.

This helps them to roam around the world without worrying about the network.

The mobile users do not have to worry about getting disconnected from the network.

This type of mobility backs productivity and service opportunities which are impossible with wired networks.

Fitting Speed and Simplicity

Setting up of a wireless system can be quick and easy. This reduces the necessity to extract cable through walls and ceilings.

Network Reach

The reach of the wireless network is very high. The wireless network can be stretched to places which cannot be wired.



Figure 1.7: mobility as an advantage of wireless networking

Added Flexibility

The flexibility offered by the wireless networks is more. Wireless networks adjust effortlessly to deviations in the configuration of the network.

Less Cost of Ownership

The initial amount of investment provisionary for wireless networks is high. It is higher than the conventional wired network system.

However, overall cost is covered in the product cycle. The total costs can be meaningfully lower in dynamic environments.

Scalability

To meet the requirements of the particular application and installations, the system of wireless network can be configured in a variety of topologies.

Configurations can be simply altered and range from person-to-person networks appropriate for a small number of users to large infrastructure networks that allow roaming over a wide-ranging area. One thing which is very clear is that as wireless technologies will evolve continually. This will continually provide other organizations and its end users much higher standard of life by making them mobile and expanding the ability of

individuals to communicate with one another by removing barriers of distance.

There is a possibility that any individual while sitting at airport can connect to the network of home or office.

Also, people could also be able to use or surf web at any place. Users can surf web on handheld computers and also while walking down the street.

Service providers of Internet can install huge wireless networks which would permit them to connect from anywhere in the city.

All these technologies are possible with the use of wireless technologies. There is a possibility that sooner or later, the network will follow us instead of us following it.

TYPES OF WIRELESS NETWORKS

A group of devices which are connected to each other is known as a network. Radio communication is commonly the standard of choice in the instance of wireless networks.

However, though amongst the radio-powered subgroup, there are lots of diverse technologies that are structured for use at diverse scales, topologies, and for vividly dissimilar use scenarios.

Another way to depict this difference is to part the use scenarios on the basis of their "geographic range":

The previous cataloguing is neither wide-ranging nor precise. There are numerous technologies and standards which begin within an exact use case, for instance, Bluetooth for PAN applications and cable replacement, and with time obtain additional competences, reach, and throughput.

As a matter of fact, the modern drafts of Bluetooth here and now deliver unified interoperability with 802.11 (Wi-Fi) for high-bandwidth use cases.

Likewise, technologies such as WiMAX have their roots as fixed-wireless solutions, however, as time passes by, developed extra mobility capabilities, make them a practical alternative to other WAN and cellular technologies.



Figure 1.8: WIMAX technology

Table 1.1: Types of network

Type	Range	Applications	Standards
Personal area network (PAN)	Within reach of a person	Cable replacement for peripherals	Bluetooth, ZigBee, NFC
Local area network (LAN)	Within a building or campus	Wireless extension of wired network	IEEE 802.11 (Wi-Fi)
Metropolitan area network (MAN)	Within a city	Wireless inter-network connectivity	IEEE 802.15 (WiMAX)
Wide area network (WAN)	Worldwide	Wireless network access	Cellular (UMTS, LTE, etc.)

Point here is to classify and highlight the high-level changes amongst each use case. The point here was not to classify of partition of each technology into a different basket. There are devices which have access to a constant power source. Other devices might just improve their battery life at all costs.

Some devices necessitate Gbit/s+ data rates and other devices are made to allocate tens or hundreds of bytes of data such as NFC.

There are many applications that need connectivity of always-on while some are delay and latency tolerant. These and other large number of standards fix the creative features of each type of network.

But, once it is set in place, every standard remains to progress: improved battery measurements, quicker computers, better modulation algorithms, and other progresses remain to cover the use cases and performance of every wireless standard.

Wireless PAN



Figure 1.9: wireless PAN

Amongst a relatively small area, wireless personal area networks (WPANs) internet devices is usually within an individual's reach. For instance, Bluetooth radio and unseen ultraviolet light offers a Wireless Personal Area networking for connecting an earpiece to a laptop. ZigBee also supports WPAN applications. Wi-Fi PANs are fetching common place as equipment creators begins to mix Wi-Fi into a variety of consumer electronic devices.

Wi-Fi has been made easier and modest in installations and configuration by the Intel "My Wi-Fi" and Windows 7 "virtual Wi-Fi" abilities.

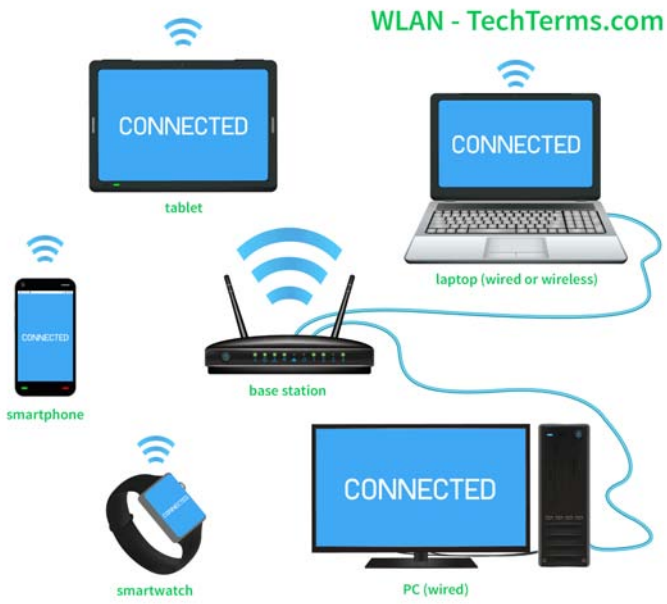


Figure 1.10: connecting different devices using wireless networking

Wireless LAN



Figure 1.11: different types of cables

The wireless network which is often used for interconnecting with local resources and the network is known as Wireless LAN.

This type of wireless network connects two or more devices within a short distance while making use of wireless distribution method, generally offering a connection by an easy access point for internet Access. This type of wireless network makes use of spread-spectrum or OFDM technologies.

This technology may permit users to roam around in a specific range of a local coverage area, while remaining intact to the network.

The products which use the IEEE 802.11standard of WLAN are sold under the brand name of Wi-Fi. Fixed wireless technology executes point-to-point links among computers or networks at dual detached locations, every so often by means of dedicated microwave or modulated laser light beams over line of sight paths.

It is very frequently used in cities to connect networks in two or more buildings without fitting a wired link.

WIRELESS AD HOC NETWORK

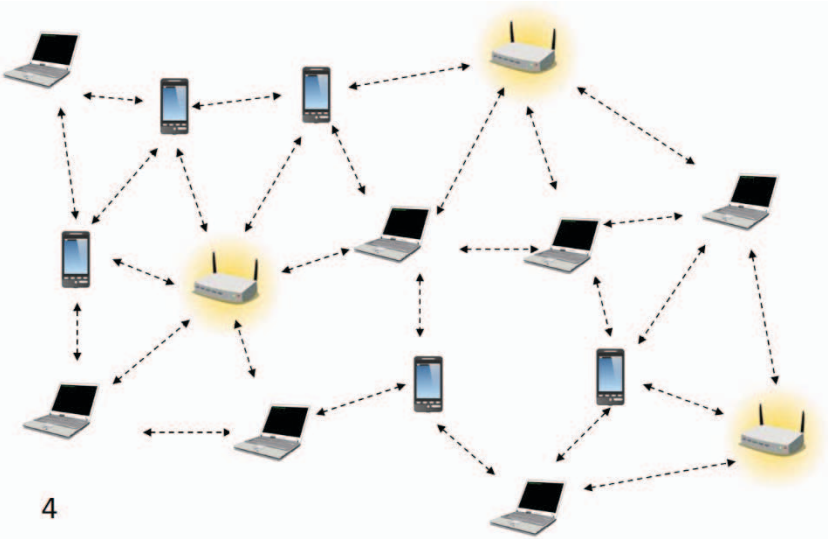


Figure 1.12: wireless AD-Hoc network

A wireless network which is made of radio nodes systematized in a web topology is referred to as a wireless ad hoc network.

This type of network is also referred to as a wireless mesh network or mobile ad hoc network (MANET).

The messages are forwarded in each node on the basis of other nodes and every node thus then performs routing. These Ad hoc networks can "self-heal". The nodes which have lost power can automatically re-route around a node.

Numerous layers of network protocol are required to identify ad hoc mobile networks, for instance, associativity-based routing, dynamic source routing, distance sequenced distance vector routing, and ad hoc on-demand distance vector routing.

Wireless MAN



Figure 1.13: wireless MAN

The type of wireless networks which connects various wireless LANs is known as wireless metropolitan area networks. WiMAX is a kind of Wireless MAN. This is explained by the IEEE 802.16 standard.

Wireless WAN



Figure 1.14: Wireless WAN

The wireless networks which cover a wide range of area are known as Wireless wide area networks, for instance, between adjacent towns and cities, or city and suburb.

This type of networks can be taken in use to attach branch offices of corporates or as a public Internet access system. The wireless connections among entree points are generally point to point microwave connections which uses parabolic dishes on the 2.4 GHz band. They do not use omnidirectional antennas which are used with smaller networks. A distinctive system comprises base station gateways, access points and wireless bridging relays.

Each access point are other configurations which performs the function of a relay also.

These systems can even stand alone when they are connected with renewable energy systems such as photovoltaic solar panels or wind systems.

Cellular network



Figure 1.15: tower of a cellular network

A radio network which is distributed over areas of land known as cells where each cell is served by at least one immovable location transceiver is defined as a cellular network or mobile network.

The fixed location known as base station or cell site. When each cell routinely uses a diverse set of radio frequencies to avoid any interference from all the direct adjacent cells.

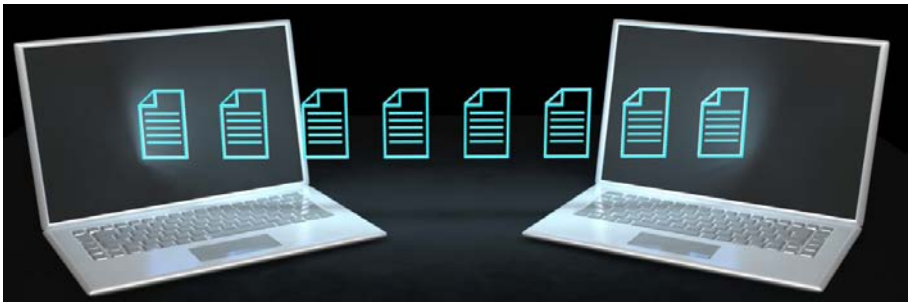


Figure 1.16: transfer of data

All these cells provide coverage of radio over wide range of geographic area when they are joined together.

This allows for a great number of portable transceivers for example, mobile phones, pagers, etc. to connect with each other and with immovable

transceivers and telephones wherever in the network, through base stations, even though some of the transceivers are stirring over more than one cell during transmission.

Even though cellular networks were initially envisioned for cell phones but with the progress and advancement in technology, such as smartphones, cellular telephone networks now habitually transmit data in addition to telephone conversations:

- Global System for Mobile Communications (GSM):

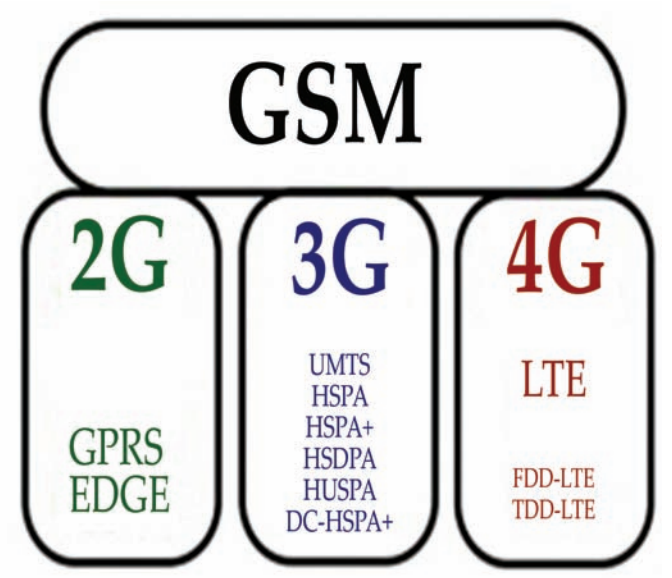


Figure 1.17: types of cellular network

The network which is partitioned among three big systems is referred to as GSM network. This network is divided between the switching system, the operation and support system and, the base station system.

The base system station is connected by cell phone that after that connects to the support station and operations. This system then connects to the switching station. Afterwards the call is transferred to the location it requires to reach. GSM is the greatest shared standard. This wireless network is used by majority of cell phones. and is used for a majority of cell phones.

Personal Communications Service (PCS)



Figure 1.18: transfer of data using cable

Personal Communications Service is a radio band which is used by mobile phones in North America and South Asia. For example, Sprint chanced to be the first service to set up a PCS.

D-AMPS



Figure 1.19: Digital advanced mobile phone service

An updated version of AMPS is referred to as Digital Advanced Mobile Phone Service. This is being phased out because of the progress in the technology. Latest GSM networks are substituting the older system of networks.

Global Area Network

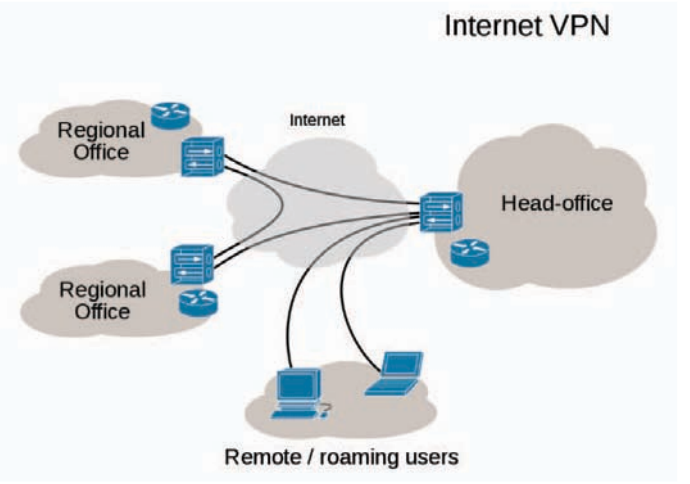


Figure 1.20: GAN

The wireless network which supports mobile across a random number of wireless LANs, satellite coverage areas, etc. are referred to as a global area network (GAN).

The most significant difficulty in mobile communications is passing off user communications from one local coverage area to the next. The succession of terrestrial wireless LANs is involved in the IEEE Project 802.

Space network

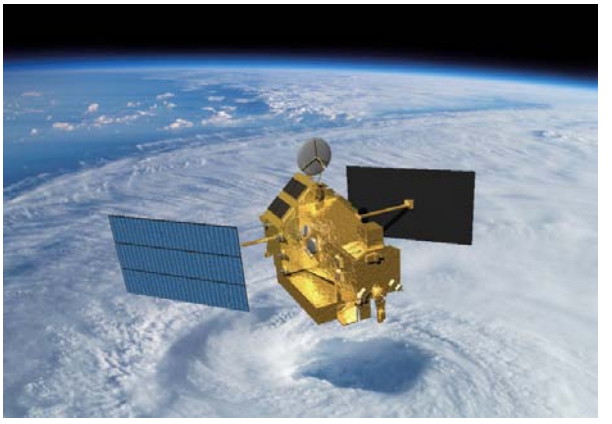


Figure 1.21: Satellite over space

The networks which are used in the space are known as space networks. They are often in vicinity of the Earth. Most known example of space network is NASA's Space Network.

Bluetooth

The wireless network which has a possibility of changing the way people make use of devices to connect is Bluetooth and 802.11b. This has the potential to change the way of communication in daily life. This requires low power and short range for replacement of Ad-hoc cable. Bluetooth enables users to connect devices wirelessly everyplace they bring them.



Figure 1.22: Bluetooth technology

On the other hand, the medium range and medium speed technology which is based on the Ethernet is referred to as 802.11b.

This technology permits people an easy access to the network of organization over a range of campus area, wirelessly. Although the technologies share the 2.4 GHz band. Technologies have some possibly overlying applications. They have been rutted against each other in the press, they do not contest and can even been positively shared for corporate use.

Different uses

The wireless networks are used in various devices on a daily basis. For instance, most common example of usage is cellular phones that are part of daily life of almost every individual. They allow easy and simple personal communications. One more example of this can be Intercontinental network

systems. This system uses radio satellites to interact across the world.

Wireless networking is used in emergency services as well. For instance, the police utilize wireless networks to connect efficiently.

Individuals and businesses use wireless networks to direct and share data quickly, whether be it in an insignificant office building or across the world. In an over-all sense, wireless networks provide an enormous variety of usages by both business and home users.

Properties

Here and now, the industry receives not many of diverse wireless technologies. All the wireless technologies are explained by standards which explain exclusive functions at both the Physical and the Data Link layers of the OSI model.

The standards of these technologies vary in their stated signaling methods, geographic ranges, and frequency usages, among various different things. The differences of these types make sure that some technologies best suit to home networks and others best suits to network larger organizations.

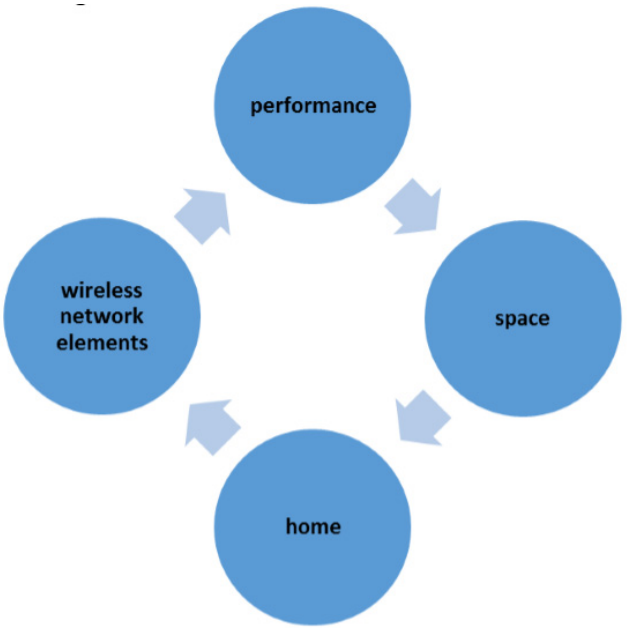


Figure 1.23: properties of wireless network

Performance

Individually every standard differs in geographical range, therefore each standard is creating each more supreme than the following which is reliant on what one is attempting to achieve with a wireless network.

Satisfaction of variety of applications for instance voice and video is dependent upon the performance of wireless networks. Widespread usage of these technologies provides room for development of these technologies as 2G to 3G and now to 4G.

4G depicts the fourth generation of cell phone mobile communications standards. Complexity is increasing rapidly in the configuration of network hardware and software as due to the fact that wireless networking has developed into a commonplace.

It has a better capability to transmit and receive greater and amounts of data, faster, is accomplished.

Space

Space is another distinguishing feature of wireless networking. Wireless networks provide numerous benefits when it is about the difficult-to-wire areas attempting to connect for example, over a street or river, a granary on the different side of the buildings or structures that are actually parted however, function as one.

Users are permitted to be designated to a particular space by wireless networks and the network will be able to interconnect with other devices by that network.

Space is also formed in households as a consequent of removing messes of wiring. This technology permits for a substitute to fit in physical network means such as TPs, coaxes, or fiber-optics. These can also be costly.

Home

Wireless network system is an efficient method related to Ethernet for sharing printers, scanners, and high-speed internet connections for homeowners. This type of network assists in saving the cost of installing cable wires and also helps in saving time for manual installation of cables.

This creates flexibility for devices that are connected to the network. This type of networks is simple and necessitate as one lone wireless access point which is directly connected to the Internet via a router



Figure 1.24: Mobile switching center

Wireless Network Elements

The telecommunications network comprises of numerous interconnected wireline network elements at the physical layer. These network elements can be unconnected systems or products.

These are that which are either provided by a lone manufacturer or else they are accumulated together by the service provider (user) or system integrator with parts from several dissimilar manufacturers.

To provide support for the backhaul networks also for mobile switching center (MSC) are used by the wireless Network Elements as the products and devices.

Consistent wireless service rest on the network elements at the physical layer which is needed to be endangered in contradiction of all operational environments and applications.

The especially significant network elements are the ones which are positioned

to the base station on the cell tower. The extra hardware and the location of the antenna and related conclusions and cables are mandatory to have satisfactory forte, strength, erosion resistance, and resistance against wind, storms, icing, and other weather conditions.

Necessities for specific mechanisms, for instance hardware, cables, connectors, and closures, intend to consider the design to which they are linked.

Security

Wireless security is defined as the preventions taken against illegal access and damage caused to computers by using wireless networks. Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) are the most common types of wireless security

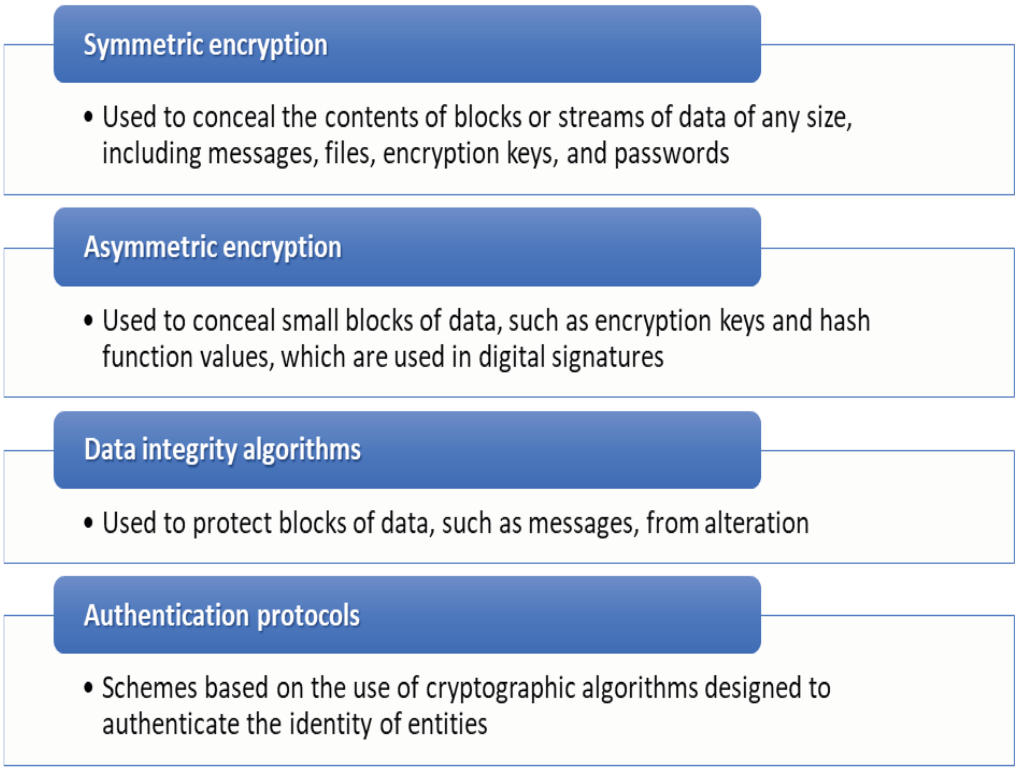


Figure 1.25: encryption

WEP is a weak security standard as the password it uses can easily be hacked within a few minutes with a basic laptop or computer and the software tools which are widely available.

WEP was introduced in 1999 and is an old IEEE 802.11 standard which was outdated by the introduction of WPA, or Wi-Fi Protected Access in 2003.



Figure 1.26: encrypted security to wireless security

It was found out to be best and quick alternative over WEP to improve security. In present scenario, the standard used is WPA2 but few hardware without firmware upgradations and replacement cannot support WPA2.

WPA2 utilizes an encryption device in which the network is encrypted with a 256-bit key and the security over WEP is improved by using the longer key.

Security Goals

Many security functions are provided by each security system that maintain the secrecy of the system. These security functions are called as the goals of the security system.

There are mainly five categories of the goals which are listed below:

Authentication

The identity of both the sender and receiver must be ensured before transmitting the data between the sender and receiver using the system.



Figure 1.27: Password security

Secrecy or Confidentiality

Most of the people determine a secure system usually by this function or feature. It means only the ones who are authenticated will be able to interpret the content of the message and no one else.

Integrity

Integrity means that the content of the data which is transmitteds between the sender and receiver does not require any type of modification. The most common form of integrity in IPv4 packets is packet check sum.

Non-Repudiation

Non-Repudiation function ensures that neither the sender nor the receiver can deny falsely that they have sent a particular message.

AMAZING FACTS!!!

"Don't click any strange links. Educate yourself about how cyber-attacks look and work on social media platforms and learn how to protect your Facebook, LinkedIn, Twitter and Instagram accounts. Install a solution that can protect you against malware and dangerous web locations."

Service Reliability and Availability

The users must be provided the services which are promised by these secure systems as many secure systems are usually attacked by hackers which not only affect their availability but also the type of services granted to the users.

CASE STUDY ONE: GENERAL CAMPUS WIRELESS NETWORK

At this institution, 40 wireless access points have been installed across the main campus. They are from the same manufacturer, use 802.11b and are connected as a single, virtual network to a gateway which requires a username and password. The access points provide wireless coverage for most recreational and social spaces on campus, such as bars and refectories. It also covers parts of the Library and some outdoor spaces where students gather.

The wireless network is predominantly used by students, although there are some staff users. Students supply their own wireless cards, although most are now using laptops with them built in, and there have been few problems with configuring their cards. There are about 200 users who have used the wireless network and email and web browsing are the most popular applications. There are a very small number of PDA users who are also using the wireless network to access their email. The wireless network was installed during the Michaelmas term 2001 and was very lightly used for the first year. The number of users has grown significantly since that time and is expected to continue to grow. The performance of the network is generally quite good in areas where the signal is strong and the large number of access points means that there are only a few active users on each. The nature of email and web page network traffic means that each user generates short bursts of network activity which works quite well with this technology.

Prior to the installation of the gateway, security was a major concern and there was some evidence of unauthorized people using the wireless network. Maintenance of the access points is fairly labor intensive and it is generally necessary for the administrator to manually change configuration settings or upgrade the firmware on each access point individually.

Where an area receives a signal from more than one access point and both are using the default channel, users can experience interference and consequently very poor performance.

To address this problem, a survey of the signals across the campus will be conducted and specific channels assigned to each access point so that there are no longer any overlapping signals on the same channels. This example demonstrates the strengths and value of a campus wireless network. It has sufficient access points, is being used for applications that generate bursts

of activity and so are suited to a shared network and is secured against extraneous use.

The security and channel interference issues do however demonstrate the importance of pre-installation planning.

CASE STUDY TWO: HALL OF RESIDENCE

In this institution, a wireless network was installed in a student hall of residence. This was a relatively small hall with 90 bed spaces housed in 4 blocks with one block including accommodation for social spaces and an open access IT room. There are 3 access points located in the loft spaces of 2 of the blocks. All access points are 802.11b.

Approximately 95% of residents have their own PC and they are supplied with a loan wireless card which must be returned at the end of the year. The network is used very heavily during the evenings for many different applications.

Some users are browsing the web or reading their email, but many are running software packages from the main campus and a significant number are streaming music and video from the Internet or using peer to peer file-sharing software.

The signal coverage is very patchy, in some rooms there is a good signal in one part of the room but virtually none at the desk. Many residents complain of poor performance and at peak times it can take 20 minutes to login to the campus network.

Investigations have shown that the file-sharing traffic has a particularly severe impact on the performance of the wireless network. Attempts to restrict the use of file-sharing software have been partially successful in improving performance but have also been very unpopular.

This example shows the inherent problems with a wireless network in a Hall of Residence where there are very heavy peaks of usage. Some of the applications being used generate long sustained streams of network activity which make them unsuitable for used on shared networks.

There are also too few access points to cope with this level of demand.

REVIEW QUESTIONS

1. How did the wireless networking evolve over the years?
2. What are the different types of wireless network?
3. Explain the various standards in wireless communication.
4. Differentiate between wireless PAN and Wireless LAN.
5. Differentiate between wireless MAN and wireless WAN.
6. What is Bluetooth technology and what is the role of Bluetooth technology in evolution of wireless networking?
7. Explain Wireless security and Security goals in wireless communication.
8. What are cellular networks and what are the different technologies used in cellular network.

CHAPTER 2

PROBLEMS IN WIRELESS COMMUNICATION

LEARNING OBJECTIVES

- What are the different types of problems that are associated with wireless communication?
- Multipath diminishing of network
- Safety and Security in wireless communication
- Bandwidth at a glance
- Problems in network because of wavelength
- Power consumption and stability problems in network communication
- Evaluation of wireless network in real time
- Methods to increase the efficiency

INTRODUCTION

In the past few years the general use of radio communication design has driven into a totally different direction from maximizing the capacity of individual to optimizing the capabilities of network with multiuser. The decisive interference now seldom comes from outside (as in military systems), but is produced by authorized users of the very same wireless network. Users thus share an interest

in developing and adhering to the best possible protocols and standards for allocating the joint network resources. "First of all, the receive signal is not a strong line-of-sight signal but are a lot of reflections from obstacles. That's called multipath reception.

But this can be resolved if you design a system in an appropriate way, using digital processing techniques. What has become very important in the last few years are three issues"

DIFFERENT TYPES OF PROBLEMS IN WIRELESS COMMUNICATION

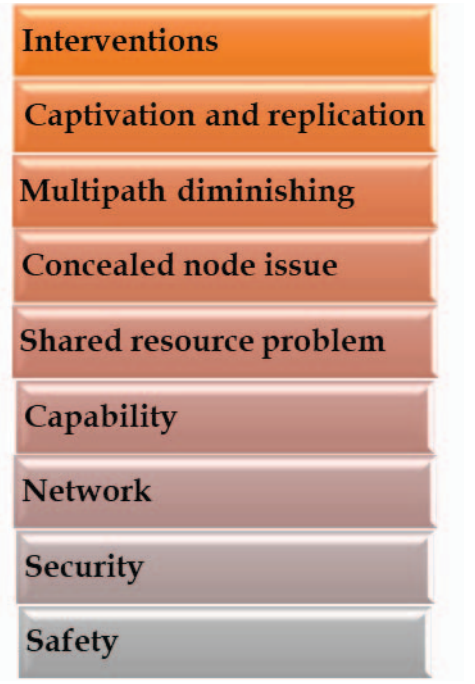


Figure 2.1: Different types of problems

The basic problems which are being faced in the wireless communications are as follows:

Interventions

While comparing to the wired systems, wireless networks are often focus to electromagnetic interference. Interventions are caused by the other networks

or by other type o devices which generate radio waves that are inside, or close, to the bands of radio.

These are used for interaction. Intervention and inference reduce the signal or may also cause failures for the system.

Captivation and Replication

Nearly some constituents cause captivation of electromagnetic waves. Thus, it prevents it from reaching the receiver. On the other hand, in many other cases, chiefly with metallic or conductive materials, replication happens.

This may reason dead zones where there is no availability of reception. In modern homes, aluminum foiled thermal isolation can effortlessly decrease indoor mobile signals by 10 dB frequently which leads to grievances about the bad reception of long-distance rural cell signals

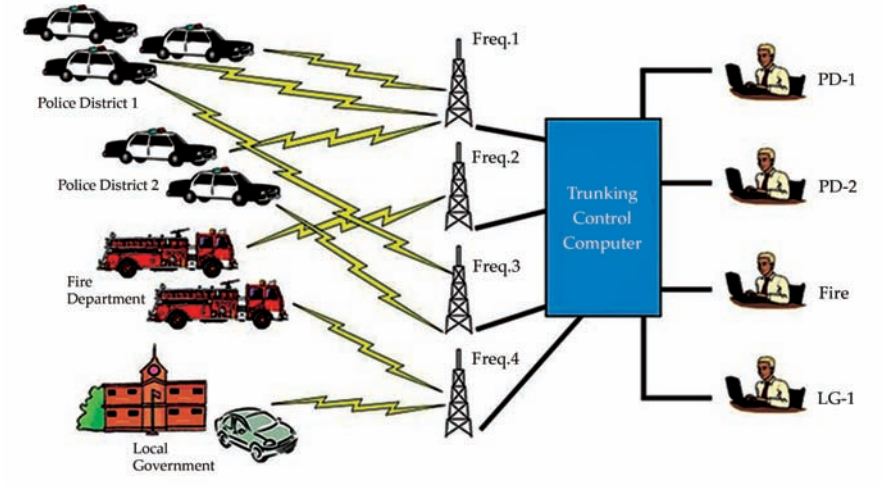


Figure 2.2: multipath diminishing

Multipath Diminishing

Two or more different paths are taken in multipath diminishing by the signal, because of reflections, may incur the signal to cancel out at sure positions, and to be tougher in other places.

Concealed Node Issue

The concealed node issue happens in different kinds of network if a node is noticeable from a wireless access point (AP), while not from other nodes collaborating with that access point. This results to problems in media access control.

Shared Resource Problem

The wireless network is an inadequate source. This is shared by all nodes in the variety of its sources. The allocation of bandwidth turns out to be multifaceted with several participating users.

Every so often users are not conscious that marketed numbers for instance, IEEE 802.11 equipment or LTE networks. These are not in their measurements, but these are collective with all other users.

Therefore, the individual user rate is very low. As the demand is increasing, the volume crisis is additionally probable to occur. The alternative solution is the User-in-the-loop (UIL) where updating to latest technology is for over-provisioning.

Capability

Comprehending single input single output (SISO), single input multiple output(SIMO), multiple input single output(MISO), multiple input multiple output(MIMO) and by means of multiple antennas and conveying in separate frequency channels can decrease declining, and can importantly rise the capability of system.

Shannon's theorem can define the data rate of maximum level data rate of any individual wireless link, which connects to the bandwidth in hertz and to the sound on the channel.

It can critically rise the capacity of channel by making use of MIMO techniques, for instance false generation of noise, and other techniques, where numerous aerials or multiple frequencies can utilize manifold paths to the receiver to attain much advanced throughout by a feature of the product of the frequency and aerial diversity at each end. While under Linux, the channel settings are controlled by Central Regulatory Domain Agent (CRDA).

Network



Figure 2.3: Network bandwidth

The over-all network bandwidth be contingent on the way of dispersion of the medium is, as additional dispersive medium commonly has advanced total bandwidth as it minimizes intervention.

This is dependent on the amount of available frequencies, the level of noise these frequencies create, the number of aerials taken into use and also if a directional antenna is in usage, if nodes employ power control and so on.

Mostly, there are only two bands for now 2.4 GHz and 5 GHz. Generally, 5 GHz band offers improved connection and speed.

Cellular wireless networks usually have decent dimensions, because of their usage of guiding aerials, and their capability to reprocess radio channels in non-neighboring cells.

Moreover, cells can be created very small by means of low power transmitters. This is in usage in cities to offer network capacity that balances linearly with population density.

Security



Figure 2.4: security to wireless network

The secrecy method of cryptography can be used in communication networks which can be taken into use to guard the communicated information from being retrieved by unlawful users.

Additional level of secrecy is attained when concealed communication is recognized, where the presence of the communication is covered from the opponent.

Safety

Wireless access points are also frequently near to humans, however the drop off in influence over distance is dissolute, subsequent to the inverse-square law.



Figure 2.5: Cyber security

The location of the United Kingdom's Health Protection Agency (HPA) is that "radio frequency (RF) exposures from Wi-Fi are expected to be lower than those from mobile phones." It also saw "no reason why schools and others should not use Wi-Fi equipment."

In October 2007, the HPA launched a new "systematic" study into the effects of Wi-Fi networks on behalf of the UK government, in order to calm fears that had appeared in the media in a recent period up to that time".

Dr. Michael Clark, of the HPA, says published research on mobile phones and poles does not enhance up to an impeachment of Wi-Fi.

PERFORMANCE FUNDAMENTALS OF WIRELESS NETWORKS

As a coin has two sides, everything comes with both pros and cons. So, almost all types of wireless technology have many drawbacks and restrains. Each and every communication method have an extreme channel capacity even though specific technologies of wireless are being utilized which can be easily determined by the following principles.

In fact, disregarding the technology which is used, Claude E. Shannon provided us an explicit mathematical formula to find channel capacity which is the rate of maximum information.

This channel capacity formula contains all the important information which is required to understand the performance of almost all the wireless networks even though the formula is very simple.

The two essential restrains are the amount of bandwidth which is available and the strength of signals among the sender and acceptor which are affecting the attainable data rates regardless of the acronym, name or the revision number of the specification.

Bandwidth

Radio communication can be achieved by using a shared medium which can be either radio waves or electromagnetic waves based on the preference.

Radio communication has its own nature which is totally different from this tethering world where every network peer has a dedicated wire running through it. For the communication to occur properly a precise range has to be decided.

Moreover, both the sender and receiver must approve of that range so that information is smoothly exchanged between the devices.

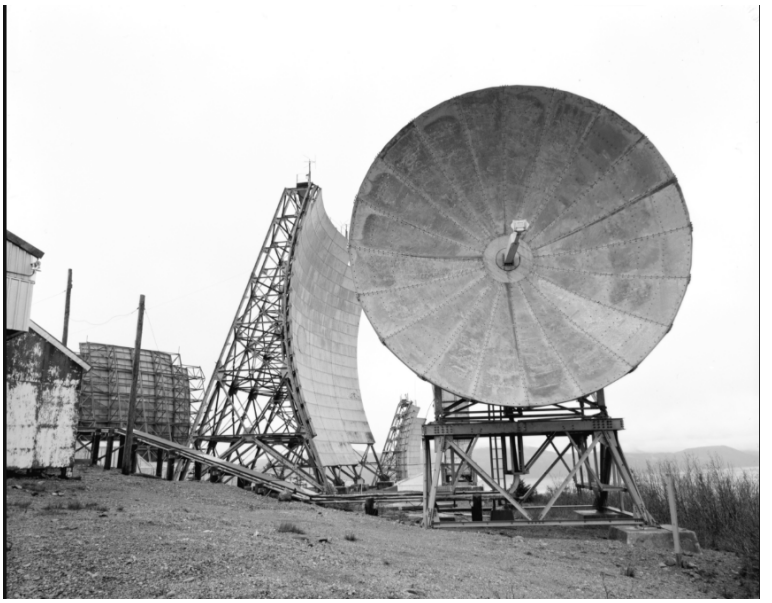


Figure 2.6: radio communication from one place to another

For instance, both the 802.11b and 802.11g standards utilize the 2.4–2.5 GHz band for all the devices which are wireless.

The range of frequency and its allotments are determined by the local government. (fig 5.1) However, this process in the United States is determined by the Federal Communications Commission (FCC).

Few wireless networks may work in some parts of the world but the same networks don't work in others due to the difference in the regulations opposed by the government.

So due to this different spectrum ranges are often assigned to the similar wireless technology by distinctive countries.

Keeping the politics aside, even though common bands are assigned for exchanging the information between the devices, the size of the assigned frequency range is still the most essential factor for finding the performance.

It is shown by Shannon's model that "the overall channel bitrate is directly proportional to the assigned range". Therefore, when all the others are equal, the rate of data will be twice automatically when the frequency range is doubled. For instance, increase in bandwidth from 20 to 40 MHz wills double the channel data rate which is the exact reason how 802.11n is taking a step ahead in improving its performance from the initially used standards of Wi-fi.

It can be noted from the above discussion that different performances are obtained from every frequency range.

Low-frequency signals require bigger antennas and more patrons competing for access, only then signals will travel far in order to cover the larger areas which are called as macro cells.

Whereas, high frequency signals require large infrastructure to transfer more data but these high frequency signals don't travel as far as low frequency signals which results lesser area to be covered and it is known as microcells.

Signal Power

Another limiting factor that restrains the wireless communication other than bandwidth is the strength of the signals among the sender and receiver which is also called as the signal-power-to-noise-power, S/N ratio, or SNR.

Additionally, the level of the desired signal is compared to the level of the background interference and noise with the aid of SNR. The signal has to be strong enough to carry the data as the amount of background noise is humongous.

Radio communication due to its nature is performed on a medium that is shared with other devices and these devices often leads to the generation of undesirable interference.

To illustrate, cross-standard interference is formed when a microwave oven working at 2.5 GHz may intersect with the frequency range utilized by Wi-Fi.

Not only this, other Wi-Fi devices such as the access point of neighboring Wi-Fi and also the coworker's laptop using the same Wi-Fi network generate a lot disturbance for the transmissions. Ideally, it is possible that there can be only one user in a particular range of frequency without any background noise or interference. But this case is unlikely due to two reasons. Firstly, there is insufficient bandwidth and secondly there are excessive numbers of devices for it to work properly.

There are two options to achieve the data rate which is desired in the presence of interference. The foremost step is that the transmit power can be increased which will increase the strength of the signal. And the other option is that the distance between the sender and receiver can be decreased or both the options can be done to get the desired data rate. In fact, there are two essential effects illustrated by this scenario:

Near-far problem

It is a condition in which it is impossible for the receiver to discover a weaker signal and can only detect the signals which are strong. Thereby "crowding out" the weaker signals effectively.

Cell-breathing

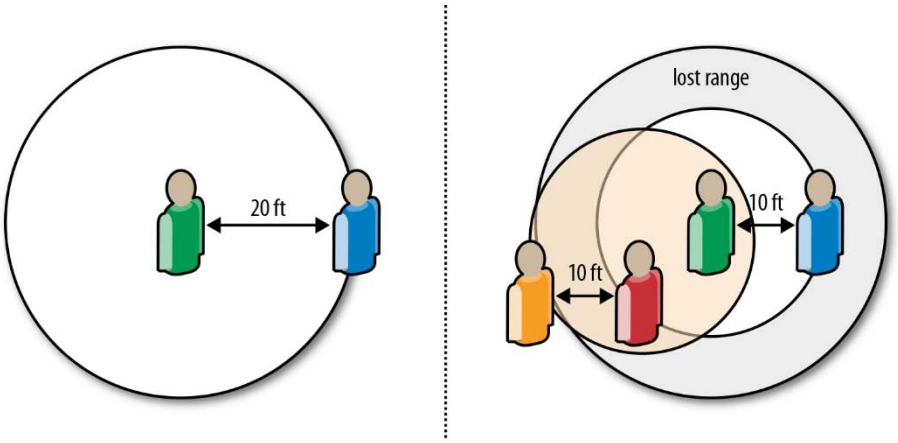


Figure 2.7: cell breathing

A condition in which both accumulative noise and interference levels leads to the shrinkage or expansion of the coverage area or the distance of the signal.

The near-far problem is that the weaker signals are blocked from reaching far due to the presence of more than one speaker near the person. Similarly, higher interference is caused due to the presence of large number of other conversations being used near-by which automatically decrease the range from which useful signals can be detected.



Figure 2.8: communication through cell breathing

And this is known as cell breathing. Regardless of underlying technology or protocol, these same limitations are present in all kinds of radio communication as well.

Modulation

The two main physical factors that control the capacity of all the wireless channels are the signal-power-to-noise-power, S/N ratio, or SNR and the available bandwidth. However, the signals which are encoded by the algorithm can also have a significant effect.

So, to hammer the nail in the wall, the binary codes i.e. 1's and 2's have to be converted into an analog signal which is radio waves. Modulation is the process which is used to convert the digital signals into analog signals.

And, there is requirement of different "modulation alphabet" which can be used to encode the digital signal with varying effectiveness. Moreover, the final output of the channel is then determined by the combination of both the alphabet and the symbol rate. To illustrate:

- 1,000 pulses or symbols per second (1,000 baud) can be processed by both the receiver and sender.
- The chosen alphabets determine each transmitted symbol which represents a different bit-sequence. (e.g., 2-bit alphabet: 00, 01, 10, 11).
- The rate of the bit for each channel is 1,000 baud × 2 bits per symbol, or 2,000 bits per second.

Computing power of both the receiver and sender, available technology as well as the SNR ratio are the three main factors on which the choice of the modulation algorithm is dependent. "A higher-order modulation alphabet comes at a cost of reduced robustness to noise and interference—there is no free lunch!"

MEASURING REAL-WORLD WIRELESS PERFORMANCE

There are mainly a small number of well-known parameters which are fundamentally restraining the performance of any wireless network regardless of the acronym, name or the revision number of the specification.

Namely, the amount of the available bandwidth and the signal-power-to-noise-power, S/N ratio, or SNR between the sender and the receiver. Furthermore, all radio-based communication is:

- Performed over a communication medium which is shared (radio waves)
- Specific bandwidth frequency ranges are regulated for usage.
- Modulated to use specific rates of transmit power.
- Subject to constant changing background noise and disturbance.
- Subject to technical limitation of the chosen wireless technology
- Subject to restrains of the device: power, form factor, etc.

All wireless technologies always declare a maximum or a peak data rate. For instance, the 802.11g standard is capable of 54Mbit/s whereas 802.11n standard elevate the bar up to 600Mbit/s.

Also, few mobile carriers are capable of 100+ Mbit/s output with LTE. However, when all the numbers are analyzed, the most essential factor that is often neglected is the significance on the ideal conditions.

The ideal conditions are the amount of available bandwidth, minimal or no background noise, the usage of frequency spectrum exclusively, maximum-throughput modulation alphabet, and, increasingly multiple radio streams (multiple-input and multiple-output, or MIMO) which are transmitting in parallel.

It is not that important to mention but whatever is shown on the label is totally opposite of the experience in the real world. Following are the few factors which are affecting the performance of all the wireless networks:

- The distance between receiver and sender
- The quantity of the background noise in the present location
- The consignment of disturbances created by the users who are using the same network.
- Also, the amount of interference created by the users who are using other or close-by networks which is called as inter-cell.
- The strength of allocated transmit power, both at sender and receiver.
- The chosen modulation scheme and the amount of processing power.

In other words, to obtain the maximum output, then following points should be taken care of.

- Try to cut short all the noise and interference that can be controlled.
- Try to keep the receiver and sender as near as possible.

- Try giving the desired power to the sender and receiver.
- Best modulation method should be selected by both the sender and receiver.
- And if the performance is not acceptable, then a wire has to be connected between the sender and the receiver. The luxury of utilizing the wireless communication does have its cost.



Figure 2.9: wireless networking

Calculating the performance of wireless communication is not an easy task. Due to the nature of radio communication, the performance of the wireless is highly variable. For instance, even a small change on the order of few inches can influence the output to be doubled in the area where the receiver is present. Whilst, a few instants later the output turns out to be half again as another receiver have started using and competing for access to the radio channel.

WIRELESS TECHNOLOGY STANDARDS

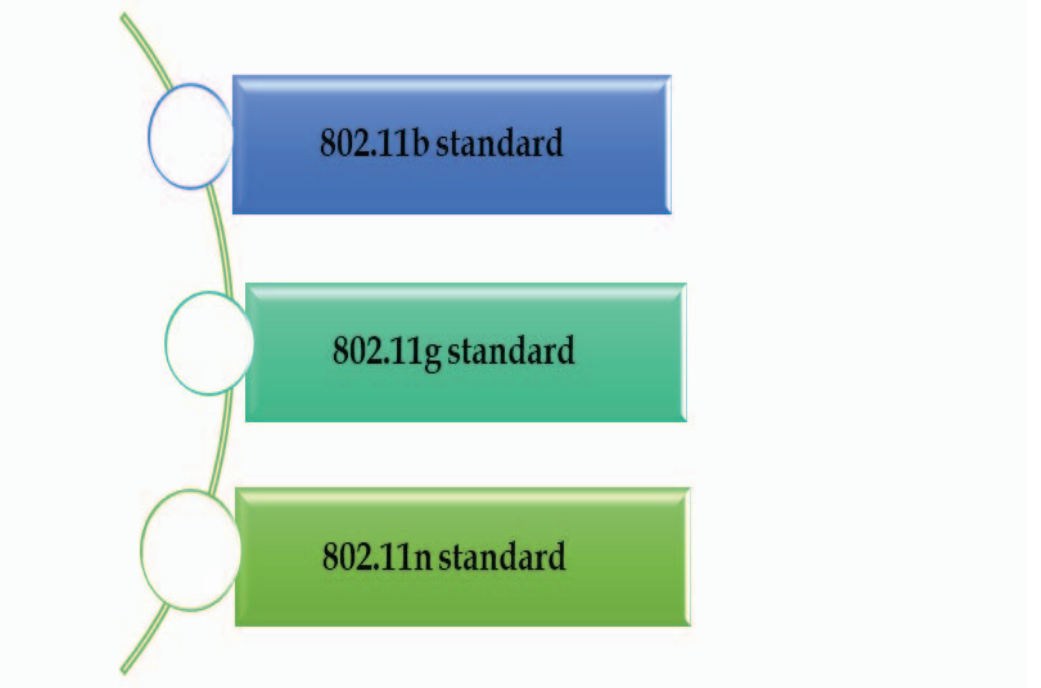


Figure 2.10: standards of wireless technology

There are numerous technology standards available for wireless networking and the patrons must ensure to find out which one will suit their requirements before buying the equipment. The most familiar wireless technology standards are as follows:

- 802.11b: This first appeared almost a decade ago and it is still in use. Moreover, it is the first widely used wireless networking technology which is known as 802.11b. And more commonly it is known as Wi-Fi.
- 802.11g: It is the foremost used wireless networking technology today. In 2003, a follow-on version called 802.11g debuted and offered better performance i.e. range and speed both.
- 802.11n: This standard is still under progress and is expected to be complete in 2009. It is another improved standard called 802.11n and regardless of the fact that this standard is yet to be finalized, the patrons can still buy devices based on 802.11n standard as it can be upgraded later to the final standard.

All the products based on these Wi-Fi variants (802.11b, g and n) are designed to be reconcilable with each other and they all use the same radio frequency i.e. 2.4 GHz so that the users can use the devices within the same wireless network based on the different standards.

However, doing this have a lot of effect on the overall performance of the network as special configuration is required to accommodate the earlier devices.

Ideally in this scenario, if possible the users will want that all the wireless devices, the computers which are wireless and the access points to be from same dealer and should be using the same standards of technology.

WIRELESS SPEED & RANGE

The wireless network devices which are available in the market, they always have the performance figures quoted i.e. the speed at which the data is transmitted based on the standards used by the wireless network as well as the addition of any technological enhancements.

In reality, all the performance figures mentioned on these devices are almost positive.

The official declared peak speeds of 802.11b, 802.11g and 802.11n networks are 11, 54 and 270 megabits per second (Mbps) respectively, but these figures are simply not attainable in the real world.

Generally, it is assumed that the user will only get one-third of the quoted performance.

It is found from the above discussion that wireless network is also said to be a shared network which means that less data will be transmitted between the user and the receiver if the number of computers connected to a wireless access point are more.

Both the range and speed of wireless network vary greatly. For instance, 802.11b and g officially can cover over a distance of up to 328 feet indoors or 1,312 feet outdoors, but the key term used there is “up to”. But in reality, there is very rare chance that these mentioned numbers are attainable.

So, it is clear that closer the user is to the access point, the better, stronger and faster connection speed and signals can be achieved. The ambience in which it operates defines the range and speed of wireless network. Due to this, the topic of interference come into existence.

WIRELESS INTERFERENCE



Figure 2.11: Wi-Fi gadget range

All the forms of radio communication have to face the issue of interference and even a wireless network is no exception. The strength and consistency of a wireless network signal can be affected as distinctive types of building materials such as wood, concrete, metal drywall, glass and so on can absorb or reflect the radio waves.

Therefore, which means that the potential for interference is mainly great indoors. Similarly, devices like microwave ovens and some cordless phones operates on the same 2.4 frequency range as 802.11b/g/n which can cause interference.

AMAZING FACTS!!!

According to an in depth statistics, there are more than 1.6 billion social network users worldwide with more than 64% of internet users accessing social media services online. Moreover, social networking is one of the most popular ways for online users to spend their time, and a preferred way to stay in contact with friends and families.

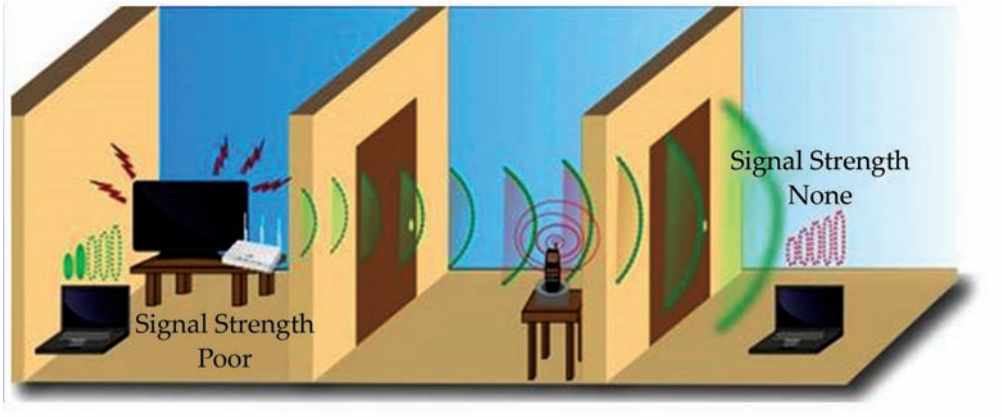


Figure 2.11: signal strength

It is very less likely that the interference can be avoided but in few cases, it is not strong enough to affect the usability of the network.

But if it does affect the usability then the user need to find the wireless networking hardware again or specialized antennas can be used to curtail the interference.

REVIEW QUESTIONS

1. What are the various problems that are being faced in wireless networking?
2. What are the performance fundamentals of wireless network?
3. How is the real—world wireless performance measured? Explain in brief.
4. Explain the various wireless technology standards.
5. Explain wireless interference with suitable real-time example.

CHAPTER 3

TYPES OF WIRELESS NETWORK

LEARNING OBJECTIVES

- Different types of wireless networks
- LAN, MAN and WAN at a glance
- Communication through satellites
- Mode of communication through WiMAX and Wi-Fi
- Advantages of wireless communication
- Disadvantages of wireless communication
- What is Bluetooth?
- What is ZigBee
- Different types of wireless data transmission
- Infrared and microwave mode of transmission
- Types of wireless devices like radio, wireless phones etc
- Advantages of wireless communication

INTRODUCTION

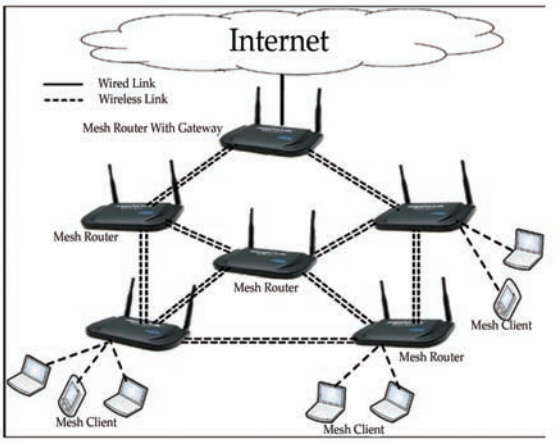


Figure 3.1: Wireless mesh network

With the emergence of wireless technologies nowadays, we have seen some serious encounter on the security breach in the wireless network. There are many measures to prevent the network managers which are looking forward to getting wireless network into the business hold. There are a lot of diversity in the opinion of incorporating wireless technology. There are many questions which arise while using the wireless network like why to adopt wireless network? How secure is our data in the wireless network? What are the threats related to wireless network? There is also an alternative network to support the flow of data which is through WEP (Wired Equivalent Privacy).

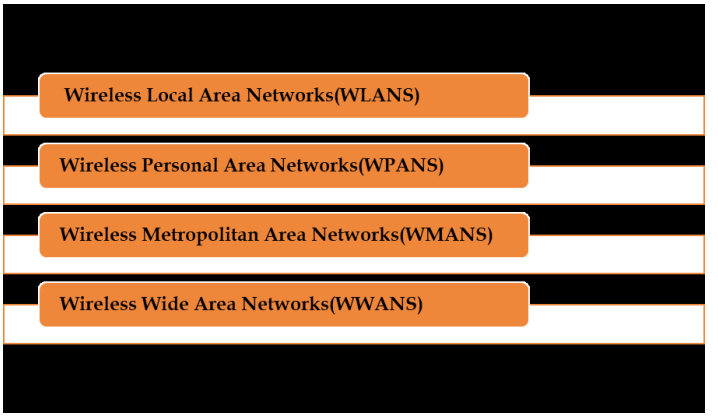


Figure 3.2: Types of wireless network

This technology is somehow the same thing, as you share the password for a network to all of your employees and you are never changing the password.

In some of the recent testing performed by the corporates says that if you are releasing 10 different enterprise based access points and eight different cards of clients then initialization of vector based attacks on WEP are no longer effective. There are several measures which are taken into consideration for the use of wireless network in business purposes.

There are many wireless security tools developed for the enterprise network managers which is used to prevent the data from being stolen or fetched.

As the security of the computer is important, in the same manner security of wi-fi is also equally important



Figure 3.3: storage area network

The personal information saved on wireless network can get leaked and anybody can access that. Anyone can misuse all the information saved on your wireless network.

The people connected on the wireless network can easily access the information and misuse that.

This may also result into the theft of identity and other nasty acts. Without the use of few tools the initialization of wireless network is not considered

as safe to use as these tools use to encrypt the data into other formats and then which giving output to it again decrypt it and execute.

But, without these tools one is considered in the dark for the wireless data speeds which has begun to surround the network.

In this wireless network security purpose, standardization has been set up by the IEEE (Institute of Electrical and Electronics Engineers) which takes all the security measures needed for the wireless network.



Figure 3.4: IEEE logo

This standard helps the data to circle up the authentication for the running technology which helps to resolve the basic wireless security problems.

There is another option which can be opted in order to overcome this problem which is use of Virtual Private Network (VPN) or you can treat the wireless users the same way VPN clients of remote access are being treated.

Today, the use of wireless network which feature comprehensive security capabilities and networks are properly protected such that the enterprises can rely on the network and further they can confidently take advantage of the services offered.

Wireless network makes people able to interact and access information easily. All this is without a wired technology.

Wireless networking offers freedom of movement.

Wireless networking enables development of skill to spread applications to diverse parts of a building, city, or approximately everywhere in the world.

This allows people to communicate with the help of mails and surf the internet from the places which they give preference to.

There are different types of wireless communication which exists in the system. However, distinctive trait of a wireless network is that communication occurs among computer devices.

The devices which are included in this are personal digital assistants (PDAs), printers, laptops, servers, and personal computers (PCs). Processors and memory along with a method to interface with a specific kind of network is inbuilt in the Computer devices.

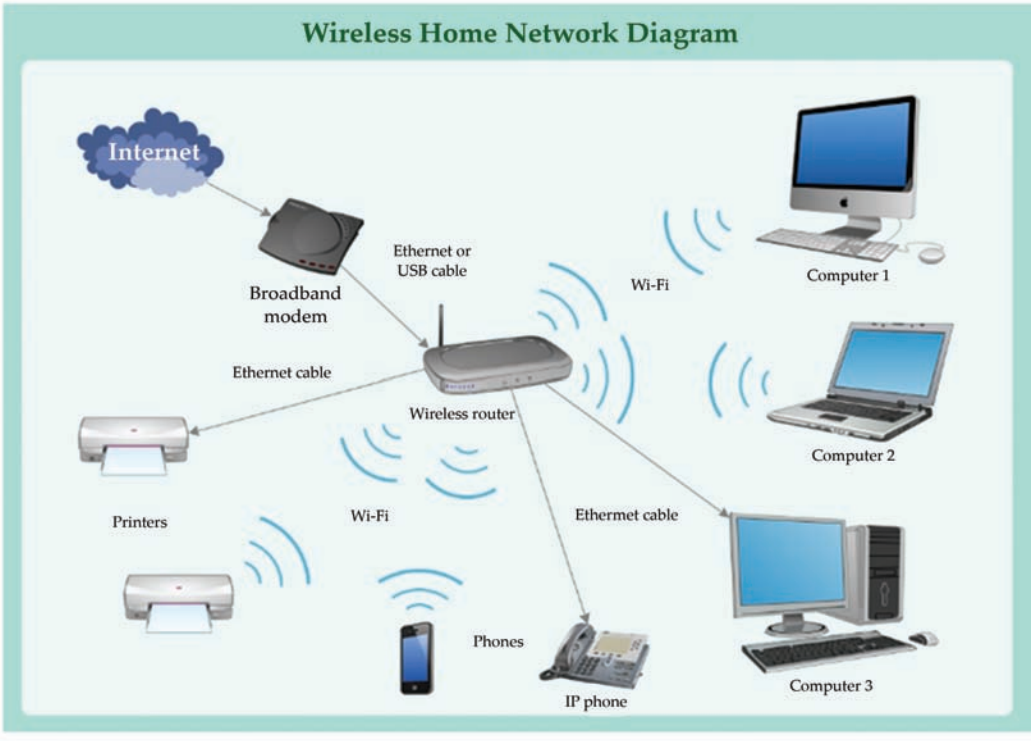


Figure 3.5: wireless connection of different devices

Conventional cell phones don't fall within the definition of a computer device; however, newer phones and even audio headsets are beginning to incorporate computing power and network adapters. Eventually, most electronics will offer wireless network connections.

As with networks based on wire, or optical fiber, wireless networks convey information between computer devices. The information can take the form of e-mail messages, web pages, and database records, streaming video or voice.

In most cases, wireless networks transfer data, such as e-mail messages and files, but advancements in the performance of wireless networks is enabling support for video and voice communications as well.

TYPES OF WIRELESS NETWORKS

- WLANS: Wireless Local Area Networks

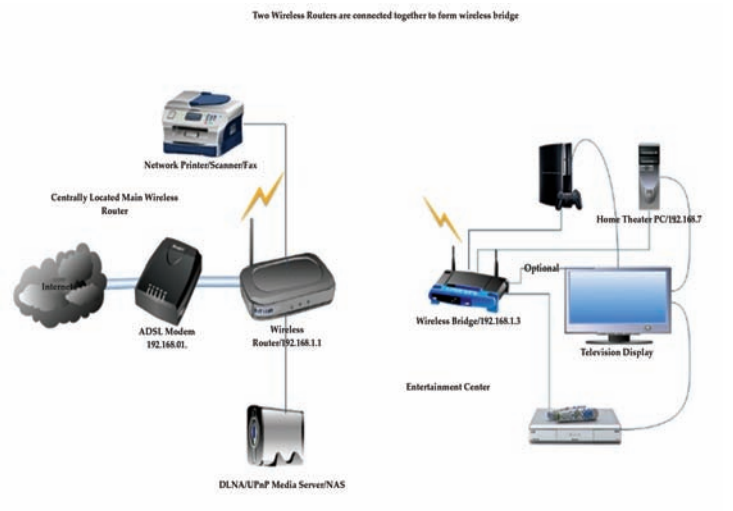


Figure 3.6: connected to home through wireless network

WLANS permits users in a neighboring area, for instance office campus or university campus or library, to develop a network or attain access to the internet. A small number of users can form a small network which does not require the access point. It is also mandatory that they do not require access to network resources.

- WPANS: Wireless Personal Area Networks



Figure 3.7: home technology

Two technologies which are the most recent ones are for wireless personal area networks are InfraRed (IR) and Bluetooth (IEEE 802.15). These technologies will permit the personal devices within a specific area of about 30 feet to connect with each other. Though, InfraRed necessitates a straight line of site and the range is very less.

- WMANS: Wireless Metropolitan Area Networks



Figure 3.8: mobile phone

WMANS i.e. wireless metropolitan area networks allows the connectivity of numerous networks in a metropolitan region, for instance, separate buildings in a city, which can be an alternate or holdup to laying copper or fiber cabling.

- WWANS: Wireless Wide Area Networks

This type of network can be upheld over large areas, such as towns or countries, through multiple satellite systems or antenna sites observed after by an Internet Service Provider. The systems of these types are known as 2nd Generation systems or 2G systems.

In current days, the wireless communication technology has evolved to turn out to be an essential part of quite a few types of communication devices.

As this lets the users to interact from the remote areas as well. The type of devices used in this type of wireless networking are, GPS units, mobiles, wireless computer parts, ZigBee technology and satellite television, cordless telephones etc.

TYPES OF COMMUNICATION TECHNOLOGIES

- Satellite

One of the most widespread wireless technology which is Satellite communication. This allows its users to interconnect with anyone anywhere in the world or even earth. People are connected to each other virtually. In this mode of communication, the used satellites communicate straight from the orbits with the help of radio signals.

The broadcasting abilities in portable satellite phones and modems are more than the cellular devices. Portable satellite phones have higher range than the cellular network phones. However, they are costlier as well than the cellular phones. Also, they are not easily available in the market.

For instance, for equipping a ship by satellite communication, an old-style communication system is connected to alone satellite, which permits many users to part the same broadcast equipment.

DID YOU KNOW

In 2014, Gartner predicted that by 2020 there would be 25 billion connected devices in a network. Cisco predicated that number would be closer to 50 billion, and Morgan Stanley thinks 75 billion.



Figure 3.9: types of wireless technology

- WiMAX

The wireless networking system where the broadband systems provide quick surfing of web without any connections with the cables. They are not connected

by any cable or DSL. One of the examples of wireless broadband is WiMAX.

Though WiMAX can possibly distribute data rates of more than 30 Megabits per second, until now, the range provided by the providers is 0 data rates of 6 Mbps. They even deliver less than that, while creating the service to be importantly sluggish than the wired broadband.

The real cost of data which is available using WiMAX extensively differs with the distance from the transmitter. WiMAX is correspondingly one of the versions of 4G wireless network which is available in phones as Sprint's 4G technology.

- Wi-Fi

The technologies involved in the wireless networking link different computers, systems and devices to each other and without the involvement of any cables. This is a wireless local area network area which is also referred to as Wi-Fi.

The low power way of communication which is used by various electronic devices such as smart phones, laptops, systems etc. is referred to as Wi-Fi. A wireless router acts as a hub for communication in a Wi-Fi setup.

The networks over Wi-Fi are enormously restricted in range as due to low power of transmissions which allows only users to link or connect within the close range to the router or signal repeater. Wi-Fi is very common in-home networking applications which offer portability without the requirement of any cables.

The networks of Wi-Fi are required to be protected with passwords for security reasons in manner to not to be accessed by others. There are certain advantages and disadvantages of this type of wireless network which are discussed below.

Advantages

Ease of Incorporation and Handiness

As this type of network is wireless, this allows users to access the resources of network from any easy and convenient. This type of networking makes the communication handy.

Flexibility

Due to the evolution and emergence of public wireless networks, access to internet from users is now even offered the exteriors of usual working hours.

Scope

Wi-Fi as a kind of wireless networks are accomplished of helping an unexpectedly enlarged number of clients with the current equipment, while in a wired network setup, extra clients necessitate extra wiring.

Disadvantages

1. At times, these Wi-Fi networks are not looked-for, for various number of reasons.
2. This type of networks such as radio frequency transmission and wireless networking signals are bound to come across various types of interference together with the complex broadcast effects which are outside the regulation of the network administrator.
3. There is definitely a threat to security in the wireless networks as they may require some of the several encryption technologies.
4. Range will be inadequate for a larger structure: the range provided by these technologies is low as in order to rise its range, users may have to buy repeaters or additional access points.
5. The speed provided on maximum wireless networks is slower than the slowest public wired networks.
6. Fitting of an infrastructure-based wireless network is a complex process to set up.

Bluetooth Technology

Bluetooth technology lets users to link a variety of different electronic devices wirelessly to a system for the transference and distribution of data. This is the major function Bluetooth.

Cell phones are linked to hands-free earpieces, wireless keyboard, mouse and mike to laptops with the assistance of Bluetooth as it conveys data from one device to another device.



Figure 3.10: connecting different devices through Bluetooth

Bluetooth technology has several functions, and it is taken into use mostly in wireless communications' market. It has certain features and aspects which are mentioned below:

1. Radio waves are used for communication between devices the Bluetooth technology. Majority of the radio waves mentioned above have a range of 15-50 feet.
2. Bluetooth are said to be using low power signal by official Bluetooth website. This uses low power with an extreme range of 50 feet with adequate speed to allow communication of data.
3. The pairing process identifies and connects any two devices to each other. It also prevents interference from other non-paired Bluetooth devices in the area.
4. It uses maximum power only when it is required, thus preserving battery life.

ZigBee

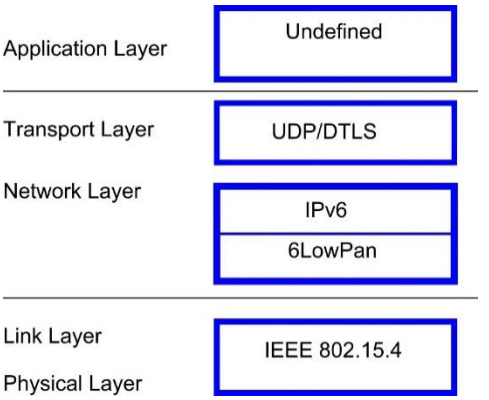


Figure 3.11: ZIGBEE protocol

To address the exclusive requirements of low-power, low cost wireless sensor, and control networks, ZigBee as a wireless communication is designed



Figure 3.12: wireless network hub

This is a technology which can be taken into use by anyone, anywhere in the world. It is very easy to execute and just necessitates a little power to function.

This has been designed by keeping in mind the requirements of the communication of data with unpretentious structure similar to the data

from the sensors. Certain features of this technology are discussed in the following:

1. These wireless networking system is structured to cater to the need of low power consumption.
2. This type of wireless networking is taken into use in Commercial Applications like sensing and monitoring applications.
3. They use very low power and have enormously long device battery life.
4. They offer elasticity to cater extra with the dependable wireless performance and battery operation.

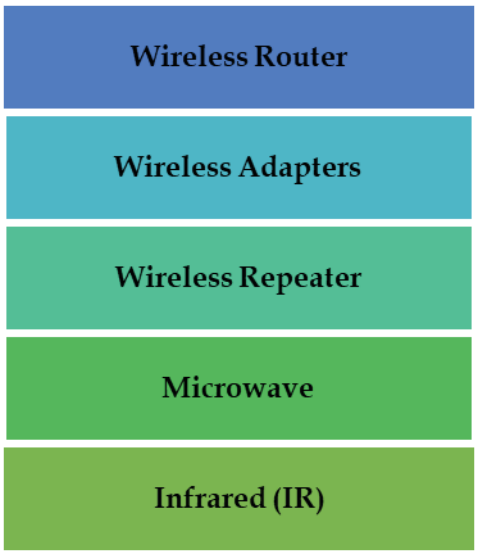


Figure 3.13: types of wireless devices

TYPES OF WIRELESS DATA TRANSMISSION

The electronic devices which communicate without cables in air while making use of radio frequency are known as wireless technology. The technology which is used in different modern device and offers better mobility are known as the Wireless technology. The devices of wireless technology play the major role in voice and Internet communications.

Wireless Router



Figure 3.14: wireless router

The device which receives an inward Internet connection and directs the data as radio frequency signals to other wireless devices that are in the range of the router are known as wireless routers.

A network which is fitted with a wireless router is referred to as a wireless local area network (WLAN). There are several routers that in-built features of security firewalls which help them safeguard devices linked to the router counter to malevolent data such as computer viruses.

A wireless device which is used in many homes to link their devices to the internet.

Wireless Adapters



Figure 3.15: adapter

The hardware devices which are installed in the computers are known as wireless adapters. These are the devices that enables wireless connectivity. When a computer is lacking a wireless adapter, it will not be possible for it to connect with a router to access the Internet.

There are computers that have wireless adapters in-built into their motherboard, despite the fact, it is also likely to connect separate wireless adapters to enhance wireless competence to a computer that doesn't have an in-built facility.

Wireless Repeater



Figure 3.16: broadband router



Figure 3.17: wi-fi repeater

The wireless networking device which extends the range of a wireless router is known as a wireless repeater.

A wireless repeater accepts wireless signals and magnifies the strength of the signals, and at that point re-emits them.



Figure 3.18: wireless repeater

By positioning a repeater between the router and connected computer, the strength of signal can be improved.

Microwave



Figure 3.19: microwave transmitter

A very effective and efficient type of wireless data broadcast which sends information by making use of two different methods is referred to as Microwave.

The method that used to send by making use of wireless media of a microwave is known as satellite method which transfers data via a satellite. This orbits 22,300 miles above the Earth.

Ground stations are responsible for sending and receiving data signals to and from the satellite with a frequency in the range of 11 GHz to 14 GHz and with a transmission speed of 1 Mbps to

10 Mbps. Additional method is an earthly method.

In this method, two microwave towers with a strong and clear line of sight amid them are taken into use for making sure that there are no hindrances to disturb that line of sight. It is used very frequently for the purpose of privacy.

The data transfer frequency for terrestrial systems is characteristically 4 GHz to 6 GHz or 21 GHz to 23 GHz, and the speed is typically 1 megabit per second Mbps to 10 Mbps.

Infrared (IR)

The media transmission system which communicates signal of data by light releasing diodes or lasers are known as Infrared.

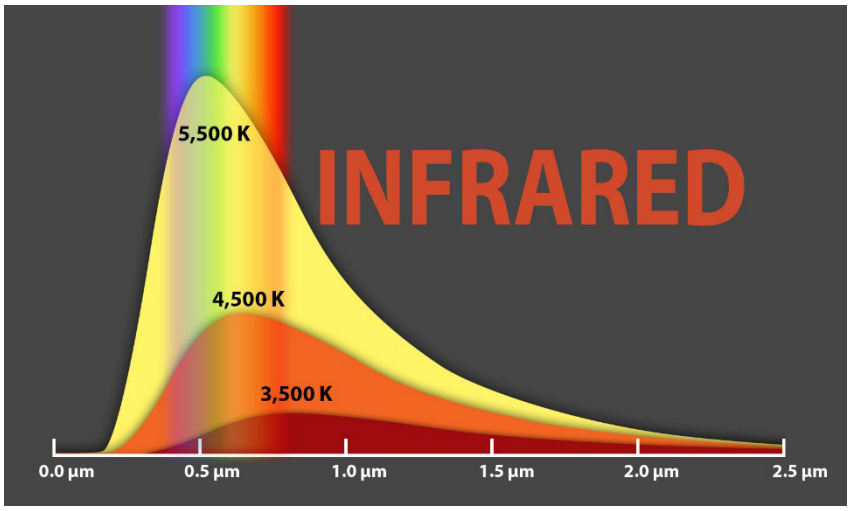


Figure 3.20: infrared waves

Infrared is an electromagnetic energy at a wavelength which is longer than that of the red light. The information cannot be travelled through obstacles in an infrared system, however it can be withdrawn by light.

Another type of infrared technology is point to point structure in which broadcast is probable only amongst two points restricted to a range and line of sight.

The frequency of signal to communicate in a point to point system is 100 GHz to 1,000 terahertz (THz). The range of speed is from 100 Kbps to 16 Mbps. Alternative way of transfer of infrared comprises the broadcast system. This method is an insightful method.

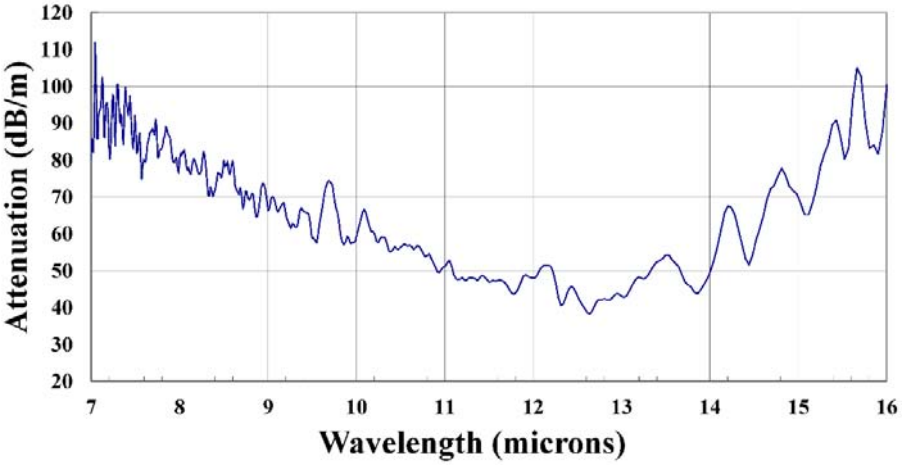


Figure 3.21: infrared transmission

In this method, transmission unit intensifies and retransmits a data signal to numerous other units. Infrared broadcast system has a normal frequency of 100 GHz to 1,000 THz with a restricted speed of 1 Mbps.

TYPES OF WIRELESS DEVICES

Radio

Another type of wireless devices is the radio system. Radio system is a type of wireless media device which transmits data by conveying electromagnetic waves with low frequencies to distant locations by an electrical conductor and an antenna.



Figure 3.22: old style radio

Many radio enthusiasts like Ham radio, transfer information and act as an emergency communication support in the time of disasters with the use of their influential incompetent broadcasting equipment.

They can even transmit the digital data over the radio spectrum.

For truckers and sailors, the mean of communication is provided by Citizen's band and maritime radios. The broadcast frequency for data transmitted over a radio system ranges from 10 kilohertz (kHz) to 1 gigahertz (GHz). These are controlled and monitored by the Federal Communications Commission (FCC).

Wireless Phones



Figure 3.23: wireless mobile phones

The development of cellular networks is computed over generations. There are several different users which communicate with each other transversely through a single frequency band by Cellular and cordless phones.

Another example of devices which make use of wireless signals is cellular and cordless phones



Figure 3.24: cellular mobile

Cell phones typically have a very high range while compared to the Cordless phones. The range of Cell phones is much larger than the local wireless networks due to the fact that all the cell phones use large telecommunication towers to make available cell phone coverage. There are certain number of phones which use signals from satellites to interconnect. This is similar system to that of Global Positioning System (GSP) devices.

Other Devices

Several other devices which use radio signal to interconnect can be taken as a wireless device. The most common example of this type of device is garage door openers, certain video game consoles, baby monitors and walkie-talkies.



Figure 3.25: video games

All these devices use the wireless networking technology.



Figure 3.26: walkie talkie

Communication using wireless technology come across several advantages and disadvantages. These are discussed below:

ROLE MODEL: DAVID SARNOFF

David Sarnoff was an American businessman and pioneer of American radio and television. As a boy in Russia, Sarnoff spent several years preparing for a career as a Jewish scholar of the Talmud. He immigrated with his family in 1900 and settled in New York City. While going to school, he helped support the family by selling newspapers, running errands, and singing the liturgy in a synagogue. In 1906 he left school to become a messenger boy for a telegraph company and with his first money bought a telegraph instrument. He soon became proficient in Morse operation and found work as a radio operator for the Marconi Wireless Telegraph Company of America (also called American Marconi), where he became a protégé of radio inventor Guglielmo Marconi. Throughout most of his career he led the Radio Corporation of America(RCA) in various capacities from shortly after its founding in 1919 until his retirement in 1970.

He ruled over an ever-growing telecommunications and media empire that included both RCA and NBC, and became one of the largest companies in the world. Named a Reserve Brigadier General of the Signal Corps in 1945, Sarnoff thereafter was widely known as "The General."

Sarnoff is credited with Sarnoff's law, which states that the value of a broadcast network is proportional to the number of viewers.

Over the 13 years, Sarnoff rose from office boy to commercial manager of the company, learning about the technology and the business of electronic communications on the job and in libraries. He also served at Marconi stations on ships and posts on Siasconset, Nantucket and the New York Wanamaker Department Store. In 1911, he installed and operated the wireless equipment on a ship hunting seals off Newfoundland and Labrador, and used the technology to relay the first remote medical diagnosis from the ship's doctor to a radio operator at Belle Isle with an infected tooth.

The following year, he led two other operators at the Wanamaker station in an effort to confirm the fate of the Titanic. Sarnoff later exaggerated his role as the sole hero who stayed by his telegraph key for three days to receive information on the Titanic's survivors. The event began on a Sunday, when the store would have been closed. Some researchers question whether Sarnoff was at the telegraph key at all. By the time of the Titanic disaster in 1912, Sarnoff was a manager of the telegraphers.

When America entered World War I in 1917, Sarnoff attempted to enlist in the navy and then the army, but he was turned away because of his prominent role at American Marconi, which was a key supplier of radio equipment to the navy. To keep American radio technology from being controlled by foreign-owned companies like American Marconi, that company was absorbed by a new company, the Radio Corporation of America (RCA), in 1919. Sarnoff was RCA's commercial manager.

In 1920 Sarnoff reiterated his "radio music box" memo and was given a small amount of money to develop a radio prototype. As RCA's new general manager, he demonstrated radio's market potential by broadcasting the boxing match between Jack Dempsey and Georges Carpentier (July 2, 1921); the broadcast created a sensation. Within three years RCA sold more than $80 million worth of receiving sets. In 1926 RCA formed the National Broadcasting Company (NBC).

The AT&T demonstrations in 1915 of long-distance wireless telephony inspired the first of many memos to his superiors on applications of current and future radio technologies. Sometime late in 1915 or in 1916 he proposed to the company's president, Edward J. Nally, that the company develop a "radio music box" for the "amateur" market of radio enthusiasts. Nally deferred on the proposal because of the expanded volume of business during World War I. Throughout the war years, Sarnoff remained Marconi's Commercial Manager, including oversight of the company's factory in Roselle Park, New Jersey.

Advantages

- Any data or information that can be carried or communicated rapidly with a high speed.
- Web can be surfed anytime anywhere in the world without the obstacle of carrying wires along. It also progresses easy access and improves the productivity.
- Wireless networking is very beneficial for the professional who are working in the remote locations such as Doctors, workers and other professionals. This enables them to remain in touch with the medical centers by using wireless communication.
- This helps in the cases of emergency situations where concerned people can be alarmed for help using the devices of wireless communication. The regions which require help, can get assistance with these alerts by wireless communication.
- Installation cost for the wireless networks are very less. The cost of maintenance in wireless networks is also comparatively lesser than the wired networks.

Disadvantages

- One of the main disadvantage of wireless devices is that any hacker can simply access the wireless signal spread in the air to get hold of all the data stored on the wireless network.
- The thing very significant is to protect the wireless network as the information cannot be exploited by unauthorized users. This also improves the danger of losing data or information.

DID YOU KNOW ?

Wi-Fi signals generally emit from your router in a doughnut shape. What a tasty thought.

AMAZING FACTS!!!

"Did you know that 80% of all cyber breaches take place as a result of weak passwords? Passwords that are easy to remember — like "12345," "abcdefg" and your name — are also easy for hackers to guess. By requiring your employees to create strong passwords, and by establishing a two-step login system, you can ward off a good chunk of potential threats to your network security systems."

Due to all these features, the fastest improving technology in telecommunication market is wireless networks. Bluetooth, Femtocell, Wi-Fi, WiMAX, and 4G are some of the most important values of Wireless technology for the next generations.

The technological progress which convey invisible electromagnetic waves to communicate data over longer distances within a short span of time is used by Radio, Mobiles, Internet, etc.



Interbrand invented the term “Hi-Fi” or “High Fidelity”. However, Wi-Fi doesn’t actually stand for anything.

REVIEW QUESTIONS

1. What are IEEE standards? Explain in detail.
2. What are the different types of wireless networks?
3. Explain different types of wireless communication technologies.
4. Differentiate between the advantages and disadvantages of wireless communication networking.
5. Differentiate between Bluetooth technology and ZigBee technology.
6. What are the different types of wireless communication?
7. Discuss the difference between Infrared and Microwave?
8. Explain various types of wireless communication devices.

CHAPTER 4

SECURITY MEASURES IN WIRELESS NETWORKING

LEARNING OBJECTIVES

- Security keys in wireless networks
- Introduction to WPA and WPA2
- Wired Equivalent Privacy at a glance
- Need for acronym
- Technologies in wireless network security
- What are the elements of wireless security
- Implementation of authentication mechanism for data transmission
- Securing the data with encryption
- Wireless security we are using today
- Standards of WPA and WPA2 based on security
- Different types of strategies on wireless security
- Captivation of applied steps in security
- Viewpoint of wireless network security technology

WIRELESS NETWORK SECURITY KEYS



Figure 4.1: security circle to wireless network

Wireless network security key is a type of network security key or passphrase that can assist in protecting the wireless network from any type of unlawful access. The setup of safeguarded Wi-Fi is simple and easy in Windows 7. There are set Up a Network wizard guide which can instruct individuals over set up of a security key.

In a situation where device is already configured, then the security key can be set up by visiting the Network and sharing center, given in the left pane, afterwards click on Manage Wireless networks. After that choose the network for which the configuration is needed. Then, click on properties and after that, click on Security tab and change the security key.



Figure 4.2: Security

WI FI PROTECTED ACCESS (WPA AND WPA2)

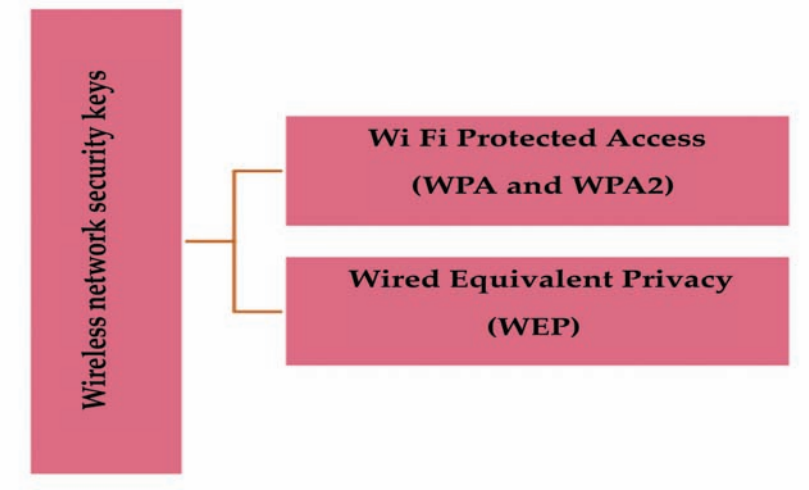


Figure 4.3: wireless network security keys

WPA and WPA2 necessitate operators to make available a security key to link. After the validation of the key, all data transmitted amongst the computer or device and the access point is encoded.

Always there are two kinds of WPA verification: WPA and WPA2. The one which is most secure is WPA2. Every user is provided the identical passphrase in WPA-Personal and WPA2-Personal. This is the suggested method for home networks.

WPA-Enterprise and WPA2-Enterprise are planned to be used with an 802.1x authentication server which allocates separate keys to every user. This method is chiefly used in work networks.

WIRED EQUIVALENT PRIVACY (WEP)

Table 4.1: Security objectives of computer

Computer Security Objectives	
• Confidentiality	• Data confidentiality • Assures that private or confidential information is not made available or disclosed to unauthorized individuals • Privacy • Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed
• Integrity	• Data integrity • Assures that information and programs are changed only in a specified and authorized manner • System integrity • Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system
• Availability	• Assures that systems work promptly and service is not denied to authorized users



Figure 4.4: coded security

The ancient security network which is accessible to back older devices is defined by WEP. However, this method is not suggested for use. after the enabling of WEP, the network security is set up.

This network security key encodes the data that one computer transmits to another computer over any network. Though, this WEP security is comparatively very simple to crack.

There are two types of WEP:

1. Open system authentication
2. Shared key authentication

Both the types of WEP are not secure. However, shared key authentication is the slightest secure of the two. Although a hacker can simply hack this by using some wireless network analysis tool.

Due to this reason, WEP shared key authentication is not backed by Windows 7 / 8.

If even after some of the individuals want to use the WEP then they can follow the below given steps:

To physically develop a network profile using WEP shared key authentication:

1. select the Network icon in Notification area and select the open Network and Sharing Center.
2. Select Set up a new connection or network.
3. Select manually link to a wireless network, and then click next.
4. On the Enter information for the wireless network you want to add page, under Security type, select WEP.
5. Select the rest of the page, and then click next.
6. Select Change connection settings.
7. Select the Security tab, and then, under Security type, click Shared.
8. Select OK, and then choose Close.

Even if the identification is required to secure the Wi-Fi network, then an individual will possibly discover that most of the security protocol abbreviations are a bit confusing.

WHY DOES THE LITTLE ACRONYM MATTER?

Everyone follow the instructions, they are given. People log into the router after they have purchased and plugged it in for the first time. they set the password as instructed.

However, it is essential to discover the need to know the meaning of the little acronym next to the security protocol chosen.

It is very significant. Due to the reason that the circumstance with all security standards, growing computer power and increased exposures have reduced older Wi-Fi standards at risk.

The network is private, data is private, when somebody hijacks any individual's network for their unlawful hijinks, police will come to the door of that individual.

The difference between providing somebody easy, simple access to personal home network is like difference between understanding security protocols and executing the utmost advanced one the router can support or else updating it when it cannot support recent most gen secure standards.

WEP, WPA, AND WPA2: WI-FI SECURITY OVER THE ERA



Figure 4.2: wireless IP cameras

From the past decade, Wi-Fi security protocols have experienced manifold advancements, with absolute deprecation of old protocols and important modification to latest protocols. A turn over the past of Wi-Fi security helps to highlight both whatever's available there right now and why any individual should evade old standards



Figure 4.3: wireless network security device

Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) is the most broadly taken into use Wi-Fi security protocol in the world. This is a meaning of age, backwards compatibility, and the circumstance that it seems initially in the protocol assortment menus in many router control panels.

Wi-Fi security standard is approved to WEP in September of 1999. The initial versions of WEP weren't chiefly durable, also for the time they were released. This was due to the reason that U.S. restrictions on the export of numerous cryptographic technology resulted to manufacturers limiting their devices to only 64-bit encryption.

It was improved to 128-bit after the restrictions were removed. Regardless of the overview of 256-bit WEP, 128-bit residues to be one of the most general applications.

In spite of modifications to the protocol and an improved key size, over time many security faults were revealed in the WEP standard. It is easier, simpler to crack the security and exploit these faults when the power of computing increases.

The FBI gave demo in manner to improve alertness of WEP's feebleness by 2005. In that public demo, they cracked WEP passwords in no time while taking use of freely accessible software.

It is highly vulnerable, in spite of several progresses, work-arounds, and extra efforts to support the WEP system. Systems that depend upon WEP should be advanced or, if security updates are not a choice, exchange. Officially Wi-Fi was retired by the Wi-Fi Alliance in 2004.

Wi-Fi Protected Access (WPA)

DID YOU KNOW ?

An article in Telematics wire predicts that by 2017, four out of five cars will have an Internet connection and send 25GB of data to the cloud per hour.

Wi-Fi Protected Access (WPA) was the Wi-Fi Grouping's straight answer and substitute to the progressively seeming weaknesses of the WEP standard. WPA was initially accepted in 2003, a year prior to when the WEP was formally suspended.

WPA-PSK (Pre-Shared Key) is the most general WPA configuration. The answers taken into use by WPA are 256-bit, an important rise over the 64-bit and 128-bit keys which is used in the WEP system.



Figure 4.4: security networking device

Many of the important variations executed with WPA comprised message integrity checks. These checks are to govern if an attacker had apprehended or changed packets approved between the access point, client and the Temporal Key Integrity Protocol (TKIP).

The fixed key system which is comparatively less secure than the a per-packet key system employed by TKIP. The TKIP encryption standard was after some time outdated by Advanced Encryption Standard (AES).

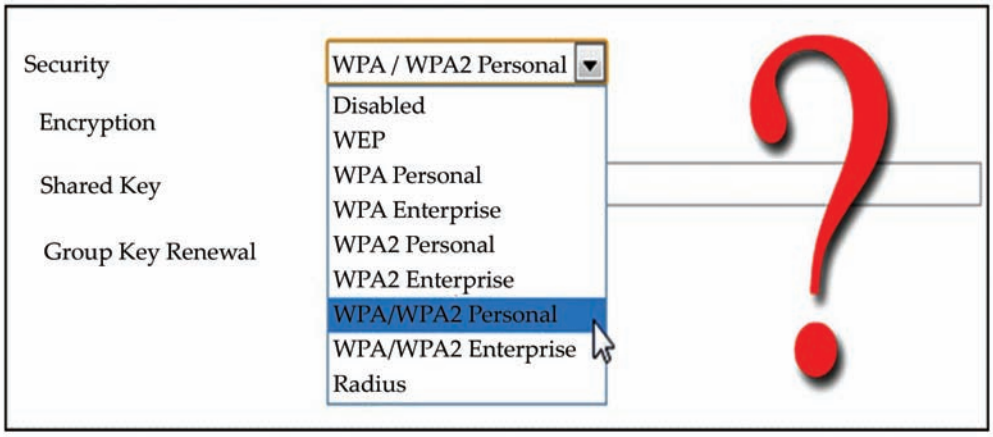


Figure 4.5: security settings

Regardless of important advancements in WPA over WEP, the duplicate copies of WEP keep on coming in way of WPA. A very important part of WPA is TKIP, which was structured to conveniently roll out via firmware advancements onto existing WEP-enabled devices. As such, it had to reprocess specific fundamentals that are taken into use in the WEP system which, eventually, were also oppressed.

Proof-of-concept and applied community demo has shown that WAP is also vulnerable to intrusion just like its predecessor WEP. Remarkably, there is no direct attack on WPA protocol to breach WPA.

However, there are attacks which have been efficaciously demonstrated. It was demonstrated by the attacks on an add-on system that was moved out with WPA: Wi-Fi Protected Setup (WPS) which was planned to make it laidback to connect devices to modern access points.

ROLE MODEL: JOHN O'SULLIVAN

Dr. John O'Sullivan is an Australian electrical engineer whose work in the application of Fourier transforms to radio astronomy led to his invention with colleagues of a core technology that made wireless LAN fast and reliable. O'Sullivan is accredited as one of the inventors of Wi-Fi. After Stephen Hawking introduced the idea that black holes might not be black, John O'Sullivan used his newly received PhD in electrical engineering to support Hawking radiation. While working with the equipment, O'Sullivan found ways to make processing data more effective and efficient through digital hardware, which led to the Wi-Fi that we use today. This technology was patented by CSIRO and forms part of the 802.11a, 802.11g and 802.11n Wi-Fi standards.

O'Sullivan received the CSIRO Chairman's Medal and the Australian Prime Minister's Prize for Science In 2009.

O'Sullivan and his team created chips for wireless connection and that's how the first WLAN was born. WLAN is short for a wireless local area network. WLAN links two or more devices using a wireless distribution method within a limited area such as a home, school, computer laboratory, or office building. This lets users move around within a local coverage area and still be connected to the network.

In 1977, Dr. John O'Sullivan co-authored a paper in the Journal of the Optical Society of America titled "Image sharpness, Fourier optics, and redundant-spacing interferometry" with J. P. Hamaker, and J. E. Noordam. In this paper, they presented a technique for sharpening and improving picture clarity in radio astronomy images.

The internet changed the world by allowing people to access information by one button. It eliminated major use of a library, newspapers, and hours of researching. It gave people a new way to communicate, allowing people all over the world to contact one another in an instant. In 1990, O'Sullivan "wanted to have a WLAN system that would be as powerful as the then existing cabled solutions." His idea was to speed up the transmission rates without the use of cables."

In the early 1990s, O'Sullivan led a team at the CSIRO which patented, in 1996, the use of a related technique for reducing multipath interference of radio signals transmitted for computer networking. This technology is a part of all recent WiFi implementations. As of April 2012, the CSIRO has

earned over $430 million in royalties and settlements arising from the use of this patent as part of the 802.11 standards with as much as a billion dollars expected after further lawsuits against other parties.

Highlights of research

- Achieved an eight-fold increase of the bandwidth processing capacity of the Westerbork Radio Telescope as project leader for the digital continuum backend receiver
- Participated in a series of innovative experiments to detect exploding black holes and other short time astronomical events
- Developed an intellectual underpinning for adaptive optics in light telescopes and redundant baseline interferometer in radio telescopes
- With Austek Microsystems created a fast Fourier transform computer chip. This VLSI chip consisted of 160,000 transistors and performed real time transforms at rates up to 2.5 Msamples/s
- Influential role in the system design for the Australia Telescope
- Led a CSIRO team comprising Graham Daniels, John Deane, Diethelm Ostry, Terry Percival who together invented a patented technology that uses fast Fourier transform and other techniques to enable fast, robust wireless networking in the home and office
- Led the system design for the world's first 802.11a (WiFi) chipset developed by Radiata Networks
- Over 40 scientific and technical papers at numerous industry conferences
- Granted 12 patents in the area of special purpose FFT processors, Wireless LANs and antennas
- Member of the Institute of Electrical and Electronics Engineers and Institute of Engineers Australia
- Member of international review committee for information and communications technologies in CSIRO
- Member of Australian Square Kilometer Array Consultative Committee
- Chair of the Mathematics, Information and Communication Sciences Expert Advisory Committee, Convener ICT Appraisal committee, 2004 CRC selection round
- Optical Society of America
- Board Director AAPT, Taggle Systems

WI-FI PROTECTED ACCESS II (WPA2)



Figure 4.6: encryption of security device

As of 2006, WPA has, has been formally outdated by WPA2. One of the most important variations between WPA and WPA2 is the obligatory use of AES algorithms and the overview of Counter Cipher Mode Protocol (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) as a substitute for TKIP.

Though, TKIP is till now well-looked-after in WPA2 as an emergency system and for the ability of computer systems or software to exchange and make use of information with WPA.

Presently, the primary security susceptibility to the real WPA2 system is an incomprehensible one.

It needs the attacker to have an easy access to the protected Wi-Fi network in manner to advance access to positive keys and then disseminate an attack in contradiction of other devices on the network.

Intrinsically, the security implications of the recognized WPA2 susceptibilities are restricted virtually completely to originality level networks and justify slight to no real thought in respect to home network security.

Inappropriately, the similar susceptibility that is the major hole in the WPA armor. The attack vector which leftovers in the latest WPA2 capable access points is through the Wi-Fi Protected Setup (WPS).

Though cracking into a WPA/WPA2 secured network while making use of this weakness necessitates wherever from 2-14 hours of continued effort with a current computer, yet it is a sincere security worry.

WPS should be incapacitated and, whenever probable, the firmware of the access point should be rushed to a distribution that doesn't even back WPS so the attack vector is totally detached.

Any individual may feel little confused or nervous at this point of time due to reason that any individual is positively making use of the top security protocol that are available for the Wi-Fi access point or individual has chosen WEP subsequently as it was at the top of the list.

Below given is the list of the recent Wi-Fi security methods which are obtainable on any modem from top to the lowest as of 2006:

1. WPA2 + AES
2. WPA + AES
3. WPA + TKIP/AES (there is TKIP as a contingency method)
4. WPA + TKIP
5. -WEP
6. Open Network (zero security)

Preferably, Wi-Fi Protected Setup (WPS) is deactivated and the router is set to WPA2 + AES.

The whole thing on the list is a fewer than perfect step down from that. The level of security is very low when anyone get to WEP, it is around as efficient as a chain link fence. There is a fence to just straightforwardly say "hey, this is my property", nevertheless anybody who essentially desired in, just could simply ascent right over it.



The number of variants of malicious software aimed at mobile devices has reportedly risen from about 14.000 to 40,000 or about 185% in less than a year, the GAO stated.

WIRELESS NETWORK SECURITY TECHNOLOGIES

Sellers are performing their job quite nicely by advancing the security features, and users are receiving a comprehension of wireless security.

However, all intimidations are till now taken into account as important, and vendors are repeatedly required to discourse the remaining insight that wireless LANs are uncertain.

Certainly, the biggest hindrance to implementation of wireless LANs is security. In addition, this is just not vast enterprise concern. Security is till date the biggest concern for enterprises across all sizes when it comes to the wireless networking.

Acquisition of an improved comprehension of wireless LAN security elements and engaging some top performances can go a long way in the direction of allowing an individual to gain the advantages of wireless networking. Only after knowing that the data is secure, an individual gets a peace of mind.

Elements of Wireless Security

Corporates or individuals may deliberately or not set up wireless networks without any security. This occurs due to the reason that maximum wireless access points are derived from the factory in exposed access mode by default. This means that features of security are all switched off. It is the responsibility of buyers to switch them on. There are three acts which can assist in securing a wireless network and are mentioned below:

- Demotivating illegal users through validation
- Avoiding connections that are unofficial by the removal of miscreant access points
- Shielding data when it is being communicated through encryption

There are many other significant issues for the company which are not unpredictable. The prior most issue of the wireless LAN security issue is users which are from external of the company i.e. illegally or cruelly retrieving the enterprise wireless LAN. Secondary issue is the interior miscreant access points, while third issue is encryption.

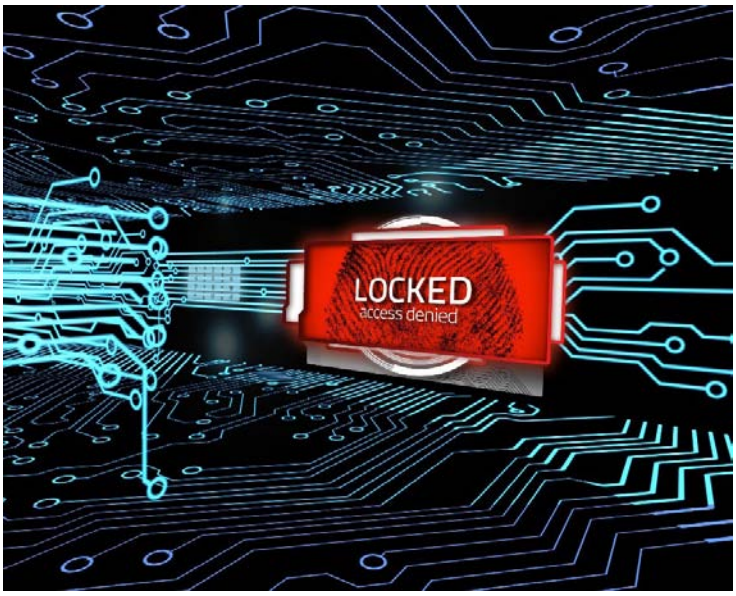


Figure 4.7: digital authentication

Making use of Authentication

To ensure that all the individuals who are using the wireless network are authorized by the enterprise then authentication is comes into effect. Authentication is at times known as access control.

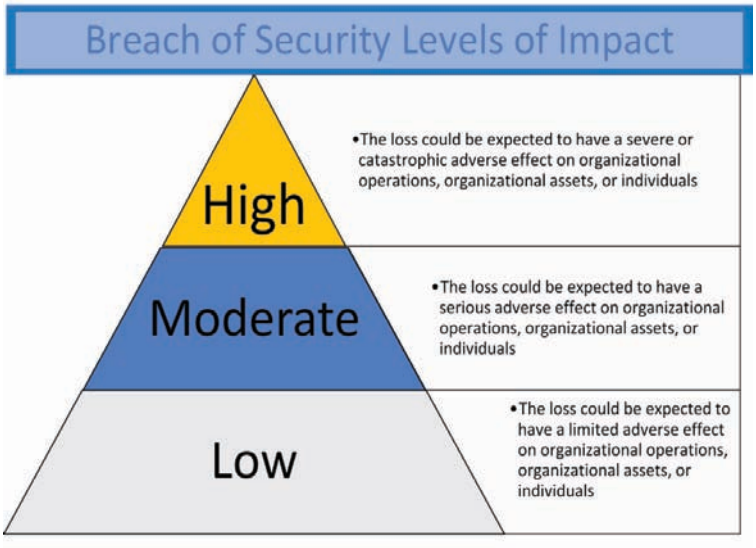


Figure 4.8: security levels breach impact

The basis of authentication is unique logins and passwords. However, there are extra tools that make authentication more protected and dependable. Per-user and per-session is the best authentication between the user and the source of authentication.

Inspecting for rogue access points

An employee who is goodhearted may desire to enjoy similar freedom at work which it enjoys at home. Therefore, it might obtain an access point which is cheap and plug it into a network jack without requesting approval. These access points are referred to as rogue access points. Maximum of these rogue access points are fit in by employees and not by any mean impostors. When the sanctioned access points of companies are not configured in proper manner, they can also be at high security risks. Inspecting for rogue access points is not at all difficult. There are certain tools and equipment which can assist on inspecting for a rogue access points.



In the early days of computer networking, coaxial cables were used, the same type of cabling that is commonly used for cable or sarellite TV today.

It can be done by using a wireless laptop and software in a small building. Also, this can be done using a management appliance collecting data from your access points. Any enterprise can have technical personnel scan for new wireless access points. When the daily scan is done, they can actually locate these things very early.

Method of Encryption

The data should be communicated between an access point and a wireless device, by using encryption to ensure that data cannot be read, and to safeguard data from being changed. In an elementary intellect, encryption is like undisclosed code as this interprets the data into rubbish that only the planned recipient comprehends.



Figure 4.9: Towers of wireless network



Figure 4.10: Cipher encryption

Encryption necessitates that together the sender and receiver both have a key to interpret the communicated data. The most protected encryption makes use of a very complex keys, or algorithms, that modify frequently to guard data.

Existing resolutions for wireless security

There are three resolutions which are already existent for safe wireless LAN encryption and authentication:

1. Wi-Fi Protected Access (WPA)
2. Wi-Fi Protected Access 2 (WPA2)
3. Virtual private networking (VPN)

The resolution selected is precise to the kind of wireless LAN which is being accessed and the level of data encryption that is essential.

WPA AND WPA2 STANDARDS BASED SECURITY CERTIFICATIONS

The standards based security certifications are WPA and WPA2 from the Wi-Fi grouping for enterprise, SMB, and small office or home office. Mutual authentication to verify separate users is offered by the wireless LANS and advanced encryption.

Enterprise class encryption and WPA2 is offered by WPA. These are the next generation of Wi-Fi security is this enterprise class encryption and WPA2, that also backs government grade encryption. It is suggested that WPA or WPA2 can be taken into use for enterprise and SMB wireless LAN placements.

The secure access point control is provided by WPA and WPA2. They provide sturdy data encryption; and, they also defend the network from passive and active attacks

VPN

Wireless effective security to individuals are provided by VPN where the users can access the network while on the road or away from the office. Users can develop a very safe tunnel between any two or more points with VPN on a network while using encryption. This is even when the encrypted data is communicated over unsafe networks such as the public Internet. VPN can also be used in home-based teleworkers with dial-up or broadband connections.

Strategies for wireless security

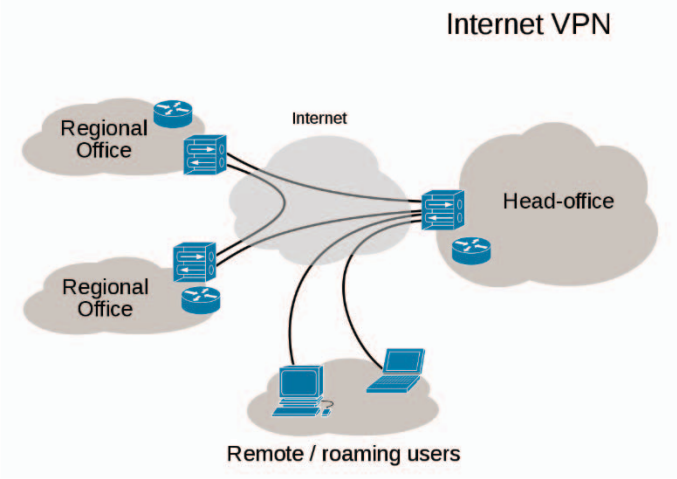


Figure 4.11: virtual private network

There can be different security settings for different users in many cases for a group of users on any network. While using a virtual LAN, all these settings of security can be recognized on the access point.

For instance, any individual can implement diverse security policies for different user groups inside the enterprise for e.g. legal, finance, human resources or manufacturing. Different security policy can also be implemented for customers, partners, or visitors trying to get into wireless LAN.

This permits them to price effectively make use of a sole access point to back multiple user groups with different security settings and security necessities.

All this is done while establishing a secure and protected network. It is also significant to deliberate wireless network security in the background of total network security and network management.

Maximum enterprises which organize, or will organize, wireless LANs may desire to accomplish it in a manner that matches the wired LAN. They may desire it to be combined with public management.

A public management system rises competence for network managers.

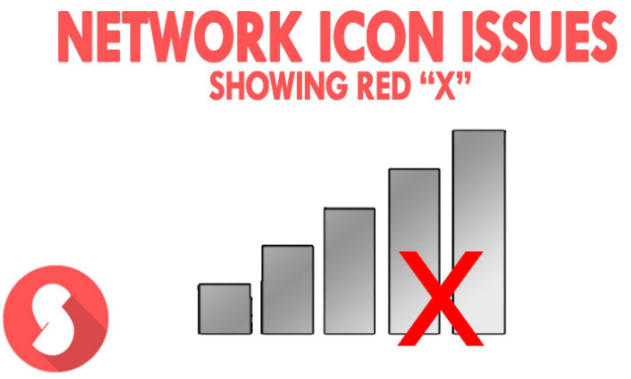


Figure 4.12: Icon issues

Only when the Wireless LAN security is turned on, it works. Only then it is taken into use constantly across the whole wireless LAN. This is the reason as to why the policies of users are additionally significant section of decent security practices. Counterattack the enticement to exaggerate while setting a wireless LAN security policy.

There are several large profits from implementing wireless in place where initial policy is every so often 'no wireless'. The task is to develop a wireless LAN user policy which is modest enough where people will stand by it, but also safe enough to guard the network

Nowadays, it is simpler to strike a balance as WPA and WPA2 are assembled into Wi-Fi certified access points and client devices.

Every enterprise's wireless LAN security policy should also cover the fact at what time and in what way, employees can make use of public hot spots, personal devices on the enterprise wireless network, the off-putting of rogue devices, and a solid password policy.

Captivating Applied Steps

The initial step in securing a wireless network is to switch on the safety features essential in the access points and interface cards. This is typically completed by operating a software program that is available with the wireless equipment.

The similar database that switches on the wireless security features will possibly also display firmware type of access points use. Keep a check on web site of the device manufacturer for the latest firmware version, and bring up-to-date the access point if it is not latest.

Up to date firmware will develop the

wireless network more safe and dependable. Also, inspect to understand all the security resources, hardware, and vendor propose.

The software used by devices such as access points and routers is firmware. Everybody is not capable enough for deploying or maintaining a safe wireless LAN that desires the advantages of the wireless networking.

In this type of case, value-added resellers, network implementers, or other suppliers of wireless networking gear can every so often benefit with these tasks. Some SMBs select to conscript the help of a subcontracted managed security service, several of which have wireless security contributions.

According to Jupiter Research, "a small but considerable segment of enterprises (13%), would outsource wireless security; compared to the 18% that would outsource their overall network management".

DID YOU KNOW

5GHz Wi-Fi actually starts at around 4.9GHz and goes all the way to 5.7GHz-- this can vary widely between different regions due to what frequencies are allowed.



Figure 4.13: two-way security

The way of proceeding doesn't matter but it should be done in a systematic manner. Security is certainly somewhat that has to be deliberate for, same as handling the network, offering attention and access. However, it shouldn't be a hindrance to the placement of a wireless LAN.

Wireless network security technology viewpoints

These days, several organizations are implementing wireless networking technologies to progress productivity, offer more advanced services to customer, and also provide access to Internet to partners and on-site visitors.

The evolution of innovative skills, extensive cellular-data service, and a cumulative number of wireless access points are developing it to be informal for users to access data they require, at any time and at any place, they want it.

As the wireless hotspots accessible in public places such as, airports, coffee shops and restaurants, professional travelers can work effortlessly without considering about the place.

Several users like the wireless fidelity i.e. Wi-Fi connections in their homes, hotel rooms etc. Though offering users' access by wireless network to file shares, applications and other network resources provides several benefits, undertaking this can pose security and organizational challenges.



Figure 4.14: proxy server

The variety of connectivity choices i.e. cellular, local area networks (LANs), wireless local area networks (WLANs), and Wi-Fi can be problematic for IT sections to organize. As the users are required to access resources from both IT organized devices for example, business laptops and from unorganized devices for example, personal digital assistants (PDAs), various already prevalent remote access solutions go away with the network exposed to security threats from viruses, malware, and Trojan horses. also, the shortage of interoperability between wireless vendors, a forever developing security framework for WLANs, and subjects concerned with Internet and firewall traversal pose additional challenges.

With SSL VPNs



Figure 4.15: Wi-Fi signal

In secure wireless networking, organizations are executing wireless technologies to improve productivity, offer additional supple work preparations for their employees, and work more carefully with their business partners. Both the local and wide area systems are included in wireless technologies.

Though, the significant security issues are developed by the multiplicity of networking options as well as computing that includes:

- A developing security outline for WLANs and interoperability problems among sellers.
- Diverse natural security options for wireless local area networks (WLANs) than cellular networks. Employees by means of both organized devices and unorganized devices, for e.g. public terminals and home computers.
- Internet traversal for numerous wireless remote-access solutions.
- Out-of-date WLAN gear that is doubtful.
- The risk of rogue access points.

The security architecture that reports all these matters is an SSL virtual private network (VPN). SSL VPNs offer a method of securing each node, whether core or exterior to the enterprise, resulting to the idea of an upturned security model that does not be contingent on a toughened perimeter.

Wireless Networks Occurrence

As discussed in the previous section, numerous enterprises are implementing wireless networking technologies to improve the productivity of their workers, to advance service to computer, and also to offer Internet access to visitors.

Business travelers are captivating benefit of wireless hotspots in public locations for e.g. airports and restaurants, also adoring the suitability of Wi-Fi in their hotel rooms and homes. They may also use cellular networks for transmission from nearly anyplace.



802.11b WLANs operate at speeds up to 11 Mb/s. 802.11a and 802.11g WLANs operate at speeds up to 54Mbps. 802.11n WLANs can operate up to 600Mbps. 802.11ac WLANs can operate up to 6.77 Gb/s.

Even though, maximum wireless-data practice is with Wi-Fi on the basis of the IEEE 802.11 family of standards, corporates are progressively making use of cellular data services, that presently provide a near-broadband experience over widespread geographic areas.

Smartphones, PDAs etc. are included in usage of Cellular-data. laptops with PC Card modems, and laptops using phones as modems also use cellular data in order of a cable or Bluetooth connection.

Cellular-data networks include manifold technologies, the greatest predominant of which nowadays comprise Enhanced Data Rates for GSM Evolution (EDGE), Wideband CDMA (WCDMA), and the CDMA2000 group of technologies.

In spite of the alphabet soup of names, all of them have a mutual ability i.e. the skill to back IP-based packet communications from almost anywhere. Developing technologies such as more improved performance over the wide area is promised by WiMAX. While cellular-data networks provide rates impending 1 Mb/s, WiMAX vendors are eager to offer advanced amount rates.

Several specialists make use of a mixture of Wi-Fi and cellular data networks. Wireless networking not

only upsurges output, but also improves personal lifestyles where employees can telecommute not just from home but from almost anywhere.

The array of connectivity options, though, increases important security contests for the enterprise, which requires safeguarding these connections whereas accepting an extensive variety of mobile computing platforms, offering a basic user experience, and restraining admission to particular resources, all inside a system which can be accomplished effortlessly.

REVIEW QUESTION

1. Explain Wired Equivalent Privacy (WEP). what are the different types of WEP?
2. Discuss the reasons that made WEP obsolete?
3. What is Wi-Fi Protected Access (WPA) and WPA2?
4. Discuss the elements of wireless security.
5. What is encryption? Explain the methodology involved in encryption.
6. Describe Virtual Private Network (VPN) in brief.
7. Discuss various strategies used in wireless security.
8. Explain the wireless network security with a technical viewpoint.

CHAPTER 5

CHALLENGES IN WIRELESS SECURITY

LEARNING OBJECTIVES

- Basic challenges in wireless security
- Problems which arises in wireless security
- Basic issues in cellular data
- Wireless security architecture recommendation
- What are the risks in wireless networks?
- Few precautions to be protected in the network
- Configuring the computer to be protected in the network
- End point security control
- How security can be controlled from anywhere of the world inside a network
- Administration control and ease
- Security control at end points

INTRODUCTION

The most prior concern for IT managers is related to the wireless networking is security. This is justified, as radio signals are integral issue to overhearing because of their lengthy circulation. Providentially, there are several active methods for safeguarding both Wi-Fi and cellular-data connections. To comprehend the welfares and limits of the numerous methods, any individual may require to initially take into account the security problems in better detail.

PROBLEMS OF WI-FI SECURITY



Figure 5.1: wireless network transmitter

Wired Equivalency Protocol (WEP) is a weak type of wireless security which was initially implemented and the network can be easily accessed by any determined attacker within few minutes with a basic laptop or computer and the software tools which are widely available.

In order to overcome the limitations or security problems of WEP, a new Wi-Fi security standard namely IEEE 802.111 came into lame light. Wi-Fi Protected Access (WPA) and WPA2 are the two iterations of this standard.

WPA is the standard in which all the security problems of WEP are addressed whereas WPA2 by utilizing Advanced Encryption Standard (AES) helps in encryption. IEEE802.111 is a port-based security architecture and is based on IEEE 802.IX where authentication (sometimes called access control) is maintained by utilizing Extensible Authentication Protocol (EAP) methods in concurrence with access control systems such as RADIUS.

However, most of the systems which are being developed now support WPA or WPA2 as both provide high security and are reasonably secure.

There are many issues that exist for Wi-Fi security for the organizations which are utilizing IEEE 802.1i.

- First, IEEE 802.11i does not entertain the devices which were previously installed.
- Second, it can only be applied to access equipment which are in the control of the organization.
- And due to the complexity of IEEE 802.11i-based security solutions, many doubts for interoperability have been raised among many vendor's equipment.

Many Wi-Fi vendors have applied the security improvements in their equipment in order to fill the gap in Wi-Fi security.

Due to all these enhancements, the patrons are required to buy access points and cards from the same seller. The framework of newly developed WLAN also includes vendor dependence in which a centralized controller is employed to manage and coordinate all the access points.



If there are 2 signals on the same frequency and they hit each other they don't actually interfere with each other.

Security functions are often included in these controllers such as giving the end points of VPN tunnel and finding the rogue access points.

The benefits of security obtained from these structures are only applicable to the WLAN nodes which are connected directly and do not expand to other connections such as Ethernet or to WLAN connections in employee homes or in public places.

Issues in Cellular-Data

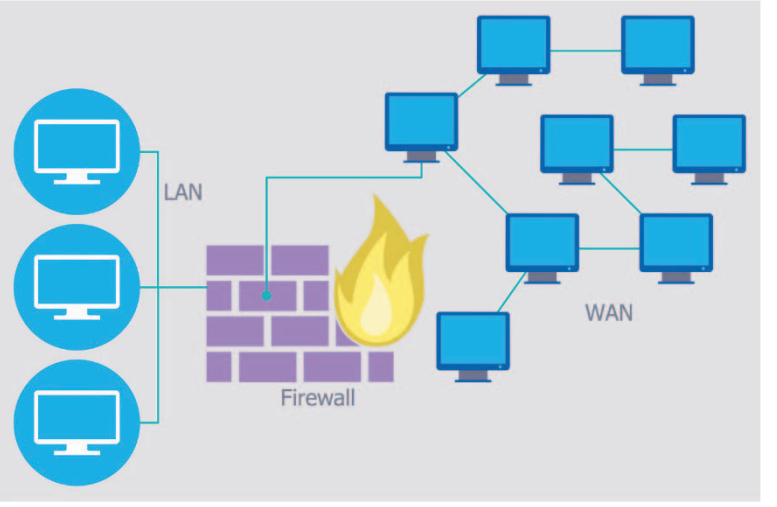


Figure 5.2 firewall security

The security issues with cellular-data connections are slightly different from the issues faced by Wi-Fi. For instance, special equipment is required to attack cellular-network in order to receive as well as decode the radio signal whilst no specialized equipment is required to attack Wi-Fi and can be easily done by using normal Wi-Fi hardware.

Such specialized equipment is very expensive due to which only few cellular networks encrypt the radio link. Cellular networks are basically designed for the latest generation of 3G technologies which offer strong encryption based on algorithms such as AES and Kasumi.

However, they depend upon the previous-generation technology for coverage in the areas which are less densely populated where encryption is not always provided. Sometimes, even if the home operator encrypts the link, the user may keep roaming onto a partner network that does not encrypts the link.

So, in the nutshell, the users cannot depend on the protection of the radio link. Both Wi-Fi hotspots and cellular-data connections share a common issue. Firstly, they both offer the connectivity to the internet and even then, the IP traffic over the internet is not protected when the radio signal is encrypted.

As an option, more secure back-end connectivity options are offered by few cellular operators from the user's core network to the network used by the customer including network-to-network VPN connections, dedicated frame relay circuits or IPSec-based.



Figure 5.3: wireless device security

However, these arrangements increase the costs both through the fees of initial networking setup and also through the reoccurring monthly fees.

RECOMMENDATIONS FOR WIRELESS SECURITY ARCHITECTURE

A security solution is clearly required which addresses all the forms of connectivity, including Wi-Fi both for on premises and off premises, home access,

cellular data, public kiosks and whatever is available in the world of mobile and wireless computing.

There are other essential features of security which are required before an effective security design is specified and these features must include the following abilities:

- It must allow conformity with government regulations which protect both medical and financial data.
- In order to check the layout of software properly such as to scan the system from the codes which are dangerous, virus protection, and to clear the caches, it must have a control over the end-point node.
- Instead of giving access to a network, granular control must be given to the resources.
- It must be able to accommodate almost all types of devices such as desktops, computers which are portable, smartphones and PDAs as well as support both managed and unmanaged nodes.

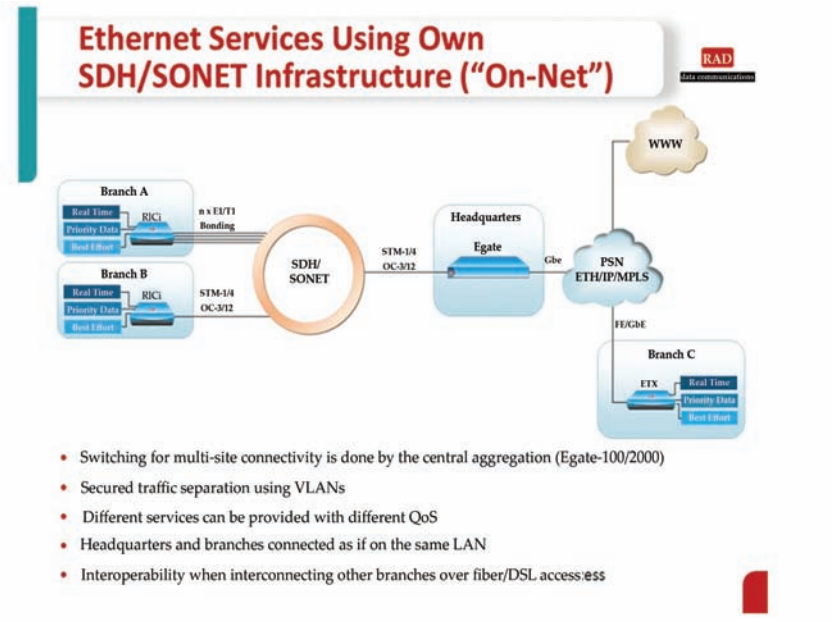


Figure 5.4: SDH and ethernet ring aggregation

VPN based on SSL is the security design that meet all of these requirements. SSL-based VPN exploit the SSL security layer and browsers that are allocated for almost all the computing platforms such as PDAs, smartphones and notebook platforms.

RISK IN WIRELESS NETWORKS

Both conventional networks and wireless networks need the same security measures. The issues that were faced using the wired networks initially are still in concern with wireless networks and devices such as keeping the encryption strong, focus on security and also keeping the certificates in place.

Wireless security was not developed to provide different security rather it was developed to provide a secure and better security to the users. The following are the most common errors made by the users and the preventions to avoid them:

- Don't breach the firewall
- Don't refuse MAC
- Don't rebuff WEP or WPA
- Don't permit uncertified access points
- Don't allow ad-hoc laptop communications

Few other measures to be protected on the network



Figure 5.5: measures to security

Don't Breach the Firewall

Firewalls are created to protect both wired and wireless networks. The configuration must ensure to place the wireless system's access points outside the firewall. Otherwise, if this is not the case then it is clear that a necessary barrier is not created and another convenient tunnel is formed which allows the hackers to attack easily.

Don't refuse MAC (Media Access Control)



Figure 5.6: access control

MAC is frequently disregarded in light of the fact that it's not spoof proof but rather it is another block in the wall. It's basically another address channel, and it obstructs the works for the potential hacker by constraining system access to enlisted gadgets that are recognized on address-based access control lists.

MAC additionally gives you a chance to turn the tables on the potential interloper. Consider that the interloper must knock on the door before being denied.

In the event where MAC is set up, the trespasser will bang into it before understanding it's there and afterward should regroup to move beyond it.

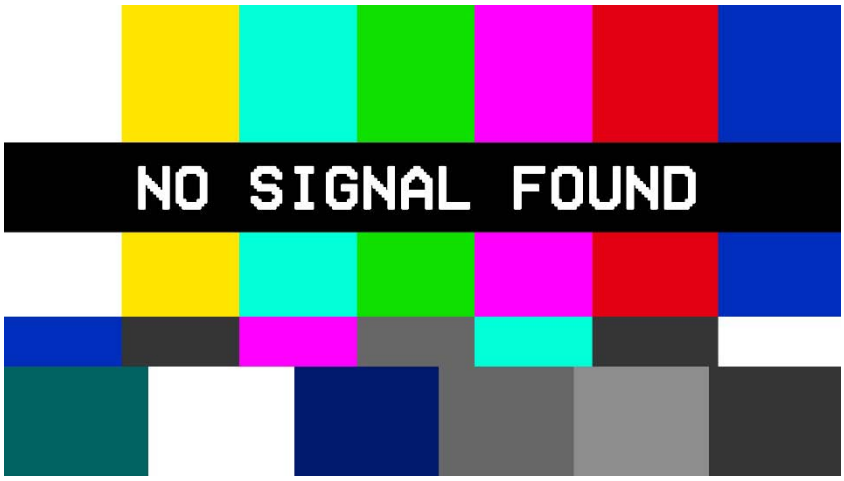


Figure 5.7: no signal

And due to this system now realizes what the interloper resembles. So now there will be three classes of visitors created in accordance with the MAC list:

- Entities that are not on the list yet are known as they've attempted to enter before, uninvited, and are now instantly identifiable if they approach again.
- Entities which are friendly entities and are on the MAC list
- Entities that are unknown and are not on the list that knock by mistake.

In the nutshell, if the wireless network is monitored and beware of the multiple attempts made by the entities at access point and not the MAC list, then the potential trespasser is caught and the trespasser doesn't know that he/she has been caught.

Don't rebuff WEP or WPA

Wired Equivalent Privacy (WEP) is a protocol definite to wireless security which is compatible to 802.11b standard.

It encodes data as it goes wireless, above and over anything else that is being used. Don't rely on the default key as it is key-based. A unique WEP key can be created for the singular users when they initially access the system but try not to depend on WEP alone.

Indeed, use WEP in group with other wireless precise security measures as even multiple layers of encryption can protect the system for being attacked.

And, don't neglect Wi-Fi Protected Access (WPA2), which tends to header shortcoming issues in WEP and is promptly accessible to the users of Windows XP.

WPA2 can be arranged to rekey the encryption which is really easier to use than WEP.

Don't permit Uncertified Access Points

Access points are inconceivably simple to set up, and an over-burdened IT department may slacken the rules to enable them to be set up on an as-required basis by anybody savvy enough to run a VCR. But in any case, don't be capitulate to this enticement.

The essential target for any trespasser is the access point. Execute a deployment technique and strategy and stick to them. Precisely layout the right guidelines for locating an access point and be sure that anybody deploying an AP must has those guidelines close by.

At that point, set up a strategy for taking note of the presence of the AP in the wireless network design for future reference and for suitably dispersing or making accessible the modified arrangement. Despite who sets up the AP, have someone else twofold check the establishment when it's convenient.

Don't allow Ad-Hoc Laptop Communications



Figure 5.8: security to AD-hoc network

This one is very difficult to implement in any enterprise. Ad-hoc mode allows the Wi-Fi clients to link directly to any nearby laptop so conveniently that one just cannot stay without utilizing it.

Since ad hoc mode is the part of the 802.11 standard, it allows the laptop's network card to function in a free basic service set arrangement.

This means that it can run peer-to-peer with another laptop by means of RF. Wireless LAN can be spontaneously formed with another laptop when ad hoc mode is on.

But, access to the whole hard drive of the laptop is licensed. If it is enabled and overlooked that it's enabled, the entire world can see the fly which is threat not only to this open machine.

A trespasser can enter into the network by utilizing the networked laptop. The entire network is exposed if the system is left in ad hoc mode and someone try to sneak in. Maintain a strategic distance from this unsafe propensity by never giving it a chance to create in any case. Simple acknowledge the fact that it is not worth the risk.

End point security control

The main advantage of using the SSL VPNs for remote access is that it empowers more clients to access the system from the far places than they would in the event that they were utilizing the traditional IPSec VPN.

Undoubtedly, the productivity is enhanced whilst access stretch out to places that IT cannot in any way, shape or form control as the security threats for both the end user and IT increases significantly.

Also, the access cannot be managed by user identity alone in order to control the risks effectively. Additionally, there must be a focus on the security of the user's environment.

For instance, your venture needs to convey secure anywhere access to network resources from the most unsafe places (New Orleans, from airport cabins, employee-owned PCs, unmanaged PDAs and wireless hot spots) without giving up the integrity of the undertaking network. In other words, a remote access policy based on end point security should be differentiated by the IT administrators. Here's what can be offered:

- Security anywhere access from many environments
- Policy Zones rather than an "access" policy
- Interrogation of the device
- Ease and control of administration

SECURITY ANYWHERE ACCESS FROM MANY ENVIRONMENTS

An official may work remotely utilizing an endeavor issued laptop PC, at that point sign into the system toward the evening to check email from a tradeshow stand. Soon thereafter, she/he may update an introduction from her home PC.

Based on the security policy that is set, all the end points are secured by the end point security control. For instance, this would mean restricting her/his entrance to specific applications or requiring advanced information security on more hazardous end points.

Policy Zones Rather Than the Access Policy

Without compromising the security, the users must be delivered as much access as possible. So, to achieve that, more options are required that allow or don't allow the access. And if there is semi-trusted end point then three more policy zones are created for example, trusted, semi-trusted and non-trusted.

Even though the untrusted environment does not warrant full access right, then also the IT users are allowed to offer some degree of centrally managed access.

Device Interrogation

All the things that are and are not on an endpoint machine can be detected. For instance, the user ought to have the capacity to launch an agent before the authentication, so login can be ceased if any vindictive software (malware) is found.

The end points can be classified automatically into one of the Policy Zones based on the view that what applications are found on the end point (for instance, a predefined individual firewall or antivirus application), so the level of access allowed is proper both to the client and the level of danger of the end point.

EASE AND CONTROL OF ADMINISTRATION

SSL VPN can be administered by the object-based policy model. This gives the capacity to effortlessly uphold approaches from a solitary point to deliver access with greatest security.

User Authentication Focused Security

Initially, the enterprises were dependent on VPN access from the relative security of the enterprise laptop. The stasis of conventional customer VPN advances really lessened IT fears of security dangers, for example, malware harming the system. IPSec customers couldn't be planted on a stand and were probably not going to be conveyed on a home network.

On account of these impediments, IT had little worry about non-venture machines and assumed that workers obtained access exclusively from big business possessed and-managed machines. Because of this model, IT security concerns concentrated exclusively on client authentication distinguishing clients as strongly as possible.

In order to recognize the clients, numerous substantial endeavors invested in two-factor authentication systems.

These ventures trusted that if clients dependably got the access from the similar location which is trust, the main problem fixated on confirming that the clients were who they said they were.



Wi-Fi uses radio waves to send a signal, which can go through walls, but often bump paths with other redio waves at similar frequencies.

Mobility Increases Risk and Productivity

In order to enhance the productivity of employees, anywhere access can be provided by enterprises from SSL VPNs. Additionally, SSL VPNs gives security advantages such as SSL encryption, full authentication support, and protection from direct network access, and granular access control.

However, the users demand the access from places that IT can't control which therefore substantially increases the risk for end users as well as IT.

Today, the issue centers on who the client is, as well as how reliable the remote access condition is. An SSL VPN client can obtain entrance from a range of end gadgets, all posturing distinctive levels of security threats.

For example, home PCs, PDAs, and tradeshow booths have a higher danger of facilitating malware that could contaminate the system with viruses or Trojan horses, catch passwords for later reuse, or reserve classified data.

AMAZING FACTS!!!

"It can be easy to assume that any new computers or computer hardware your business purchases will be completely free of malware and protected from any vulnerabilities. Shockingly, however, this isn't always true. A number of devices come with vulerable adware and backdoor alredy installed on their systems. In fat, nine out of every 1,000 will be infected with spam or average".

IT Must Address Risk and User Identity

IT directors beyond a reasonable doubt have worries about their capacity to secure venture resources when access can occur from any desktop or gadget.

The users can unintentionally can leave the data behind at a kiosk or hotel business if the viewed e-mail attachments, downloaded files, password and web pages are stored on the hard drive.

For the client, the issue rises above security approach and the uprightness of the corporate system; it turns into an issue of individual privacy.

The remote access approaches will experience inspection when the SSL VPN access becomes widespread and must address the worries of end clients, reviewers, business partners, and IT. Due to the current press report which gives an account of incidents in which data was furtively caught through keystroke logging at open booths, this pressing security issue is quite recently starting to get the public attention.

A couple of composed IT strategies boycott booth kiosk access, yet practically speaking it is a hard arrangement to implement.

In addition, that kind of limitation fundamentally diminishes a portion of the profitability gain that SSL VPNs offer.

Up until now, few enterprises have the clear idea how they are going to deal with this worry. End point security control empowers IT to deal with the danger of Web-based access.

Presently endeavors will never again need to boycott mobile access to big business resources or acknowledge a high level of hazard as a byproduct of giving more prominent client efficiency.

Improved Data Protection and Remediation

Semi-trusted zone must contain all the essential flexible remote access options. Furthermore, in a non-trusted zone for example kiosk access, ASD could be vital for remediation.

REVIEW QUESTION

1. Describe the issues in wireless cellular communication?
2. Explain the challenges in wireless communication.
3. What is Media Access Control (MAC). Discuss in brief.
4. What is the importance of firewall in wireless communication? Also mention the alternative technological solutions that can be used in place of firewall.
5. Explain End-point security control. What is the importance of End-point security control in wireless communication?
6. Discuss the role of administration in wireless security.

CHAPTER 6

ARCHITECTURE OF WIRELESS NETWORK

LEARNING OBJECTIVES

- Things to be keep in mind while architecture of network
- Architecture of wireless network
- Introduction to wireless sensor network
- Wireless sensor network architecture
- Introduction to the basic seven layers of OSI model
- Things to be keep in mind while dividing the layers
- Security perspective of each layer in the OSI model
- Host layers configurations in OSI model
- What are the characteristics of wireless network?
- Basic advantages of wireless network
- Use of wireless sensor network

INTRODUCTION

In this chapter we will study about the architecture of the network which provides services to the internet users and the mobile subscribers who are connected

to the base station. They are usually connected with the communication protocol named as CIA (Common Air Interface) which makes sure about the handshakes of the network through protocols.

The CIA works with the connection to the base station and the subscribers who intercommunicate in between the radio frequencies. This is determined by the control channel by signaling to the base station. The interface which is common should provide a good deal of channel is reliable to make sure that the data which is send and received have a proper and secured connection with the base station and the subscriber.

This is done by the channel and speech writing in code. In the base station, the common air interface component which is used to synchronize the data and helps in signaling of the mobile transmission is not used and the remaining traffic on the network is passed over to the switching of mobile center along with fixed communication networks. Although, all of the base station might have managed the simultaneous calls.

A mobile switching center is worthy of credit that it connects more than 5000 phone calls at the same time with using not more over 100 base stations for the public switched telephone network.

Thus, the connection between the MSC and PSTN involve substantial capacity at any moment of time. It makes clean and clear that the networking standards and schemes might change widely according to contingent upon the circuit of single voice or total population in metropolitan city.

The cellular communication network is dependent upon digital communication and digital radio network technologies in order to maximize the capacity and lineament of services. The speech coding, channel coding and interleaving, equalization are the techniques of digital radio which offer some superior air interface.

This is carried out and spectral efficiency apartment when there is a comparison on one or more previous analog system in a not changing radio channel. In the way towards the application of data some new wireless systems stock a large range of signals and transform them into packets which is used for the transmission in the interface.

The designing of the digital air interface radio formatting is operated well on the architecture of the communication network and then the wireless system is carried on the egress, and the difference among the personal communication system and the digital air interface.

This is a blurred image or we can say backbone of the architecture in the wireless network. if we talk about the fundamental characteristic of ISDN which is common channel signaling is a critical component in the wireless communication network. This process is carried out and is used to be in a bigger cellular capacity. SS7 which is a signaling system is a very important component in the background of wireless networking all over the world.

This is the first step in the field of communication which is packet based and which is moving the trend towards more use of wireless communication and creating wireless traffic.

The distribution and arrangement of the data is on the basis will be a vital component in the rapid increase of the network which is wireless in the communication system.



50% of the companies require 35+ full-time employees to manege endpoint.

The growth in the use of optical fiber structure which is due to the reason of providing maximum bandwidth in the packet of data transferred.

As we can see, today The Voice Over Internet Protocol which is commonly known as VOIP and the web browser of the internet is available at affordable rates for the access of mobile and the data services. In this process the packets are shifted in the wireless networks towards data and voice. Thus, wireless network works by transferring of packets from one place to another and it is architect in such a way that it provides the best services with better security perspective.

Architecture of a wireless network

Currently, wireless network is considered as one of the most standard services which are provided by the service providers in industrial and commercial purposes.

This enhancement was possible with the development in the communication network, processor of devices and lower consumption of power with the more use of embedded computing devices. The wireless network is built with nodes which are used to notice the surroundings such as humidity of the place, position, pressure, temperature, sound, vibrations etc. These nodes are used to figure out the real-time positioning of the applications which are set in order to perform in tasks such as smart detecting which is a discovery of neighbor node.

There are many other tasks performed by the applications such as storage and data processing, target tracking, data collection, control and monitor of the traffic according to the situations, node localization, synchronization, and more effective routing in between the nodes and the base stations.

Presently, wireless network is in the beginning state which is to be organized in an enhanced step. We should not think that in the next 10 to 20 years we will be more secure and protected with the attack on wireless network as it is connecting more with the internet now a day.

This can be concluded as the internet is becoming more physical network and its users are getting increased day by day. This technology is delighting with infinite potential in many applications such as environment, medicine, military, transportation, homeland defense, entertainment, in the field of crisis management and in so many smart spaces.

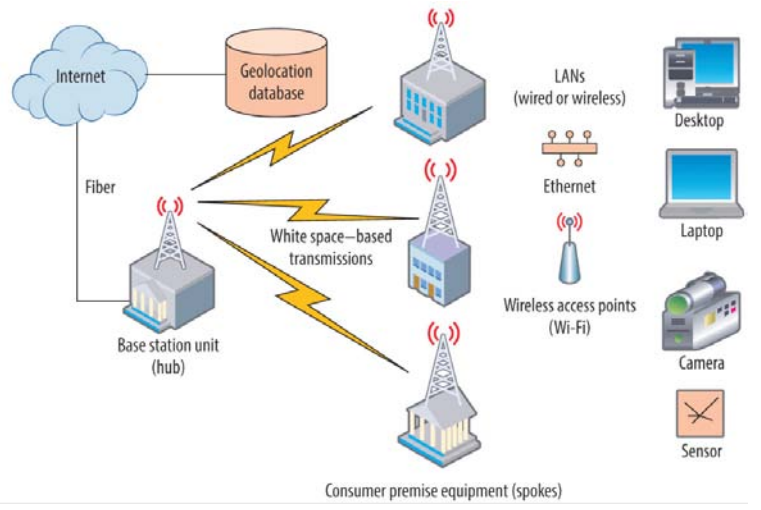


Figure 6.1: architecture of connectivity

What is a Wireless Sensor Network?

Wireless network is one kind of network in which huge number of circulating, minute, self-directed, low powered devices are present as a sensor which are commonly known as motes. There networks cover a large number of spatially distributed, battery operated, little and embedded devices.

These devices are networked in such a way that it softly collects the data, process it and then transfer it to the operators. Then the operators work in a controlled way with capabilities of processing and computing the data accordingly. All of these processes are carried up by the device which is known as nodes. Nodes are tiny computers which work in joints to form a network.

Wireless Network Sensor

The node of the sensor is designed in such a way that it acts as a multifunctional and energy efficient wireless device. The motes applications in the industries are widespread. The alignment of sensor nodes which collects all the data nearby to it is collected and achieve to specific application objectives. The two-way communication in between one node and the other can be made with the use of transceivers.

In a wireless sensor network, there are number of motes which could be hundreds or even thousands. The number of motes totally depend on the number of users present in that very area. With the increase of people in that area the motes also need to be increased.

If we look on the sensor network then we can notice that Ad Hoc network has more few number of nodes without any structure. An Ad Hoc network is a decentralized type of network in which there is



90% of consumers are being driven towards the connected smart home trend by better security for their homes and families.

creation of a network without any infrastructure and it does not have any nodes so, it is free to move.

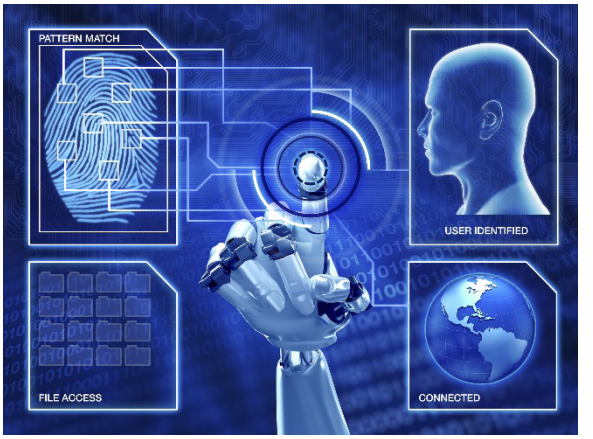


Figure 6.2: Touch security

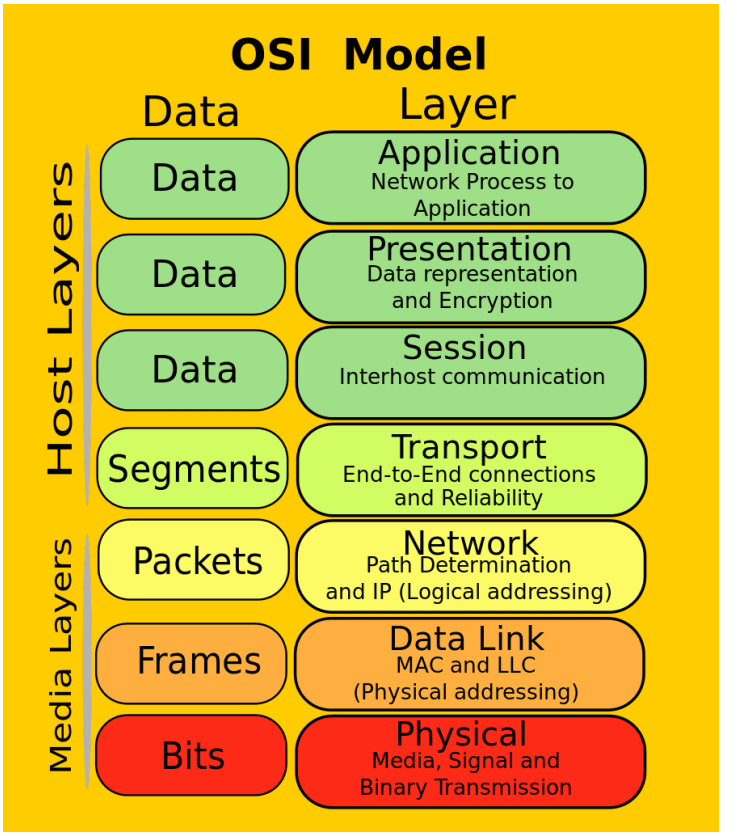


Figure 6.3: multilevel OSI model

Architecture of Wireless Sensor Network

This is considered as the most common type of wireless network architecture which is totally based on the OSI (Open System Interconnection) architecture model. The architecture of wireless network is based on the seven basic layers of network in the OSI model which are:

1. Application layer
2. Presentation layer
3. Session layer
4. Transport layer
5. Network layer
6. Data link layer
7. Physical layer

Each and every layer of the OSI model is designed in such a way that they all perform some specific function. Each of the layer supports the layer just above it and offer services the layer which lie below them.

The bottom three of the layer focuses on the passing of traffic through the network which is being monitored from the end system. The four layers from the top come into act just after the passing of data in order to complete the process. We are going to discuss all of the seven layers one by one which will also include their function and the reliability and relationship with another layer of network.

It is basically the overview of the network process which can later act as a framework for the understanding of computer networking in detail. Here are the different layers of the OSI model explained.

The Physical Layer

The physical layer in the OSI model is defined as the medium of connection between interface. The mechanical, electrical and all other specifications are provided with the sending of a bit stream on a computer network. There are a lot of component in the physical layer which are:

- Cabling of the system with components.
- Setting up the adapters which will be need to connect the physical interface to the media.
- Designing of connectors and assignments of pin.
- Specification of repeater, patch and hub panel specifications
- Components of wireless system
- Simultaneous work on Small Computer System Interface
- Card for Network Interface

In the environment of LAN, we generally use Unshielded Twisted Pair of cable wire which is used for the physical layer in an individual device connection. Optical fiber is also an option which is also used in

the physical layer. The standard bodies like IEEE, EIA/TIA, ANSI have developed these standards for this layer.

The Network Layer

The third layer in the OSI model is the network layer. This layer provides an end to end address to the system in such a way that a packet of data can be send and receive across several layers. Network layer works with various methodology of sending secure data with Ethernet, Token Ring Frame Relay etc.

The network layer addresses are also referred as logical addressing of the network. In the basic part, software manufactures such as Novell developed proprietary layer 3 of addressing. However, the industry of networking has evolved to a point where it requires a common layer 3 in addressing system.

DID YOU KNOW ?

In 2016 over 15 billion Wi-Fi connected devices were shipped across the globel That's a lot of techl.

The Internet Protocol addresses make networks easier to both connect and set up with one another. The internet uses IP addressing in order to give connection to millions of subscribers in the network all around the world



Figure 6.4: Eavesdropper to transmitter to intended receiver

In order to make it easier to control the flow of packets and manage the network, there are many organizations which separate their network layer addressing into smaller parts which are called as subnets.

So, basically subnets are dividing the Internet Protocol address into smaller sections in order to assign one to every user. These subnets are used to track the record and individual for their activity on the internet.

Routers use the subnet portion or we can say the network of the IP addressing to route the traffic in between different networks.

There are several routers assigned for a network. Each of the router should be configured specifically for the subnets or networks such that it will get connected to the interfaces.

Routers communicate with each other with the use of protocols, the protocols could be Open version of Shortest Path First (OSPF) and Routing Information Protocol (RIP) to learn about the networks which are present.

This protocol also uses to calculate the best way to find the path in the network based on the variety of criteria.

The other networked system as well as routers make the routing decisions in the network layer. While transferring of packets in between the different networks, it might be necessary to adjust their outbound size which should be compatible with the layer 2 protocol.

The network layer fulfils it with fragmentation process. The reassembly of fragmented packets happens in the network layer of the final destination system.

There are two more functions which are performed by the network layer which are reporting the logical variations and diagnostics in normal network operations.

As the network layer might be initiated by any networked system, the system is discovered by the variation reports in to the actual sender of the packet.

This packet is found to be outside the normal network operation. The reporting is done by the content validation calculations. The calculation is done by the system of receiving system and it does not match the value which is sent by the system of originating. Then the receiver discards the packet related with no report to the sender.

The again and again transmission is left to the higher layer of transmission protocol. Few of the functional security can also be set up with the filtering of traffic using layer 3 and addressing on routers or devices which is used to transmit data from one place to another.

The Transport layers

The fourth layer is the transport layer

which is needed for the communication in between end to end devices through the network. Relying on the application, that the application is safe and can be trusted with its authentication.

The transport layer offers a connection oriented and best effort communication in the mode of connectivity. There are various functions which are involved in the transport layer which includes the following parts:

- Identification of application
- Identification from client-side entity
  - Making sure that entire message arrived is as it is
  - Segmentation of data for network transport
  - Control in the flow of data to prevent memory over run
  - Maintenance and establishment of both ends of virtual circuits
  - Detection of transmission-error
  - Realignment of segmented data in the correct order on the receiving side
  - Sharing of multiple sessions or Multiplexing over a single physical link

The most commonly transport layer protocol is connection-oriented TCP (Transmission Control Protocol) and the connectionless User Datagram Protocol (UDP).

DID YOU KNOW ?

By 2020 it is estimated there will be over 50 billion Wi-fi connected devices world-wide being used by 7.8 billion people - over doubling the amount of avereage devices per personal.

The Session layers

This is the fifth layer in the OSI model which provides various services. The services include the tracking of number of bytes which is tracked by the end of every session. An acknowledgement is sent from the sender side to the receiver side along

with the number of files and the file size. Then after receiving the data it the receiving side sends a token of receive to the sender if it received all data.

If the token is received by the sender then it will send the data again and if it doesn't receive the token then it will again send the same data until a token is received.

The session layer also allows the function of applications on the device which is used to create, manage and terminate the dialogues inside a network. The function of session layer includes:

- Creating a virtual connection between entities of application
- Data flow synchronization
- Dialog unit creation
- Negotiations on connection parameter
- Partitioning of services into functional groups
- Acknowledgements of data received in a session
- Transferring the data again and again until it is made sure that it has reached.

The Presentation layers

Presentation layer is known for the presentation of data which has been transported in the network with a mode of application. Presentation layer is responsible for how the format of a data which has been sent to the network.

This layer mainly takes care of the alignment of application according to the format of data which could be easily executed on the receiving end. The presentation layer goes through a lot of process in the network which includes:

- Encryption and decryption of messages sent in order to prevent from data theft.
- Compression and expansion of messages such that it could be transferred easily.
- Formatting of graphics
- Translation of content
- Translation of system-specific codes

The Application layers

Application layer is the seventh layer in the OSI model. The application layer gives a platform in the interface for the users in order to operate a device which is connected to the network. This layer basically is what we see on our side while the application is loading in a web browser or e-mail.

The application layer is the data which user is able to see in the process to use the application.

The main function of application

layer includes:

- Support for file transfers
- Ability to print on a network
- Electronic mail
- Electronic messaging
- Browsing the World Wide Web

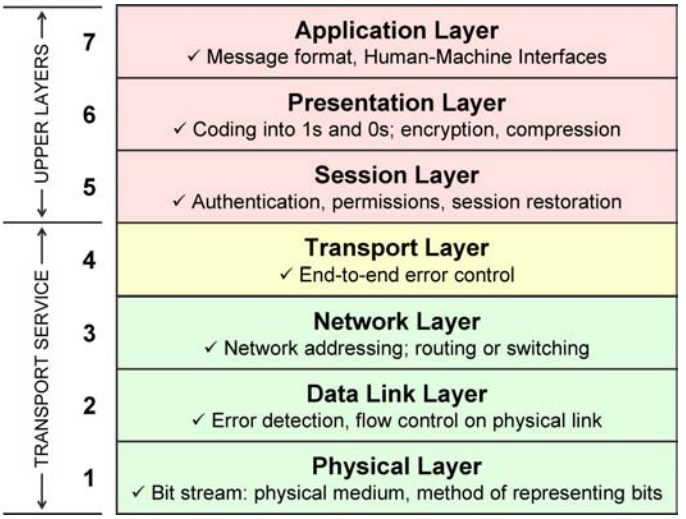


Figure 6.5: OSI 7-layer model

Table 6.1: architecture and their uses

Layer	Function	Protocols	Network component
Application User Interface	Used for applications specifically written to run over the network Allows access to network services that support applications; Directly represents the services that directly support user applications Handles network access, flow control and error recovery Example apps are file transfer, e-mail, NetBIOS-based applications.	NS; FTP; TFTP; BOOTP; SNMP; RLOGIN; SMTP; MIME; NFS; FINGER; TELNET; NCP; APPC; AFP; SMB	**Gateway**

Presentation Translation	Translates from application to network format and vice-versa All different formats from all sources are made into a common uniform format that the rest of the OSI model can understand Responsible for protocol conversion, character conversion, data encryption / decryption, expanding graphics commands, data compression Sets standards for different systems to provide seamless communication from multiple protocol stacks Not always implemented in a network protocol		**Gateway Redirector**
Session Syncs and Sessions	Establishes, maintains and ends sessions across the network Responsible for name recognition (identification) so only the designated parties can participate in the session Provides synchronization services by planning check points in the data stream => if session fails, only data after the most recent checkpoint need be transmitted Manages who can transmit data at a certain time and for how long Examples are interactive login and file transfer connections, the session would connect and re-connect if there was an interruption; recognize names in sessions and register names in history	NetBIOS Names Pipes Mail Slots RPC	**Gateway**

Transport Packets; Flow control & Error-handling	Additional connection below the session layer Manages the flow control of data between parties across the network Divides streams of data into chunks or packets; the transport layer of the receiving computer reassembles the message from packets A train is a good analogy => the data is divided into identical units Provides error-checking to guarantee error-free data delivery, with on losses or duplications Provides acknowledgment of successful transmissions; requests retransmission if some packets don't arrive error-free Provides flow control and error-handling	TCP, ARP, RARP; SPX NWLink NetBIOS / NetBEUI ATP	GatewayAdvanced Cable Tester Brouter
Network Addressing; Routing	Translates logical network address and names to their physical address (e.g. computer name ==> MAC address) Responsible for addressing determining routes for sending managing network problems such as packet switching, data congestion and routing If router can't send data frame as large as the source computer sends, the network layer compensates by breaking the data into smaller units. At the receiving end, the network layer reassembles the data Think of this layer stamping the addresses on each train car	IP; ARP; RARP, ICMP; RIP; OSFP; IGMP; IPX Newline NetBEUI OSI DDP DEC net	Brouter Router Frame Relay Device ATM Switch Advanced Cable Tester

Data Link Data frames to bits	Turns packets into raw bits 100101 and at the receiving end turns bits into packets. Handles data frames between the Network and Physical layers The receiving end packages raw data from the Physical layer into data frames for delivery to the Network layer Responsible for error-free transfer of frames to other computer via the Physical Layer This layer defines the methods used to transmit and receive data on the network. It consists of the wiring, the devices use to connect the NIC to the wiring, the signalling involved to transmit / receive data and the ability to detect signalling errors on the network media	Logical Link Control error correction and flow control manages link control and defines SAPs 802.1 OSI Model 802.2 Logical Link Control Media Access Control communicates with the adapter card controls the type of media being used: 802.3 CSMA/ CD (Ethernet) 802.4 Token Bus (ARC net) 802.5 Token Ring 802.12 Demand Priority	Bridge Switch ISDN Router Intelligent Hub NIC Advanced Cable Tester
Physical Hardware; Raw bit stream	Transmits raw bit stream over physical cable Defines cables, cards, and physical aspects Defines NIC attachments to hardware, how cable is attached to NIC Defines techniques to transfer bit stream to cable	IEEE 802 IEEE 802.2 ISO 2110 ISDN	Repeater Multiplexer Hubs Passive Active TDR Oscilloscope Amplifier

SECURITY ASSOCIATED WITH EACH LAYER OF THE OSI MODEL

As we have seen in past few years about the high-profile hacking taking place. Security in application layer has been the call of hour. In the awareness of security in the network system, the developers as well the security officers don't know exactly needs to be secured from the hackers.

The most important thing to keep in mind while the development of an application or during development of a website is to secure the application layer on the first place because of the reason that application layer is directly shown to the user.

This topic will cover an article about the aspect about how crucial it is to secure the applications fully. As we have seen above in the OSI model that it has seven layers. Optimizing the OSI model security cannot be achieved if all of the layers are safe. Let us see the security perspective issues in all the seven layers of wireless network.

Physical Layer

This layer gives the model physical and electrical specifications of the data connections and its responsible for the physical communication between various ends of stations. The simple actions which could be unplugging of the power source or pulling out the network cable can make it riskier as the security in physical layer is extremely crucial.

To secure this breaches in the physical layer there are some steps which needs to be taken like guarding this layer safely involves enhanced surveillance of security with biometric authentication solution, using advanced lock mechanism to secure the data and use of electromagnetic protection.

Data Link Layer

As we have seen above that the data link layer includes data packets which are transported by the physical layer. This fact is often ignored by the security professionals. Faults and malfunctions in this layer obstruct the functionality of the network layer. The area which could be affected by this layer can be VLAN circumvention and MAC address spoofing.

To secure these breaches some common methods are there to protect which includes MAC address filtering and through evaluation of wireless applications which ensures that they have built an encryption and authentication.

Network Layer

This network is the third and is the last one to correspond to the real or physical world. This basically revolves around the addressing, controlling and routing of the data traffic. IP spoofing is when the inbound malicious packets claimed with the source addresses from the network which has become threat to the industry of application. To secure this network layer, the network needs to be strengthen because that is the only way to protect the data or information from being stolen. This means to route filters and rigid anti-spoofing. The information could also be prevented from network layer by proper configuration of firewall.

The next four layers are considered as host layers.

Transport layer

This is the first logical host layer in the OSI model. The transport layer transfers sequence of data of variable length. The transport layer protocol needs to be reliable and it should work on the mechanism of segmentation additional with error control and good flow. The protocol which is commonly used in transport layer is Transmission Control Protocol.

To secure the data in transport layer can be done by proper firewall implementation. This will also include limiting the access of protocol transmission and information on sub-protocol (i.e. UDP/TCP port number), this is paramount to transport layer security.

Session Layer

This is the fifth layer in the OSI model. The session layer mainly deals with the controls of inter-machine communication. This layer handles the interaction between remote and local application.

This will also include establishing, terminating and managing the connection as per the requirement of the network. In this layer of network, a weak authentication mechanism which are being vulnerable to brute-force attacks are weak points.

The best way to secure the data in session layer is to make sure that the passwords are encrypted while exchanging it to the storage or while passing it through the network.

This step will help us to end secure the data with encrypted data and will be very tough to crack. The encryption should be ending to end such that it has less chances of getting stolen. The session layer should also

include the limiting of failed transactions with the help of timing mechanism such that in a fixed time, if the transaction fails then it will block the session.

Presentation layer

Presentation layer is the sixth layer in the OSI model. As the name suggests that it deals with the presentation and organization of the transferred data from application layer into the network layer.

The layer standardizes the data to and from various local formats which is done by number of conversion schemes. But, somehow the poor handling of malicious input leads to crashes or exploitation of data.



Right now, 3.7 billion people are using Internet - that's over half the world's population connected to the world wide web.

In order to secure this network, one of the most effective way is to create a separation gap between the users. "This should not be sanitized before it gets passed into function from the program control function"

Application Layer

Application layer is the seventh and last layer in the OSI model. The application layer accommodates the user interface and the other key functions. This layer is the closest to OSI model and is connected directly to the user end. This layer also provides the hacker with the widest attack surface. If this layer is exploited then the entire application can be manipulated. The data of the user can be stolen or in few cases where they are giving very high security then the entire system can be shut down.

Table 6.2: security architecture

OSI Security Architecture	
Security attack	• Any action that compromises the security of information owned by an organization
Security mechanism	• A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack
Security service	• A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization • Intended to counter security attacks, and they make use of one or more security mechanisms to provide the service

The applications which are considered as poor code design and integrity flaws can create huge number of problems starting from performance to stability or bugs.

Thus, the hackers get a loop in the application layer and can exploit the application or information provided in the network.

There are also some traditional security methods which are named as Web Application Firewall (WAF) are not effective anymore as it is supposed to be stand alone in the solutions because of their inherited deficiencies.

To secure this layer the application should be enhanced in the security layer.

The key to the deployment of breaches lie in the application code while developing the application. Only Practices and awareness can boost the code of integrity.

Wireless Network Characteristics

- Power limits for nodes with batteries consumption.
- Node failure handling capacity
- Heterogeneity of nodes and mobility of nodes
- Large scale of distribution for scalability.
- Strict environmental conditions capability for guarantee.
- Simple in use
- Designing in cross layer

Advantages of Wireless Networks

The advantages of WSN include the following

- Network arrangements can be carried out without immovable infrastructure.
- Apt for the non-reachable places like mountains, over the sea, rural areas and deep forests.
- Flexible if there is a casual situation when an additional workstation is required.
- Execution pricing is inexpensive.
- It avoids plenty of wiring.
- It might provide accommodations for the new devices at any time.
- It can be opened by using a centralized monitoring



Figure 6.6: Applications to wireless sensor networks

Wireless Sensor Network Applications

Wireless sensor network is made up of various number of sensors like low sampling rate, magnetic, visual, thermal, seismic, acoustic, radar and infrared. These sensors are clever enough to monitor a huge range of ambient situations.

These nodes are used in constantly sensing the event ID, local control of actuators and event detection. There are many applications of wireless sensor network in the field of private as well as commercial area, which are as follows:

- Health Applications
- Environmental Applications
- Home Applications
- Military Applications
- Commercial Applications
- Area monitoring
- Health care monitoring
- Environmental/Earth sensing
- Monitoring pollution in air
- Detection of forest fire
- Detection of landslide
- Water quality monitoring
- Industrial monitoring

AMAZING FACTS!!!

An average cell phone user uses his/her phones 708 minute per months. 5.5 billion wireless subscribers worldwide send and receive more than 5 billion SMS per day.

REVIEW QUESTION

1. Explain the following terms:
   a. Public Switched Telephone Network (PSTN)
   b. Voice over Internet Protocol (VOIP)
   c. Transmission Control Protocol/ Internet Protocol (TCP/IP)
2. Explain the architecture of a wireless network in detail.
3. Describe Wireless Network Sensors.
4. Explain the architecture of wireless sensor network.
5. Discuss the security concerns in each layer of ISO OSI model?
6. What are the characteristics of wireless network?
7. What are the advantages and applications of wireless network?

CHAPTER 7

THREAT TO WIRELESS NETWORK- ACTIVE AND PASSIVE ATTACK

LEARNING OBJECTIVES

- What are the threats to wireless network?
- Types of threat to wireless network
- Introduction to Active attacks
- What are the types of Active Attacks?
- What are DOS ATTACKS?
- Different types of DOS attacks
- Introduction to Passive attacks
- Methods of passive attacks
- What are the different types of passive attacks?
- What is Sybil Attack?
- What is node replication?

INTRODUCTION

There are several types of attacks which are specifically vulnerable to sensor networks. All these attacks cover a wide range from denial of services to traffic

analysis, physical attacks, privacy violation and so forth. The two most common types of attacks which are studied widely are as follows:

Active Attacks

An active attack is defined as the network exploit in which the attacker tries to change the data on the target or the data which is being transmitted to the target.

- Masquerade attack
- Replay
- Modification of messages
- Denial of service

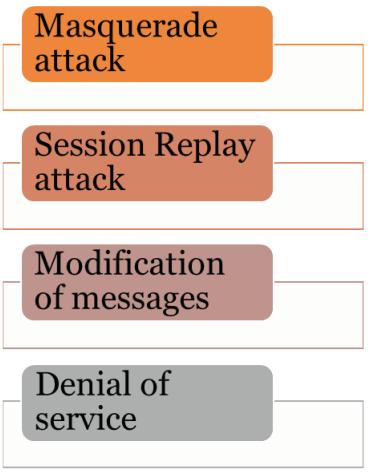


Figure 7.1: Different types of active attacks

Masquerade Attack

Generally, a masquerade is a bluff. But, in terms of security network issues, a masquerade is a category of the active attack in which the hacker pretends to be a sanctioned user of a network in order to achieve entrance in the network or to achieve better benefits than they are approved for.

Table 7.1: active attacks and their solutions

Active Attack			
Problem	**Layer**	**Solution**	**Comments**
Denial of service (DoS) attack. / Sybil attack.	Neighbour maintenance.	Limit the number of joining nodes, with slowing down the joining process with puzzles.	A puzzle could be sent to the client at login, or every time a new round starts in the game. It can also be extended with a captcha to make the login process more secure.
Black hole attack. / Routing table modification. / Location disclosure.	Neighbor maintenance.	Collect information from nodes that are x hops and see if the routing table advertisements are consistent.	The size of the routing table does not grow dramatically because the number of neighbors is low. With majority decision it is possible to eliminate malicious nodes.
Black hole attack. / Forwarding a packet to a node that is not eligible to receive it.	Multimedia	Make the attack pointless with hiding the identity of the senders of the multimedia traffic.	When a node generates a multimedia packet, and sends it out, it does not put its accurate location info in it. Instead, it uses slightly different coordinates. This way, it is impossible to detect if the node is just a forwarder or the originator and as a result the receiver does not know if it is worth to forward or through away the message.

Through the use of logon IDs and passwords which are stolen, by discovering the security gaps in the programs, or through evading the authentication mechanism, a masquerade can be attempted.

Masquerade can be attempted from inside the organization, for instance, an employee from within the organization, or a user from outside who have some connection to the free network.

The authentication which is very weak gives the masquerade an opportunity to gain the access as they are one of the easiest points of entry and it becomes very easy for an attacker.

And if once the attacker gains the authorization for entry, they have the privilege to access all the important data of the organization and depending

upon the advantage they wish to take can alter and delete the data or software and can make changes to the routing data and network structure.

SESSION REPLAY ATTACK

Session replay attack is a scheme in which a hacker by stealing the session ID, steals an authorized user's log in data. Once the attacker gains the access then the intruder has the capacity to do anything same as the authorized user can do on the interactive website.

Session IDs enable the user to trace for a Web site and can give automatic authentication for future visits to that site or related sites. The session ID can be deposited as a cookie, URL or form field. The attacker can conduct either a session replay or session hijacking attack once he gets the session ID data.

It is very easy to detect a session hijacking intrusion as it is happening while a session is in progression. Since a session replay assault does not happen progressively, however, such an assault may just be found when the client learns he has been the casualty of data fraud or some other type of extortion.

Effects

The attacker can perform the following things once the session ID is stolen, the attacker can:

- To keep the track of the user the attacker can use the session ID.
- Can look at the details of the user's account.
- Can perform fake transaction/ activity after viewing the user's account

There is few software which are developed to minimize the risk of session replay as well as application security.

For instance, these include conventional firewalls, decryption/ encryption programs, application firewalls, pop-up blockers, anti-virus programs and spyware removal/ detection programs.

The preventions which must be taken to avoid these attacks are: immediately deletion of the cookies which are stored and the files which are temporary from Web browsers, the passwords should never be saved on any browser, updating the system on time whenever they are available, questionable Web sites must be avoided.

Modification Attack

In a message alteration assault, an interloper adjusts packet header delivers to guide a message to an alternate goal or change the information on a target machine.

DOS attack

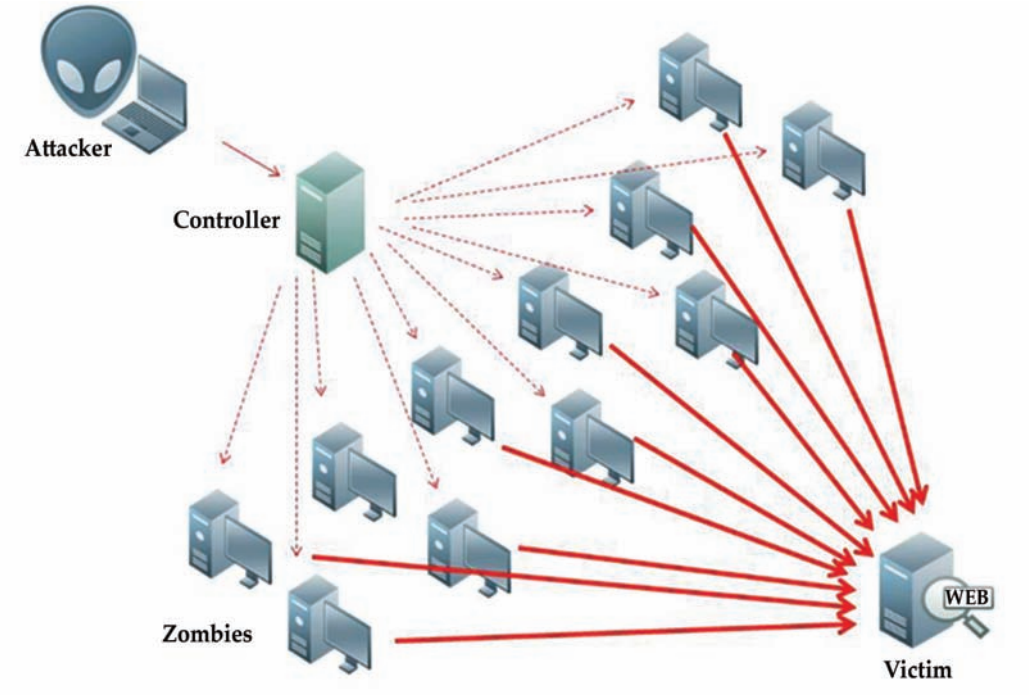


Figure 7.2: Structure of an attack

In a denial of service (DoS) attack, clients are denied of access to a system or web asset. This is generally achieved by overpowering the objective with more activity than it can deal with.

In other words, DOS attack is a security event that happens when an intruder takes steps that stops authorized clients from accessing targeted devices, computer systems, or other network resources.

Denial of service (DoS) attacks normally overflow the servers, frameworks or systems with traffic keeping in mind the end goal to overpower the casualty assets and make it troublesome or inconceivable for true blue clients to utilize them.

While an assault that crashes a server can regularly be managed effectively by just rebooting the framework, flooding assaults can be harder to recoup from.

3Some guidelines are provided by the United States Computer Emergency Readiness Team (US-CERT) for finding when a DoS attack may be started. US-CERT proposes the following may specify such an attack:

- When trying to access the files that are stored on the network or websites then there is degradation in performance of the network.
- When incapable to reach a specific website;
- Troublesome in opening any website; and
- When the number of spam email is higher than usual volume.

A number of strategies are recommended for the users to shield against a denial-of-service attack.

Firstly, an incident response plan must be prepared well in advance of any attack and if there is doubt that a DOS attack is starting then the user must contact their internet service provider (ISP) to be sure whether the attack is a real DoS attack or the performance is degraded due to some other factor.

The ISP can help alleviate the attack by rerouting or controlling the traffic and utilizing load balancers to mitigate the effect of the attack.

Moreover, there are products available in the market to detect the DOS attacks which the users may want to discover the possibility of using them such as intrusion detection systems, intrusion prevention systems and firewalls.

Other strategies can be contracting with a backup ISP and utilizing cloud-based anti-DoS services.

There have been few cases where DoS assailants request instalment from casualties to end the assaults, financial benefit isn't generally the intention behind this kind of assault.

Much of the time, the aggressors wish to cause damage to the association or individual focused in the attack; otherwise, the invaders are just trying to vandalize the casualty, producing the extreme damage or bother a number of casualties. At the point when a culprit of a DoS assault is recognized, the purposes behind an assault may likewise be uncovered.

Some prominent DoS assaults are really disseminated assaults, which means the assault activity is coordinated from various attack frameworks. DoS assaults starting from a solitary source can be simpler to reduce since protectors can cease system traffic from the felonious source whereas attacks coordinated from various attacking networks are much more tough to recognize and shield against in light of the fact that it can be tough to separate authentic traffic from malicious traffic and channel pernicious bundles when they are sent from everywhere throughout the web.

TYPES OF DOS ATTACKS

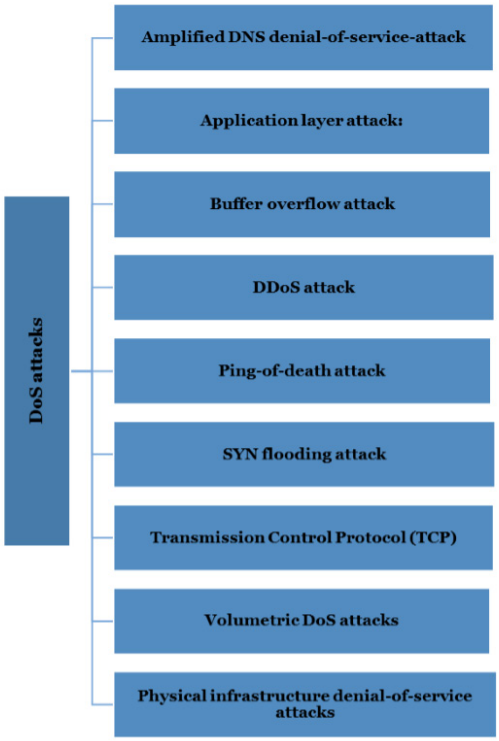


Figure 7.3: type of DOS attack

DOS can be characterized by the techniques the attack uses, in addition to differentiating between a single-source denial-of-service attack and a distributed denial-of-service (DDoS) attack.

Amplified DNS denial-of-service-attack

In an amplified DNS denial-of-service attack, the assailant creates created domain name system (DNS) requests that seem to have started at the casualty's system and sends them to misconfigure DNS servers administered by outsiders.

The intensification happens as the intermediate DNS servers react to the faked DNS requests. The reactions from the intermediate DNS servers to the created assault solicitations may contain far more prominent volume of information than common DNS reactions, requiring more assets to process, with the outcome being to deny real clients access to the service.

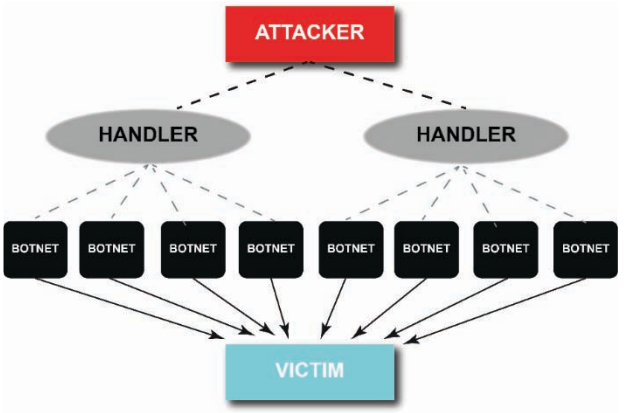


Figure 7.4: Architecture of a DOS attack

Application layer attack

Application layer assaults create counterfeit traffic to web application servers, particularly DNS servers or HTTP servers.

While some application-layer denial-of-service assaults depend basically on flooding the application servers with system information, others rely upon misusing shortcomings or vulnerabilities in the casualty's application server or in the application procedure itself.

Buffer overflow attack

A buffer overflow assault is a catchall depiction most normally connected to DoS assaults that direct more traffic to a system resource than was at any point expected by the engineers who planned the resource.

One case of such an assault sent, as email attachments, documents that have 256-character record names to beneficiaries utilizing Netscape or Microsoft email customers; the lengthier than-expected record names were adequate to crash those applications.

DDoS attack

In a DDoS attack, the assailant may utilize PCs or other system associated gadgets that have been tainted by malware and made portion of a botnet.

Distributed denial-of-service attacks, particularly those utilizing botnets, utilize command-and-control (C&C) servers to coordinate the activities of the botnet members. The C&C servers direct what sort of assault to dispatch, what sorts of information to transmit and what frameworks or system resources are to be focused in the assault.

Ping-of-death attack

The ping-of-death attack mistreat the Packet Inter-Network Groper (ping) convention by sending request messages with curiously large payloads, causing targeted frameworks to end up overpowered, quit reacting to real requests for benefit and conceivably slamming the casualty networks.

SYN flooding attack

A SYN flooding attack manhandle TCP's handshake convention by which a customer builds up a TCP association with a server.

In a SYN flooding assault, the assailant coordinates a high-volume stream of solicitations to open TCP associations with the casualty server, with no expectation of really finishing the circuits.

The cost of producing the brook of SYN requests is moderately low, however reacting to such demands is resource concentrated for the casualty. The outcome is an effective assailant can deny true blue clients access to the targeted server.

Transmission Control Protocol (TCP)

TCP additionally called state exhaustion attacks happen when an aggressor focuses on the state tables held in firewalls, switches and other system gadgets by filling them with assault information.

At the point when these gadgets fuse state full assessment of system circuits, aggressors might have the capacity to fill state tables by opening more TCP circuits than the casualty framework can deal at once, keeping authentic clients from getting to the system resources.

Teardrop attack

The tear attack misuses defects in the way more established working frameworks dealt with divided Internet Protocol (IP) parcels.

The IP detail permits parcel discontinuity when the bundles are too big to be handled by middle switches, and it requires parcel sections to determine portion counterbalances; in teardrop assaults, the fragments counterbalances are set to cover each other.

Hosts running influenced OSes are not able to reassemble the parts and the assault may likewise crash the network.

Volumetric DoS attacks

Volumetric DoS attacks intend to meddle with authentic access to system resources by spending all the data transfer capacity (bandwidth) accessible to achieve those resources.

Keeping in mind the end goal to do

this, assailants should send a high volume of system traffic against the casualty's frameworks. Volumetric DoS assaults surge victim gadgets with systems packets utilizing the User Datagram Protocol or the Internet Control Message Protocol, in substantial part on the grounds that those protocols require generally minimal overhead to produce expansive volumes of traffic, while, in the meantime, requiring nontrivial calculation with respect to the casualty's system gadgets to process the approaching malicious datagrams.

Physical infrastructure denial-of-service attacks

A denial-of-service attack can likewise abuse vulnerabilities in a physical architecture to refute genuine client's access to PC or system resources.

While many administration interferences are disturbed by system attacks, a similar outcome can likewise be accomplished by physically disjoining wiring or stopping power and cooling assets from being retrieved. In such cases, the physical assault may likewise be alluded to as sabotage.

Passive Attacks

A passive attack is a system assault in which a network is observed and occasionally filtered for open ports and vulnerabilities. The reason is exclusively gain information about the objective and no information is changed on the objective.

Active reconnaissance and Passive reconnaissance are included in passive attacks. In active reconnaissance, the interloper involves in with the target network through techniques like port scans. In passive reconnaissance, an interloper through techniques like session capture monitors networks for vulnerabilities without connection.

METHODS OF PASSIVE ATTACKS

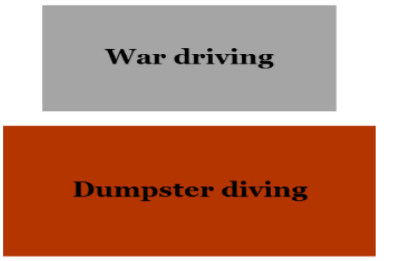


Figure 7.5: methods of passive attacks

- War driving: War driving identifies susceptible Wi-Fi networks by examining them from adjacent areas with an antenna which is portable.

The assault is normally completed from a moving vehicle, once in a while with GPS networks that attackers use to plot out territories with vulnerabilities on a guide.

War driving is possible just to steal an Internet connection or as a preparatory action for a future assault.

- Dumpster diving: In dumpster jumping, interlopers search for data deposited on disposed of PCs and different gadgets or even passwords in waste canisters. The gate crashers would then be able to utilize this data to encourage undercover section to a system or framework.

Types of passive attacks

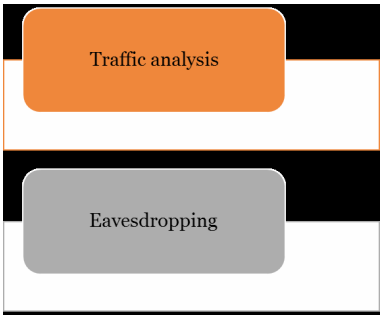


Figure 7.6: types of passive attack

Traffic Analysis

During a traffic analysis attack, the following functions are performed such as the eavesdropper examines the traffic, finds the area, recognizes conveying hosts and detects the recurrence and length of traded messages.

Any individual utilizes this data to anticipate the nature of communication.

All approaching and active traffic of the system is examined, yet not adjusted. Traffic analysis is a special type of inference attack technique that looks at communication designs between elements in a system.

"Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted.

In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic.

Traffic analysis can be performed in the context of military intelligence or counter-intelligence, and is a concern in computer security."

Knowing who's talking to whom, when, and for how long, can sometimes clue an attacker in to information of which you'd rather she not be aware.

The size of parcels being traded between two hosts can likewise be profitable data for an assailant, regardless of the possibility that they aren't ready to see the content of the traffic (being encoded or generally inaccessible).

Seeing a short whirlwind of single-byte payload parcels with reliable stops between every bundle may demonstrate an intelligent session between two hosts, where every bundle shows a solitary keystroke.

Expansive parcels managed after some time have a tendency to demonstrate file exchanges between hosts, likewise showing which host is transmitting and which host is accepting the document.

Independently, this data might not be horrendously harming to the security of the system, yet an imaginative aggressor will have the capacity to join this data with other data to sidestep expected security components.

Eavesdropping

Eavesdropping is the unapproved ongoing interference of a private correspondence, for example, a telephone call, instant messages, and videoconference or fax transmission.

The term "eavesdropping derives from the practice of actually standing under the eaves of a house, listening to conversations inside".

VoIP frameworks that don't utilize encryption make it generally simple for an interloper to block calls. Here's Gary Audin's clarification:

Eavesdropping is simpler to perform with IP-based calls than TDM-based calls. Any convention analyzer can pick and record the calls without being seen by the guests.

There is programming bundles for computers that will change over digitized voice from standard CODECs into WAV documents.

The speakerphone function can be turned on remotely, with the guest on mute so that there is no sound originating from the telephone. This has occurred with some IP telephones in administrators' workplaces. Their workplaces can be listened without their insight.

PCs and tablets that have amplifiers connected or incorporated into them can be empowered as listening gadgets without the client's learning.

There is a rootkit accessible for this reason. Indeed, even frameworks that do utilize encryption can be defenseless, in any case. In August 2009, Symantec issued a security release about a wiretap Trojan known as Peskyspy.



Figure 7.7: Tree structure of wireless network

Peskyspy was intended to access Skype call sound before it was scrambled. Eavesdropping on a traditional phone line through specialized techniques is known as wiretapping.

For a release of message content, a telephonic discussion, an E-mail message or an exchanged record may contain private information. A passive attack screens the substance of the transmitted information.

Passive attacks are extremely hard to identify on the grounds that they don't include any alteration of the information.

At the point when the messages are transmitted neither the sender nor the collector knows that an outsider may catch the messages. This can be avoided by encryption of information.

DID YOU KNOW ?

There are currently around 150 million smart homes_ worldwide - it wan't be long before Wi-Fi connected homes are the norm.

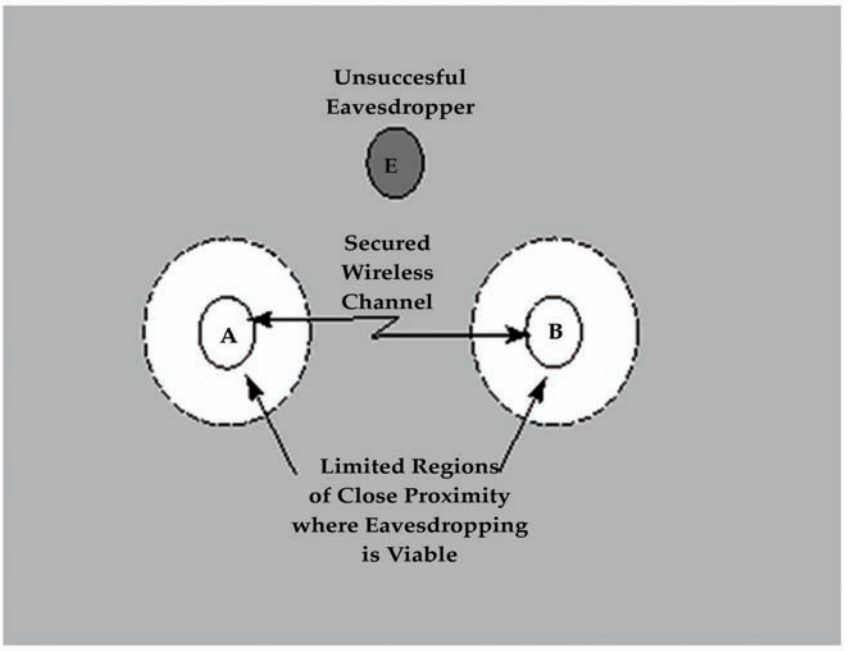


Figure 7.8: unsuccessful eavesdropping by encryption

The Sybil Attack

The Sybil assault can be characterized as a "malicious device illegitimately taking on multiple identities".

It was initially portrayed as an assault ready to overcome the excess components of disseminated information stockpiling systems in shared systems. Furthermore, the Sybil assault is likewise effective against directing calculations, information accumulation, voting, reasonable asset allotment and foiling trouble making recognition.

Notwithstanding the objective (voting, directing, accumulation) the majority of the assaulting methods include the utilization of numerous characters.

For example, in a voting plan, the Sybil attack may use various characters to create extra "votes". Likewise, to assault the routing convention, the Sybil assault would depend on a noxious node going up against the personality of various nodes, and along these lines steering numerous ways through a solitary pernicious node.

Node Replication Attacks

A node replication attack is like the Sybil assault. Rather than having a node utilizing more characters (with respect to the Sybil assault), the assailant here looks to add a node to a current sensor arrange by duplicating (repeating) a node's memory into the memory of a recently made node.

The energy of this assault is that, cloning both the ID of the first nodes and the cryptographic material used to demonstrate the genuineness of the corresponding ID, it is difficult to distinguish that we are looking with a false node. A node reproduced in this form can extremely disturb a sensor system's execution: Packets can be defiled or even misrouted.

This can bring about a disengaged network, false sensor readings, and so on. And, if the assailant can gain physical access to the whole system it can duplicate cryptographic keys to the recreated sensor and can likewise embed the repeated nodes into vital focuses in the system.

For instance, by embedding's the duplicated nodes at particular system points, the assailant could easily control a particular portion of the system.

AMAZING FACTS!!!

Malware is often bundled with other software and may be installed without your knowledge. For instance, AOL Instant Messenger comes with wild Tangent, a documented malware program. Some peer-to-peer (P2P) applications, such as KaZoA, Gnutella, and LimeWire also bundle spyware and adware. While End User License Agreements (EULA) usually include information about additional programs, some malware is automatically installed, without notification or user consent.

REVIEW QUESTION

1. What are active attacks? Discuss various types' active attacks.
2. What are the various types of DOS attacks?
3. Explain passive attacks in detail.
4. Discuss various types of viruses, malware, and ransomware.

CHAPTER 8

MEASURES TO PREVENT ACTIVE ATTACKS AND PASSIVE ATTACK

LEARNING OBJECTIVES

- Measures to be protected from active attacks and passive attacks
- Use of firewall for the defence of passive attacks
- Use of antivirus software and access control
- Tools by which we should be aware of
- Passive attacks defence conclusion
- Pre-emptive attacks at a glance
- Response of network for the attacks made
- Counterattacks effects on the network
- Introduction to active deception and its fundamentals
- Defence communication in Active and Passive attacks

INTRODUCTION

To correct the security weaknesses and adapt the response tools which are recently comprised in the maximum computer network attacks are firewalls, anti-virus software, access control with encryption, access control without encryption, updates.

These passive measures are not only important part of the data guarantee, they should also be employment of efficient defenses in a preventive or counterattack role. These defenses are probable to be come across on the system of the hacker's due to this reason, the main types of passive defenses are discussed in the section below.

TYPES OF PASSIVE DEFENCES

Firewalls

A combination of hardware and software or only a software application is known as firewall. PIX firewall 4.1 is example of combination hardware and software provided by Cisco to work with its routers.

The software application example is Norton Personal Firewall. It attempts to avert unlawful users by examining inward packets of data from accessing a network. This can be arranged to do so in very precise manner.

Initially, a firewall can demonstrate users by point of source, such as, DoD limited unsystematic networks make use of firewall configuration which permits only users from a known area to have access.

Additionally, it can be organized to permitted only specific groups of users to access particular applications, such as, the firewall may also permit access to a database of mine competition scores solely to members of the Wing Weapons shop.

A firewall can also be used to protect information; for instance, it can be trained "to identify and eliminate implementable code for e.g. Java, or even an identified attack signature.

Finally, Sun Microsystems 'Sunscreen type firewalls can conceal "vacant ports from scanners." Attaining a balance between the security and usability is involved in configuration of a firewall; i.e., additionally preventive the configuration is, a reduced amount of the capability to interconnect easily is through the network and/or between the network and the Internet.

To allow free and easy access from the systems to be regulated by trustworthy administrators is another way to work around this module.

This is known as "trust relationship", and it lets active communication without unnecessarily negotiating security as long as the reliable network is itself not cooperated. The attacker can bypass the firewall by exploiting the trust relationship.

Updates are necessary for recognition and exclusion of newly found threats are required in effective firewall configuration.

A firewall is almost as beneficial as the system administrator who runs

it due to all these reasons. Once it is entered, it is no longer defensive to the network, as was done to Microsoft 's.

Antivirus Software

Possibly one of the most ordinary among all the measures of security, active use of antivirus software can be the vital additional line of protection for a network.

Viruses are merely self-imitating files, and two specific subdivisions of the virus family, trojans and worms, can be taken into use to bypass security of a network.

Both of them carry code which will affect after receipt of an external trigger, for instance a date or a command directed by the attacker. Consistent updates to virus signature lists that recognize threats by the length, or assembly of their code and daily scans are perhaps the finest method to distinguish trojans and worms which may have intruded a network firewall can also be complemented by Antivirus software after being configured to scan all inbound e-mail for recognized virus signatures.

The growing occurrence of centrally measured operating systems in DoD (such as Windows NT/2000) styles it to be considerably easy for system administrators to inevitably download and install latest virus signatures, and to list automatic virus scans, on each machine in the network.

Access Control

The simplest and lengthiest in succession method to protect a network is over access control. Users are allocated dissimilar levels of consents, which distinguish the directories and files they may or may not access, and may or may not change.

The most influential access is "root" access that has authorization to access and change any directory or file on the network. "User" access has the smallest consents, and is characteristically limited to those functions which are required by the normal account holder, for instance, e-mail, web browsing, certain shared applications such as office automation, and a personal directory where files any individual has made may be kept.

Fluctuating transitional levels may happen, like "superuser", to permit the system administrator to assign particular daily tasks.

Typical protection to access to an account is through a password, which develops a vulnerability; for example, any hacker who can crack the account can then use different tools to then crack the root account and attain access to the whole network.

As the passwords are simpler to crack, in the same manner they are also

easy target for password crackers; on the other hand, those that are problematic to speculate, provide improved security, however users are additionally possible to note them down due to the fact that they are also tough to remember, therefore growing risk of compromise.

An experiment by Daniel Klein of the Software Engineering Institute at Carnegie-Mellon University discovered the comparative ease with which an intimidating party could attain access to a network.

As discovered by Daniel Klein "Using 15,000 actual passwords supplied by systems administrators, applied various common cracking programs, and within 15 minutes cracked 368 passwords." Subsequently to the initial week of testing, the number grew to approximately 3,000 passwords, 21% of the tested sample.

Effective password security can be ensured by system administrators only by motivating users to select passwords that are simple for each of them to recall but which are not fabricated of general phrases or words, and by frequently using their own password crackers to recognize vulnerabilities.

Password security again is only strong as long as the system administrator has the time, energy, and influence to apply it.

PATCHING KNOWN VULNERABILITIES

The SANS institute identified most common internet security weaknesses as January 2001, none of which had already been recognized in 1999 and one of them in 1998.

There are measures to fix all of them, yet they remain to be the frequently exploited security bugs. As stated by the report of SANS, "attackers are opportunistic, [t]hey count on organizations not fixing the problems, and they often attack indiscriminately, by scanning the Internet for vulnerable systems."

However, system administrators report that they could not fix all of these flaws as they basically do not have the information of which of over 500 possible difficulties are the ones that are most hazardous, and also, they are too occupied already to fix them all.

Detection of intrusion and adaptive response tools

Application logs and processes are scanned by the Intrusion detection software which are watching for abnormal activity.

Abnormal activities are ones which the system administrator defines while configuring the software.

This will then alert the system administrator to take any action. The latest development is adaptive response tools. They comrade intrusion detection software with automated responses. They permit a network to "defend itself" counter to attacks.

Conclusion to Passive Defenses

As wrote by Sun Tzu, "if he [the enemy] does not know where I intend to give battle, he must prepare in a great many places." Passive defense has the issue that it is as strong as its feeblest part. The problem is that a hacker is only required to discover only one available weakness to attain access to a system.

As reported by the SANS Institute, "the problem is not that these are hidden holes only a few security flaws account for the majority of security incidents, and these are already well known." It is usually recognized that hackers do not attack particular servers so much as they guise for those which have weak security, which would recommend that a beleaguered computer network attack is improbable.

Though, the positive dispersions of Microsoft and Security Focus demonstrate that with adequate training, and also carelessness on the part of even a single employee or a very well-hidden computer network attack tool, the prior is positively conceivable.

Promise is shown by adaptive response tools however, for the maximum part passive defenses are only as sufficient as the system administrators and users who contribute in them, and in any circumstance, they surrender the initiative to the hacker.

Active attacks



Figure 8.1: weapons to active attacks

The previously discussed electronic weapons may or may not exist but the presence of the theory does demonstrate that some of the hindrance system administrators sense while dealing with common networking attack. Passive defenses not only relinquish the resourcefulness to the attacker, but additionally they flop to carry inside themselves any direct threat of counteraction.

In the following description, diverse possible active defenses, the needed fundamentals for each are discussed and then limit probable outcomes.

Pre-emptive Attacks

Air Force policy embraces that the greatest efficient methods of counteracting an enemy's aggressive aerospace latent is by attacking its aerospace forces and their support structures.

On the other hand, should an enemy's computer network attack assets not be susceptible to preemptive action, real attacks on its information infrastructure might also stop or disturb its computer network attack efforts.

By investigating both the prerequisites for a fruitful computer network attacks and the probable consequences, any individual can regulate whether any of these representations of preemptive attack is a hands-on option.

In the meantime, preemptive attack is by description an antagonistic act, expertise authorities are probable to favor it individually for use in contradiction of previously distinct hostile state and non-state actors, and 17 even then only if they have sensible guarantees that the attack 's influences can be limited to the intimidating actor 's network.

The main expectations fundamental preemptive attack policy is that the enemy 's aggressive forces and/ or their provision edifices can be situated and either incapacitated or demolished beforehand they can be efficiently used. Finding an enemy 's computer network attack pressurizes itself and grants a hard problem.

In the meantime, the "weapons" themselves are the software applications, and are confined and used in computer networks alike to those that occur in corporate offices and bureaucracies, physical signatures are immaterial.

Computer Network Exploitation agreed through the Internet might find a possible attacker, offensive "weapons", but then again meanwhile there is no requirement to attach them to the Internet up until prepared to attack, this is improbable.

One improved choice might be to attack any scanners, sniffers, and password crackers started functioning on enemy networks. Meanwhile these are also defensive tools, such preventive attacks will also progress welcoming attacking efforts, and may in fact previously be ongoing as share of friendly computer networking attack activities.

A detailed examination of the enemy 's networks might disclose these possessions, but this should be intelligent to overthrow all its defenses if it is to make available a whole response, and this will be very time consuming.

More quick and precise identification

of attacker can be done by detection and tracing of the efforts of attacker to scan any network. even though, there is no surety that they will find out the actual basis of the attack.

The network which gives an impression of being the basis of attack might merely be the in-between connection which is taken in use by the hacker to mislead from the actual basis, meanwhile hackers have the equipment that can remove sign of their doings, such as utclean.c and tlnthide.c.

Otherwise, the attacker might also be operating its computer network exploitation from a unbiassed or even welcoming network that the attacker may also have already conceded. In the prior case offending its computer network exploitation tools is at the finest difficult and at nastiest unbearable for tactful when there are no mechanical reasons, and in whichever case the protector can refute one computer network exploitation capability but then also it has not achieved to damage its enemy's own network.

Following, though establishments in impartial and welcoming countries may be eager to agree to searching of their webs to back law enforcement, they may be not as much of eager to do so in support of a preventive computer network attack.

Had better any share of the enemy's power been positioned; a computer network exploitation of the enemy's passive defenses is desired to plan out the enemy 's network and permit a fruitful preemptive attack to be intentional.

This will consume additional time, and if the target for preemptive attack was found by tracing an adversary computer network exploitation effort, the enemy 's attack may start early, or even be in progress.

For an additional comprehensive conversation of directing thoughts in scheduling computer network attack, as in "Operationalizing" Information Operations by Major John Glock.

A significant warning comes into action if the network which carries the target for the preemptive attack does not fit to the intimidating entity, as is particularly probable when the enemy is a non-state actor: computer network attack in contradiction to a network in a unbiassed or welcoming country is rather of expertise authorities who are probable to be very cautious, even if such an attack is governed to be permissible under national and international law.

If the enemy's computer network attack pressurizes themselves are not locatable or weak, additional option might be to depend on the invasive against the enemy's information infrastructure to anticipate its computer network attack.

A fruitful effort there will expected to make it additionally problematic to unveil attacks from in place assets,

though the movability of computer network attack "weapons", that can be burdened from disconnected intranets to laptops, means this is distant from a whole response.

Retaliations

Meanwhile the basis and features of an enemy common network attack are improbable to seeming till it is really in improvement, additional choice for active defense is counterattack.

Though prerequisites for counterattacks are alike to individuals for any other common network attack (with preemptive attacks), the circumstances below which they must be skillful are dissimilar. As for preemptive attacks, the basis of the attack must be positioned and perused for weaknesses, IPB performed, and the attack carried out.

Contrasting preemptive attack, nevertheless, all these tasks must be accomplished earlier than the attacker finishes its attack and eliminates the network presenting its "weapons" from the Internet.

Initially, a counterattack will need following the original attack posterior to the basis, just like tracing enemy investigations in addition of preemptive attacks, with numerous of the similar drawbacks together with the chance a network might be misidentified as the basis.

While sociable countries are probable to take a much more promising opinion of tracing hackers over their networks once an attack is in progress, there is no assurance neutrals will.

Also, despite the fact international contracts enable tracing hackers through other countries 'networks for law implementation drives, alike contracts for armed drives will be lone between the US and friendly nations.

Additionally, even if the basis is dependably situated, the time available for searching and IPB is improbable to be adequate.

When the computer network exploitation has been skilled, the real attack takes comparatively slight time, and meanwhile by meaning the attacker is somebody who should distinguish the time obligatory for making an effective attack, it is not likely that it will take extended than that to implement its own.

Though it is likely to decrease the training time by start it as soon as a enquiry is noticed, an enemy who reviews from one network and attacks from another mechanically refutes this counterattack. While counterattacks on the enemy 's computer network exploitation competence is improbable to prevent an attack, meanwhile the concluding is probable to start long formerly the 20 defenders 's IPB is even partly comprehensive, it can anticipate following attacks.

Finally, a full-sized computer

network attack on an enemy 's information infrastructure may disagree any indigenously created computer network attack and computer network exploitation initiatives the access to the Internet they essential, nonetheless will not disturb any teams by now organized outside the intimidating country.

Also, a competence can be reconstructed comparatively fast, meanwhile computer network attack and computer network exploitation tools and employees can effortlessly be organized to other nations where they can recover access.

EFFECTS OF POSITIVE PRE-EMPTIVE OR COUNTERATTACKS

When making assumptions about a preemptive or counterattack which can be positively launched, then also deliberate any effects which it may have.

Terminating or destructing the computers from which an opponent strategizes to launch a computer network attack is possible to have only a momentary effect, as the computers themselves are comparatively inexpensive in the background of governments 'or even terrorist groups 'military expenditures, and damaged software together with "weapons" can be rapidly substituted from backups. The actual midpoint of significance is the knowledge of hacker.

Misleading initiatives are more probable to be more efficient; positive preemptive attacks and/or counterattacks to change an adversary 's CNE competences can successfully "blind" its common networking attack forces, till the time that the change is not revealed.

After it is done, the challenger can swiftly reestablish its ability from backup sources and transmit on as earlier, however at the cost of missing time.

Active Deception

The alternate approach to passive defense is the active deception. As an alternative of trying to have impostors out of the network, it will require to send them into an untrue network, entirely occupied with the similar type of data and network resources that would be on an actual one, that happens exclusively to betray them.

There are particular set of prerequisites to active deception, all of which will be discussed in the following.

Though it may not reason real harm to the attacker 's system, it does enforce attacker to waste effort for no profit, and permits the protector to perceive attacker's techniques and probably apprehend its tools, and consequently offers the time and knowledge to generate barricades against them.

Moreover, by generating the incorrect imprint that the attack has been fruitful, active deception additionally misrepresents the opponent 's task study of the efficiency of the common networking attack effort.

AMAZING FACTS!!!

Some types of malware contains files commonly identified as Trajan viruses. Others leave your computer vulnerable to viruses. Regardless of type, malware is notorious for being at the root, whether directly or indirectly, of virus infection, causing conflicts with legitimate software and compromising the security of any operating system, windows or Macintash.

Fundamentals for Active Deception

A real defense be able to discriminate among the attackers and legitimate users. The most unassuming method to do this is to offer a consumable weakness "trap door" which will result it into the simulated dummy network, for instance, an unprotected port or a user account with a password susceptible to a password cracker.

Additional resources might be to fit a solution for a recognized vulnerability, then make use of an adaptive response tool that distinguishes the signature of the attack that deeds it, and permits the invader into the fake network.

To be actually active to the trap door will have to be changed frequently, due to the reason once it is documented as such, it is no elongated beneficial and the attacker will distillate on discovering actual weaknesses.

Additionally, like all trick initiatives, the fake network will have to produce data that creates the attacker 's initiatives seem to be operative.

At least it should comprise invented user accounts, wide-ranging with casually rationalized user files including untrue but possible information along

with sufficient true information to offer trustworthiness to the deception, and computer network attack applications.

It should be made up of more than a few sub compartments, each with its own set of made-up users and established data.

Active and Passive Defence Communication

A time to prepare for an attack is a general prerequisite for both preemptive and counterattack forms of active defense.

The methods which can actually delay the success of an enemy common Passive defenses and active deception are both methods that can delay the success of an enemy 's computer network attack, and therefore should underwrite to the achievement of any preemptive or counterattacks.

In the same way, any attack on an enemy's network which decreases its capability to examine responsive networks will in chance upsurge the efficiency of passive defenses.

For these explanations, active defense should be measured end to end with passive defenses relatively than self-governing of them.

Although passive defenses cannot shelter their vital feebleness, that they concede the ingenuity to the enemy and that they depend upon imperfect human activity to uphold them, there is still much that can be done to reinforce them before resorting to active defense. Active deception and counterattacks passed out correctly established units can contribute meaningfully to the security of the US DII.

The US IO community should discover development in these areas to help guarantee information dominance in all upcoming battles.

REVIEW QUESTION

1. Discuss the measures to counter passive attacks.
2. What are pre-emptive attacks? Discuss different types of pre-emptive attacks.
3. What are the effects of positive pre-emptive or counter attacks?
4. Discuss active deception, what are the fundamentals for active deception?
5. Explain active and passive defense communication in brief.

CHAPTER 9

SECURITY MEASURES FOR ROUTING PROTOCOLS AND IEEE STANDARDS

LEARNING OBJECTIVES

- How to get protected of attacks in routing
- Defending on Sybil attack
- Making privacy to defend in the network
- Approach to solve the privacy problem
- Basic standards of IEEE
- Physical and logical networking concept of IEEE

PROTECTING AGAINST ATTACKS ON ROUTING PROTOCOLS

According to the recent research, the routing in wireless sensor network has been constantly focusing on providing the least energy consuming routing. However, there is requirement for both energy efficient and secure protocols in wireless sensor networks to prevent them from attacks in the network which could be sinkhole, Sybil attacks and wormhole.

Generally, the routing packet algorithm exchange the messages with the nodes in the sensor which are normally outside of the radio range. This is basically

different than the sensors which are in the range of radio where packets can be sent using one hop.

In a single hop there is more risk on the security which one should be concern about but it is more accurately transmitted to the address through multitasking and broadcasting.

The first packet in the routing algorithm is made up with the node identifiers which are same as the traditional routing. Here, each of the identifier is marked up with the address and the routing to the sensor which is based to the address.

In general, it is taken as inefficient in the field of sensor network as the nodes are marked by their location instead of their identifiers.

In respond to the distaste of routing which is based on identifiers node are geographically routing the protocol which has been introduced. GPRS is one of the most common routing protocol which allows the nodes to send packets to some particular region instead of a particular node.

These kinds of routing protocol let someone use themselves gently with the concept of data-centric networks. There are many security perspectives as well in regards of these nodes which are explained further.

These techniques to secure the routing protocols two scientist proposed a theory named Deng Han and Mishra. They proposed that "an intrusion tolerant routing protocol, INSENS that is designed to limit the scope of an intruder's destruction and route despite network intrusion without having to identify the intruder and the TRANS routing protocol is designed for use in data centric networks.

It also makes use of a loose-time synchronization asymmetric cryptographic scheme to ensure message confidentiality." In the implementation of TESLA, it is necessary to ensure that the message confidentiality and authentication is properly maintained.

With the use of μTESLA and TRANS, we make sure that the message which we send is along with the path of trusted nodes while one is using location aware routing.

One specific challenge to make secure routing is wireless sensor network is to make sure that each of the single node is disrupt the entire routing protocol just by disrupting the route of discovery process.

Papadimitratos and Haas propose that "a secure route discovery protocol that guarantees, subject to several conditions, that correct topological information will be obtained.

The security relies on the MAC and an accumulation of the node identities along the route traversed by a message. In so doing, a source can discover the sensor network topology as each node along the route from source to destination appends its

identity to the message." In order to make sure that the message we sent are not being or not have been tempered then a MAC is made and it can be cross checked at both of the place which are source and the destination. This problem is related to the concept of wormholes in the sensor network.

Here a wormhole attack is one in which an infected node spy on a packet or a group of packets, and route them through the sensor network to another infected node which act as a pirate in the system, then it keeps a copy of the packet and replays it.

This can also be done to misrepresent the distance between the two colluding nodes. It is also being used in more general disrupt the routing protocol by misleading the discovery of neighbours process.

We have often seen that the additional hardware which is directional antenna is used to prevent themselves from the wormhole attacks. This process can be more cost prohibitive when it is counted for the deployment of large-scale network.

Two another scientist named Wang and Bhargava used the approach of visualization which was used to identify the wormholes. "They first compute a distance estimation between all neighbour sensors, including possible existing wormholes.

Using multi-dimensional scaling, they then compute a virtual layout of the sensor network. A surface smoothing strategy is then used to adjust for round-off errors in the multi-dimensional scaling.

Finally, the shape of the resulting virtual network is analysed. If a wormhole exists within the network, the shape of the virtual network will bend and curve towards the offending nodes. Using this strategy, the nodes that participate in the wormhole can be identified and removed from the network.

If a network does not contain a wormhole, the virtual network will appear flat."

DEFENDING AGAINST THE SYBIL ATTACK

In order to defend against the Sybil attack, there should be validation at each of the nodes identity because it is the only identity which is shown to the representing physical node. There are basically two ways to validate the identity.

In the first way we use the validation of direction. In this way one node is directly tested to whether another of the node identity is valid or not and in the other way to validate the identity the nodes are already been verified and are allowed to confirm for or prove another node.

There is an exception of key pool defense, in this mechanism "we present here are for direct validation. We leave secure methods of indirect validation as future work. Previous Defences Douceur proposes resource testing as a method of direct validation.

In resource testing, it is assumed that each physical entity is limited in some resource. The verifier tests whether identities correspond to different physical entities by verifying that each identity has as much of the tested resource as a physical device." This resource was proposed by the Douceur.

The purpose behind this resource was to storage, computation and communication. Storage and computation are not suitable in the field of wireless network as the hackers may attack it by using a physical device with higher magnitude.

By this more storage and computational ability is resourced to starved sensor node. This method was proposed of the testing communication was to "broadcast a request for identities and then only accept replies that occur within a given time interval.

This method is also unsuitable for wireless sensor networks because all the replies converging at the verifier will result in that part of the network becoming congested."

In the section of remainder of this section, there were several defenses proposed against the Sybil attack in the sensor network which also included the verification of key sets for random key, radio resource testing, position verification and pre-distribution of random keys. It also provides quantitative analysis for the defense.

In order to defend this Sybil attack, the network needs to have a mechanism to valid the particular identity of the identity which is provided in the physical node. Newsome et al. proposed two methods to prove the identities which were Direct and Indirect validation.

"In direct validation a trusted node directly tests whether the joining identity is valid. In indirect validation, another trusted node is allowed to vouch for (or against) the validity of a joining node.

Newsome et al. primarily describe direct validation techniques, including a radio resource test." In this radio test, one of the node is assigned for each of their neighbor for some another channel in which they usually communicate. Then this node randomly chooses one of the channel and listens to it.

If there is a detection on the transmission of one channel then it is assumed that the node which is transmitting is physical node.

In the same way, if any of the node is not detecting any of the transmission in a specified channel then the node is assumed to have the identity assigned to the channel then it is not the physical node.

One another technique to get protected against the Sybil attack is the random use of key to pre-distribution techniques. The basic idea behind this technique is that in a given number of keys in a key ring, there is a node which is randomly keeps on generating the identities will not possess more keys to adapt many identities.

Thus, it will be unable to exchange the messages on the network because of the fact that invalid identity will not be able for the process of encryption as well as decryption.

Detecting Node Replication Attacks is an important part of WSN networks. This is already discussed that the static WSN is not a very effective technology in the mobile WSN. The detection of mobile in WSN in the process of node replication attack is basically sorted into two categories.

1. Centralized
2. Distributed

DEFENDING ON THE ATTACKS IN PRIVACY SENSOR

With regards of the attacks on the privacy, there is effective techniques which is used to encounter many of the attacks imposed against the sensor. Here are some of the common techniques which are locating information of a user or track the movement which is feasible. This is considered as a threat to the privacy of an individual or enterprise.

Mechanism of anonymity depersonalize the data even before the release of data which present an alternative to the privacy policy based control.

The researchers have even discussed on the approaches which were using the anonymity mechanism as for example Grunewald and Gruteser proposed "as to analyse the feasibility of anonym zing location information for location-based services in an automotive telematics environment.

Beresford and Stajano independently evaluate anonymity techniques for an indoor location system based on the Active Bat. Total anonymity is a difficult problem given the lack of knowledge concerning a node's location."

Thus, it is required to trade-off is required between anonymity and the need for the information of public when solving of privacy problems. The four main approaches which were proposed was:

Decentralize Sensitive Data

The basic idea of this approach is to distribute the sensed location data through a spanning tree, so that no single node holds a complete view of the original data.

Secure Communication Channel

Using secure communication protocols, such as SPINS in which the eavesdropping and active attacks can be prevented.

Change Data Traffic

De-patterning the data transmissions can protect against traffic analysis. For example, inserting some bogus data can intensively change the traffic pattern when needed.

Node Mobility

Making the sensor movable can be effective in defending privacy, especially the location. For example, the Cricket system is a location-support system for in-building, mobile, location dependent applications.

It allows applications running on mobile and static nodes to learn their physical location by using listeners that hear and analyse information from beacons spread throughout the building.

Thus, the location sensors can be placed on the mobile device as opposed to the building infrastructure, and the location information is not disclosed during the position determination process and the data subject can choose the parties to which the information should be transmitted.

The approaches which are policy based are now a day a hot topic to address the problem of privacy. The access control authentication and decisions which are made are based on the privacy policies specification.

Two scientist names Wagner and Molnar proposed a concept of "private authentication, and give a general scheme for building private authentication with work logarithmic in the number of tags in (but not limited by) RFID (Radio Frequency Identification) applications.

In the automotive telematics domain, Duri et al. propose a policy-based

framework for protecting sensor information, where an in-car computer can act as a trusted agent."

After that Snekkenes showed some advanced concept for specifying policies which was "in the context of a mobile phone network. These concepts enable access control based on criteria such as time of the request, location, speed, and identity of the located object.

Myles and colleagues describe an architecture for a centralized location server that controls access from client applications through a set of validator modules that check XML-encoded application privacy policies." Steenkiste and Hengarther together pointed out that "access control decisions can be governed by either room or user policies.

The room policy specifies who is permitted to find out about the people currently in a room, while the user policy states who is allowed to get location information about another user."

To claim this access control Ozturk et al. gave an anti-traffic analysis mechanism in order to "an outside attacker from tracking the location of a data source, since that information will release the location of sensed objects.

The randomized data routing mechanism and phantom traffic generation mechanism are used to disguise the real data traffic, so that it is difficult for an adversary to track the source of data by analysing network traffic." There are several similar mechanisms which are also being used in order to disguise an opponent from finding the location of a base station by figuring out the network traffic.

The major problem for the analysis of anti-traffic analysis mechanism is the cost of energy occurred by anonymization.

There is one more strategy which is used to hide the location of information from eavesdroppers which was proposed by two way greedy random-walk strategy GROW (Greedy Random Walk), it said "Threats to node privacy can also come from specific application protocols such as the data aggregation protocol.

Threat to privacy data aggregation which is in a new privacy-preserving aggregation protocol is presented."

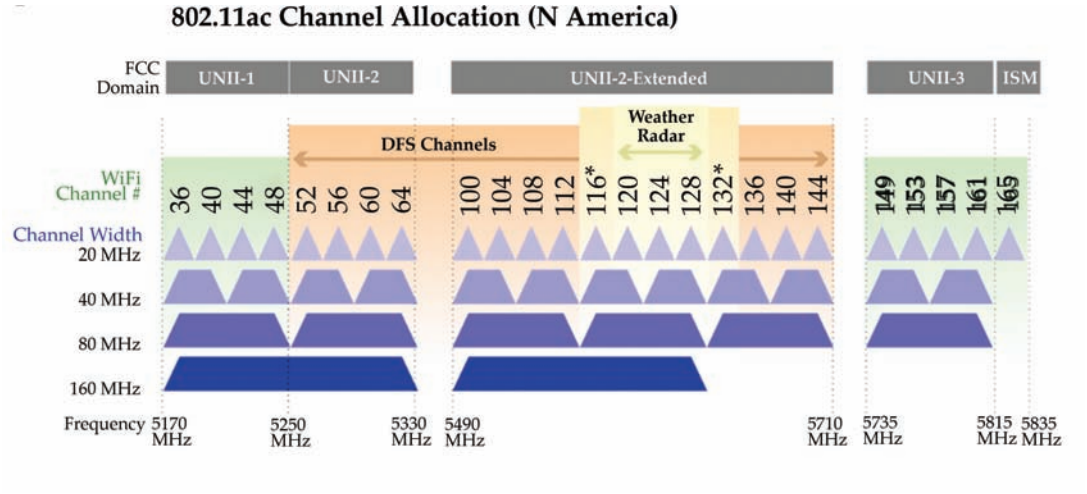


Figure 9.1: Non-overlapping channels

BASIC IEEE STANDARDS AND THEIR CONCEPTS

Table 9.1: basic standards and networking concepts

802	Overview	Basics of physical and logical networking concepts.
802.1	Bridging	LAN/MAN bridging and management. Covers management and the lower sub-layers of OSI Layer 2, including MAC-based bridging (Media Access Control), virtual LANs and port-based access control.
802.2	Logical Link	Commonly referred to as the LLC or Logical Link Control specification. The LLC is the top sub-layer in the data-link layer, OSI Layer 2. Interfaces with the network Layer 3.
802.3	Ethernet	"Grandaddy" of the 802 specifications. Provides asynchronous networking using "carrier sense, multiple access with collision detect" (CSMA/CD) over coax, twisted-pair copper, and fibre media. Current speeds range from 10 Mbps to 10 Gbps.
802.4	Token Bus	Disbanded

802.5	Token Ring	The original token-passing standard for twisted-pair, shielded copper cables. Supports copper and fibre cabling from 4 Mbps to 100 Mbps. Often called "IBM Token-Ring."
802.6	Distributed queue dual bus (DQDB)	"Superseded, Revision of 802.1D-1990 edition (ISO/IEC 10038). 802.1D incorporates P802.1p and P802.12e. It also incorporates and supersedes published standards 802.1j and 802.6k. Superseded by 802.1D-2004."
802.7	Broadband LAN Practices	Withdrawn Standard. Withdrawn Date: Feb 07, 2003. No longer endorsed by the IEEE.
802.8	Fibre Optic Practices	Withdrawn PAR. Standards project no longer endorsed by the IEEE.
802.9	Integrated Services LAN	Withdrawn PAR. Standards project no longer endorsed by the IEEE.
802.10	Interoperable LAN security	Superseded, Contains: IEEE Std 802.10b-1992.
802.11	Wi-Fi	Wireless LAN Media Access Control and Physical Layer specification. 802.11a, b, g, etc. are amendments to the original 802.11 standard. Products that implement 802.11 standards must pass tests and are referred to as "Wi-Fi certified."
802.11a		Specifies a PHY that operates in the 5 GHz U-NII band in the US - initially 5.15-5.35 AND 5.725-5.85 - since expanded to additional frequencies Uses Orthogonal Frequency-Division Multiplexing Enhanced data speed to 54 Mbps Ratified after 802.11b
802.11b		Enhancement to 802.11 that added higher data rate modes to the DSSS (Direct Sequence Spread Spectrum) already defined in the original 802.11 standard Boosted data speed to 11 Mbps 22 MHz Bandwidth yields 3 non-overlapping channels in the frequency range of 2.400 GHz to 2.4835 GHz Beacons at 1 Mbps, falls back to 5.5, 2, or 1 Mbps from 11 Mbps max.

802.11d		Enhancement to 802.11a and 802.11b that allows for global roaming Particulars can be set at Media Access Control (MAC) layer
802.11e		Enhancement to 802.11 that includes quality of service (QoS) features Facilitates prioritization of data, voice, and video transmissions
802.11g		Extends the maximum data rate of WLAN devices that operate in the 2.4 GHz band, in a fashion that permits interoperation with 802.11b devices Uses OFDM Modulation (Orthogonal FDM) Operates at up to 54 megabits per second (Mbps), with fall-back speeds that include the "b" speeds
802.11h		Enhancement to 802.11a that resolves interference issues Dynamic frequency selection (DFS) Transmit power control (TPC)
802.11i		Enhancement to 802.11 that offers additional security for WLAN applications Defines more robust encryption, authentication, and key exchange, as well as options for key caching and pre-authentication
802.11j		Japanese regulatory extensions to 802.11a specification Frequency range 4.9 GHz to 5.0 GHz
802.11k		Radio resource measurements for networks using 802.11 family specifications
802.11m		Maintenance of 802.11 family specifications Corrections and amendments to existing documentation

802.11n		Higher-speed standards Several competing and non-compatible technologies; often called "pre-n" Top speeds claimed of 108, 240, and 350+ MHz Competing proposals come from the groups, EWC, TGn Sync, and WWiSE and are all variations based on MIMO (multiple input, multiple output)
802.11x		Mis-used "generic" term for 802.11 family specifications
802.12	Demand Priority	Increases Ethernet data rate to 100 Mbps by controlling media utilization.
802.13	Not used	Not used
802.14	Cable modems	Withdrawn PAR. Standards project no longer endorsed by the IEEE.
802.15	**Wireless Personal Area Networks**	Communications specification that was approved in early 2002 by the IEEE for wireless personal area networks (WPANs).
802.15.1	Bluetooth	Short range (10m) wireless technology for cordless mouse, keyboard, and hands-free headset at 2.4 GHz.
802.15.3a	UWB	Short range, high-bandwidth "ultra-wideband" link
802.15.4	ZigBee	Short range wireless sensor networks
802.15.5	Mesh Network	Extension of network coverage without increasing the transmit power or the receiver sensitivity Enhanced reliability via route redundancy Easier network configuration - Better device battery life
802.16	Wireless Metropolitan Area Networks	This family of standards covers Fixed and Mobile Broadband Wireless Access methods used to create Wireless Metropolitan Area Networks (WMANs.) Connects Base Stations to the Internet using OFDM in unlicensed (900 MHz, 2.4, 5.8 GHz) or licensed (700 MHz, 2.5 – 3.6 GHz) frequency bands. Products that implement 802.16 standards can undergo WiMAX certification testing.
802.17	Resilient Packet Ring	IEEE working group description

802.18	Radio Regulatory TAG	IEEE 802.18 standards committee
802.19	Coexistence	IEEE 802.19 Coexistence Technical Advisory Group
802.20	Mobile Broadband Wireless Access	IEEE 802.20 mission and project scope
802.21	Media Independent Handoff	IEEE 802.21 mission and project scope
802.22	Wireless Regional Area Network	IEEE 802.22 mission and project scope

AMAZING FACTS!!!

Interbrand invented the Interbrand invented the term "Wi-Fi" as a play on words of the term "Hi-Fi" or "High Fidelity". However, Wi-Fi doesn't actually stand for anything. What added to the confusion was the Wi-Fi alliance's use of a nosense advertising slogon, "The Standard for Wirelsess Fidelity," which lead many people to think that Wi-Fi was an abbreviation of "Wireless Fidelity".

REVIEW QUESTIONS

1. What are the measures taken to provide protection against attacks on routing protocol?
2. How can the Sybil attack countered?
3. Discuss the steps taken to prevent the attack against privacy sensors?
4. What are the different types of secure communication channels?
5. Discuss the IEEE basic standards in brief.

CHAPTER 10

SECURITY GOALS IN WIRELESS COMMUNICATION AND ISSUES

LEARNING OBJECTIVES

- Introduction to security goals in wireless network security
- Authentication of data for security in wireless network
- Using encryption for confidentiality purpose
- Integrity, service reliability and availability for making data confidential
- What is protocol?
- Introduction to wired equivalent privacy
- Advantages of WPA over WEP
- What is Virtual private network?
- Wireless security privacy
- Security challenges in wireless security
- Basic issues in Wi-Fi network
- Challenges in Mobile Data
- Multiplicity of connections as a goal in wireless network

INTRODUCTION

The wireless communication has made the day-to-day life very convenient and easy by providing the flexibility of communication without having a negative impact on communicated content.

The wireless communication technology has made its place in every possible location like majorly in houses, corporate offices spaces and with the technological advancements the facility of wireless fidelity (Wi-Fi) can also be seen on the mobile vehicles.

Since the inception of wireless communication, the security concerns are always the part of discussion as in wireless communication the data transfer takes place in space taking the space as a channel as contrary to the wired communication that uses the physical wires as the channel.

Security concerns are a grave problem when it comes to the wireless networking, and not only the big organisations are facing these issues but also the enterprises that are operating on a small scale.

Everyone these days, is busy in enjoying the benefits of the wireless communication and ignoring the very basic requirement of a communication; Security.

Due to the nature of the transmission channel of wireless communication, it is vulnerable to attacks like active jamming or passive eavesdropping as it is not a tough job to execute for the professional hackers.

Hence, it is very important to protect the data in the open air as it generally contain private, sensitive and confidential data and a leak in channel can cost the losses in billions of dollars. (Zhang et al, 2017).

For example, considering a case in healthcare sector, there are numerous sensors used to collect private and highly confidential information on patient's health such as blood pressure, heart rates, ECG, MRI, CT-Scan, and many more. To transmit this information a secure transmission channel is needed.

However, the systems used are full of vulnerabilities and are far from being safe and secure. (Grau, 2015). To overcome this query the security countermeasures are developed. These measures are divided into information-theoretic security and computational security (Zou,2016).

The latter part is the one that deals in protecting the wireless communication system by deploying the protocols and cryptographic algorithms at the upper layer of protocol stack. (Granjal, 2015) For example, Wi-Fi Protected Access (WPA) is developed in order to secure the media access control (MAC) layer as mentioned in the IEEE 802.11 systems (Technical Report 802.11i). A classical cryptosystem is shown in the figure below, which uses both public key cryptography

(PKC) and symmetric encryption. PKC is used for key distribution and symmetric encryption methodology for data protection. In figure, there are two legitimate users, Alice and Bob, who want to communicate privately and securely.

On one hand, PKC distributes the same session key to both users by employing discrete algorithms achieved by exploiting the computational hardness of mathematical problems and on other hand, symmetric encryption takes place in the upper layers; MAC layer or data link layer and above, which allows the encryption of plain text by using the common session key only, which is shared by users using PKC.

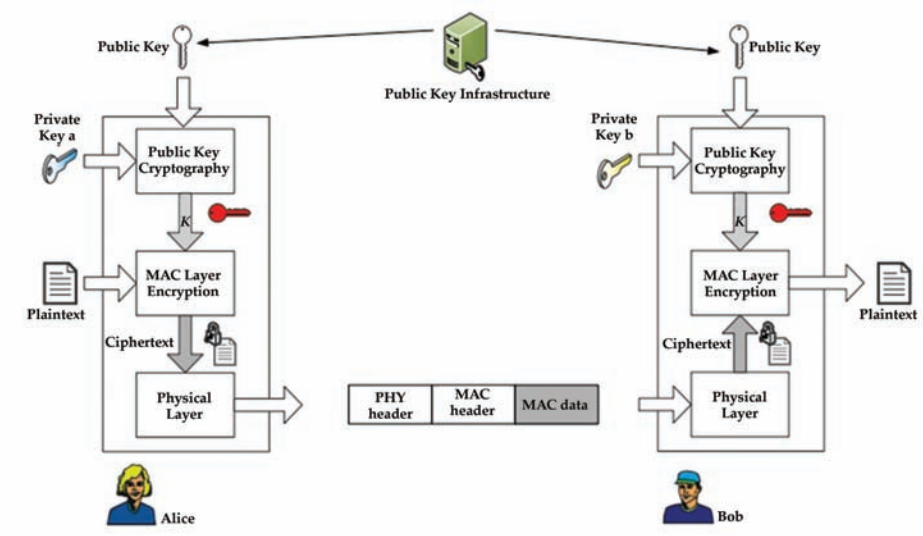


Figure 10.1: Classic cryptosystem with media access control (MAC) layer encryption as an example. The grey blocks represent the encrypted data.

There is no dearth of the issues that are related to security and privacy of confidential information when the wireless communication channels are used in transmission of data. The main concern regarding the security arises due to the fact that the data transmission in wireless networks takes place through the air via radio waves, and this is very prone to phishing and interception from unauthorised personnel.

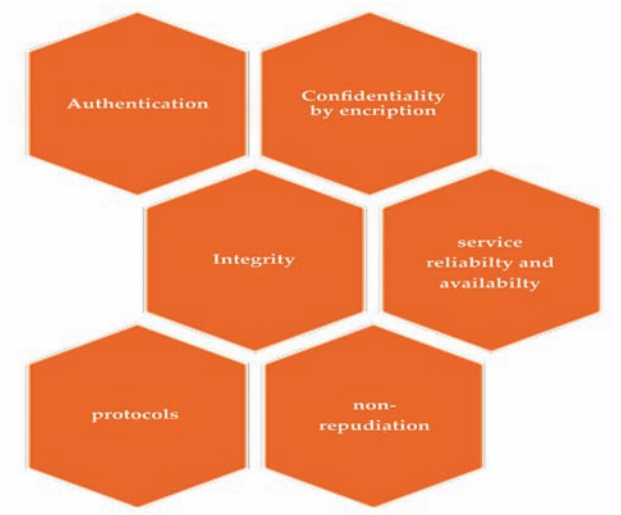


Figure 10.2: security elements/goals

SECURITY GOALS/ELEMENTS

These protocols are described in coming sections, but first let's discuss the security goals that every system must provide. These security goals are implemented in order to make sure that the system is providing the sufficient secrecy and privacy to the network. These goals can be listed a following five goals (Earle, 2005) (Imai, 2006):

DID YOU KNOW ?

In 1992, Vinton G. Cerf, VP, Know as the "Father of the Internet," First predicted that IP would appear on everything. He also ware a controversial T-shirt with the phrase, which apparently caused quite the stir at the time.

Authentication

This goal focuses on the identity authentication of the sender and receiver before the data is being sent or received. As we are dealing in wireless communication there is no physical channel present and hence to ensure the authenticity of sender and receiver is very important.

To make sure of authenticity in very first step is crucial because even with the presence of a secure standard set for the wireless communication by the

leading organisations for example the 802.1x suite, there still exists the gaps that are very risky from the security point of view.

In this suite, the transmitted information remains in its unprotected plain form for few seconds before it gets re-encrypted into the other format. These few seconds are more than enough for the information criminals to invade and take away the data.

Confidentiality by Encryption

Generally, this goal is about the perception of people about a secure system.

Once the authenticity of sender and receiver is confirmed, the next goal is to make sure that the delivered message is only interpreted by the intended personnel and no one else.

In this step, certain encryption techniques are used and the keys to the information is shared only by the sender and receiver.

In general terms, encryption is like creating a secret code, by translating the data into gibberish information that only the intended recipient can understand. In case when there are multiple receivers a public key is issued by the sender and transmitted to the intended receivers. The receiver with the combination of public and private key can access the data. The most secured encryption uses very complicated keys, or algorithms, that keep on changing on regular basis to protect data.

Integrity

Integrity goal deals with the fact that there is no mid-way modification in the message delivered. It is achieved by ensuring that the content of the message is free from any data loss, eavesdropping or phishing between the end points (sender and receiver).

There are several ways to identify the same as the parity check bit or packet check sum in IP4 packets.

In parity check an addition parity bit, 0 or 1, is added to make the parity count in the message even or odd. These details are shared with the receiver. When the message is received by the receiver, he/she can check the parity bit and make sure that there is no data loss happened during the transmission.

The packet bit checksum in IPv4 or IPv4 header checksum is a simple message check used to protect the header of IPv4 data packets against data invasion/corruption. This checksum is 16 bits long and is a part of packet header. This checksum is calculated for header bytes only.

The cascaded ones' compliment is used in checksum i.e. the checksum is evaluated by creating the ones' compliment of ones' compliment sum of the 16-bit words of the header. To make sure that there is no corruption in the message, the result of the summation of IP header and checksum must be zero.

Non-Repudiation

This goal implies that there should be no miscommunication between the sender and receiver and none of them can falsely claim that they have sent or received a certain message.

It also makes sure that neither sender nor the receiver can deny the authenticity of their signature on the document.

As no means of communication is error-free, it is recommended that multiple approaches must be taken into consideration, for example taking unique biometric information of the sender and other authentic data of sender that would be not easy to reproduce/repudiate

SERVICE RELIABILITY AND AVAILABILITY

This goal has the aim to make sure that the user is getting the quality service up to the mark. As the secure systems are more prone to attack by the hackers and intruders, it is more likely that this may affect the system availability and reliability among the users.

To ensure that their intrusive attacks does not harm the system workings, the service reliability and availability came into force.

Protocols

The capability of a system to protect, manage and distribute confidential and private information determines the security standards for that system in digital communication. To maintain this, a set of rules and regulations are declared called Protocols.

Since the very beginning of the digital era, even before the wireless communication, data security has been a matter of concern because of the need of mankind to transmit the information whether it is for war time or in the time of peace with complete confidentiality.

For example, ENIGMA, the first and most famous device used by German military in times of WWII to encrypt the messages.

It was more of a simple typing machine with a scrambler unit to jumble the content of the messages and can only be decoded by someone that has the key.

It is impossible to contain the transmission signals within the physical boundaries of an organisation or a defined area as the radio waves are being used as a medium.

Since the data is not ravelling through physical mode i.e. the wired network, there is always a potential risk of an unauthorised access by ant spurious element without being present in the physical boundaries of the organisation or being attached to the network, which makes it impossible to track back the access location of the invasion. This all leads to the fact that it is not possible for the organisations to control the data being transmitted over a wireless network.

It signifies that secure use of wireless networks is based on users that are connected to the network through access points that are predetermined and are under surveillance in order to use the network securely.

The protocols extensively used are wired equivalent privacy protocol (WEP)/ HQi and the wireless fidelity (Wi-Fi) Protected Access Protocols (WPA or WPA2).

WIRED EQUIVALENT PRIVACY (WEP)

Wired Equivalent Privacy (WEP) is a set of protocol specially designed for wireless security, on the set guidelines according to the 802.11b standard.

Its main purpose is to encrypts data as soon as it goes wireless, over and above anything else you're using. It is a key-based protocol, and hence the user is expected to change the default key. It is also recommended that the user should create a unique WEP key for individual users when they first access the system.

It is also suggested by the researchers that the users must use WEP in combination with other wireless specific security measures.

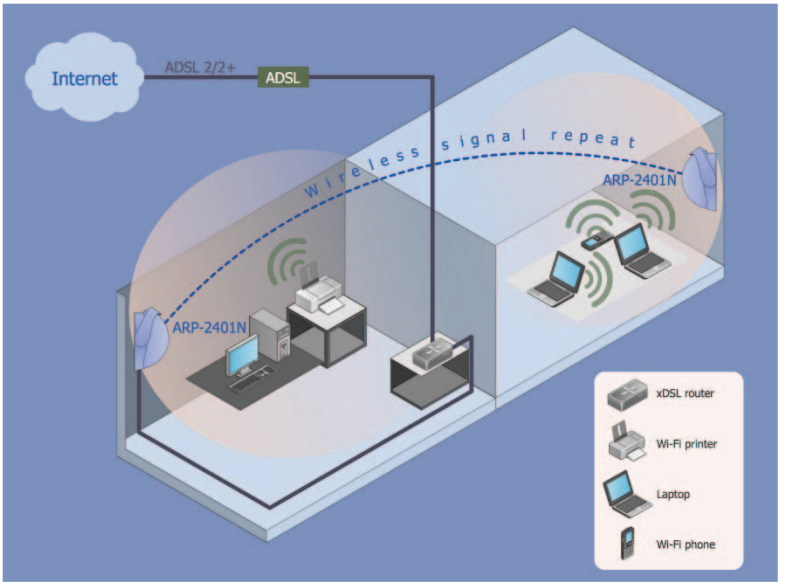


Figure 10.3: Wired Equivalent Privacy (WEP)

At the time of its introduction to market, the WEP security was believed to be impenetrably resistant to hackers and eavesdroppers. But soon enough, the popularity of wireless networks was huge and many researchers and crypt analysts found the flaws in the original WEP design.

Most of them believe that very less amount of time was dedicated in testing and review of the WEP protocol.

It is also claimed that many of the flaws and errors would have been caught in the early design phase only if the proper quality check was imposed and the protocol had been reviewed thoroughly.

The only thing that kept the WEP alive was the lack of availability of other security solutions as for most of the networking users especially home users, it was the only choice.

But the era of WEP fell soon enough post the introduction of new security mechanisms are added to the IEEE 802.11 standard. And as it is said "Something is better than nothing", WEP is still effective and better than no security at all, even when its weaknesses are known.

At least it will provide the basic security against unauthorised access to one's wireless network and prevent eating up of bandwidth. (Vibhuti, 2005).

WIRELESS PROTECTED ACCESS (WPA) AND WIRELESS PROTECTED ACCESS 2 (WPA2)

After the collapse of WEP, IEEE started developing a new security architecture called 802.11i.

Both WPA and WPA2 are standard-based security certifications that were issued by SMB, Wi-Fi Alliance for enterprise, and small home/office wireless LAN in order to provide a mutual authentication to verify individual users and advanced encryption.

WPA is known for providing Enterprise-class authentication while WPA2 is known for providing next generation security and support the standards of government grade encryption.

It is preferable that WPA and WPA2 should be used for enterprise and SMB wireless LAN operations.

These protocols are proficient in providing secure access control, active and passive attacks protection of the network, strong data encryption WPA2 protocol has a longer key and hence it provides a more safe and secure wireless network and a stronger encryption, as it takes a longer time and is not easy to decipher a 64-bit or a 128-bit key.

The main advantages that WPA control system has over WEP are:

- It is based on 802.1X authentication model (brief discussion in later sections)
- WPA has flexible authentication framework based on Extensible Authentication protocol (EAP)
- WPA has authentication based on strong protocols like transport Layer Security (TLS)
- WPA authentication process results in a shared section key which prevents session hijacking
- WPA has different functions like integrity and encryption which uses different keys that are derived from the session key with the help of a one-way function.
- WPA has improved integrity and encryption functions as compared to WEP.

Virtual Private Network (VPN)

A virtual private network (VPN), as the name suggests creates a virtual network by extending a private network into a public network. The VPN allows the users connected to the network to send or receive data across this virtual public network.

It projects the case as if each of the public network users are directly connected to the host private network.

The special feature of VPN is that the connected public users can enjoy the benefit from security, management and functionality of the private network. (Mason, 2002).

From security point of view, VPN provides effective security to the users who are wirelessly accessing the network while on the go or while they are away from their office.

VPN allows users to create a secure tunnel between two or more points on a network with the use of encryption, even if the transmission of encrypted data is taking place over unsecured networks such as open or public internet.

Policies for Wireless Security

Many a times, it is required to have different security settings for different user groups under a same network. Virtual LAN (VLAN) can be very useful in establishing these kind of security settings on the access point.

For example, VPAN gives user the ability to set up different security standards or policies for different user groups within the same organisation such as legal, finance, HR or manufacturing.

It also gives the user the ability to set up separate security policies for partners, customers or visitors accessing the wireless LAN. This allows the cost-effective use of a single access point that can support multiple user groups which have different security requirements and settings, without compromising the security and privacy of the network.

Most of the enterprises that deploy or are planning to deploy the wireless LANs, want it to be a replacement for the wired LAN.

The organisations want the WLAN system to be integrated with the common management in order to keep the track of all activities and to increase the efficiency of network administrators.

The management tools can be used by resource-strapped SMBs to simplify and automate many time consuming and repetitive administrative tasks.

User policies are a very critical and important part of a good security system as wireless LAN security even when it is integrated with overall network management is only works if it is used consistently and across

the complete wireless LAN.

When setting and optimizing the LAN security practices, the people often tend to resist the temptation to overact. A majority of users do not get the point that there are massive gains by implementing wireless system in place.

The major challenge that developers face is to design a wireless LAN user policy such that it is simple enough for people to abide by on one hand and secure enough to protect the whole networking system on other.

These days, it's an easier balance to develop because WPA and WPA2 are built according to Wi-Fi certified access points and client devices.

WIRELESS CONNECTIVITY SECURITY CHALLENGES

The most talked about concern by the IT managers regarding the wireless networking is 'Security'. And this is a valid concern altogether as wireless communication works on the radio signals that are very much prone to the unauthorised access and incidents of eavesdropping to the extended propagation.

With all the technological advancements happening over the globe, there are many effective approaches for efficiently securing both cellular and Wi-Fi connections.

To understand this in a deeper sense, lets discuss the challenges related to wireless communication in greater detail.



The pigenons were used to communicate from one place to another wirelessly.

Issues for Wi-Fi Security

As discussed earlier, the initial Wi-Fi security

implemented was Wired Equivalency Protocol (WEP), that was completely inadequate and inefficient and was ineffective against any determined hacker to easily access or monitor connections over the network.

To overcome this protocol, a new Wi-Fi security standard, IEEE 802.111, was came into force.

This system has two iterations: WPA and WPA2. WPA was used to address all the deficiencies and WPA2 was particularly designed to bolster encryption by using standards such as Advanced Encryption Standards (AES).

WPA and WPA2 are based on IEEE 802.1X architecture, which is a port based security system where all the authentication related queries are handled by using Extensible Authentication Protocol (EAP) methods in conjunctions with systems such as RADIUS, known for their authentication expertise.

Most of the new devices support WPA and WPA2, both of which are reasonably secure. (Rysavy, 2005) For the organisations using IEEE 802.111 for Wi-Fi security, there exists a number of issues. Some of them are mentioned below:

1. IEEE 802.111 is not compatible with the older deployed equipment.
2. These standards only apply to the devices and equipment that are under the control of the organisation.
3. There are interoperability issues already arising among different vendor's equipment due to the complexity of IEEE 802.11i. To overcome this security gap in Wi-Fi, most of the vendors have modified their systems devices in order to implement security enhancements.

Many of the proposed enhancements make the users to buy the extra cards and access points from the vendor.

This dependency on vendors is also applicable to new WLAN architecture that employ a central controller to manage and coordinate access points.

The security features that are supported by these cards include detection of rogue access points and providing VPN tunnel end points.

However, the security benefits of these architectures are limited only to the directly connected WLAN nodes and are not extended to other connections, like Ethernet, or public connections.

Measures for mobile data

The security issues and concerns with the cellular- data connections are completely different from those in Wi-Fi. For example, in cellular data transmission, specialized equipment and devices are required to decode

and receive the radio signal by the attackers, whereas Wi-Fi attackers can use normal Wi-Fi hardware for their attacks.

The cost of such kind of specialized equipment by itself, however, is not enough to deter the attackers. As a result, this make it necessary for cellular networks to encrypt the radio links and signals.

The general trend is of 3G and 4G technologies in cellular networks and these telecom technologies are designed in order to offer very rigid security based on strong algorithms such as AES and Kasumi.

Even when the new technologies are widely available, the telecom companies are still using the older technologies for the areas that are less populated and to provide the latest technological services in these areas would be a loss-making proposal.

In these areas encryption is not always provided and even if your home system encrypts the link, you may still roam onto a partner network that does not. The concluding remark is that you cannot rely on the protection of the radio links.

Though both cellular and Wi-Fi connections have a distinct set of problems, they any ways share a common issue.

This problem is that both cellular and Wi-Fi primarily offers internet connectivity, and even when they encrypt the radio signal, the IP traffic that is on the internet portion remains unprotected.

This issue is taken care by the cellular network providers who offers a more secure option of back end connectivity to connect with the core network of the operator to the customer network, which includes dedicated frame relay circuits or IPsec-based, network to network VPN connections.

Ultimately, these arrangements made the operators to bear additional costs, both through initial networking setup charges and then through monthly charges.

AMAZING FACTS!!!

5GHz Wi-Fi actually starts at around 4.9GHz and goes all the way to 5.7Ghz-- this can vary widely between different regions due to what frequencies are allowed.

Platforms and connections multiplicity

There is a possibility that the implementation of specific security solutions for cellular data and Wi-Fi connections.

Maybe each of them would be unique and managing both is not practically possible. There is another concern which we should worry about like, the employees might be using variety of computing device which will also include portable computers, smartphones, home computers, PDA's, and public systems.

The department of IT will control over these issues but they can't monitor them all at once.

The unmanaged device which include public workstation and home system might leave the network at open risk. This is something the department of IT should be most concerned about.

CASE STUDY: INTERFERENCE IN FRENCH UNIVERSITIES COMPUTER SYSTEM

In 2010, Nice University decided to complaint for the hacking of its websites. Two years later the hacker was finally arrested. They had difficulty finding him because he used free hotspots and unsecured Wi-Fi to complete his felony. To find these unsecured wireless networks he drove around (wardriving).

He succeeded to crash some university servers and to accede to sensitive data. Some other French Universities had been compromised during this period. Even if he gathered a lot of information about people as name, address, he didn't use them. He declared that he did it as an intellectual challenge. He was sentenced to a three-year prison term.

CASE STUDY: A PUPIL HACKED HIS UNIVERSITY NETWORK

A student at Florida State University Panama City hacked the university wireless network and had redirected users to a porn site for about thirty minutes. He declared that he did it to expose the lack of security in its university wireless network.

As a result, Florida State University Panama City improved its wireless network security and now authentication is required to log into the network. The student has been suspended and is facing felony charges for "offenses against computer users".

REVIEW QUESTIONS

1. Discuss the security goals in wireless security networking.
2. Explain the following terms in brief:
   a. Wired equivalent privacy (WEP)
   b. Wireless Protected Access (WPA) and Wireless Protected Access 2 (WPA2)
   c. Virtual Private Network (VPN)
   d. Connection Multiplicity
3. What are the policies implemented in wireless security?

REFERENCES

1. Newsome, J., Shi, E., Song, D., & Perrig, A. (2017). The Sybil Attack in Sensor Networks: Analysis & Defenses. People.eecs.berkeley.edu. Retrieved 17 October 2017, from https://people.eecs.berkeley.edu/~dawnsong/papers/sybil.pdf
2. Agarwal, T. (2017). Different Types of Wireless Communication Technologies. Buy Electronics & Electrical Projects in the United States. Retrieved 17 October 2017, from http://www.efxkits.us/different-types-of-wireless-communication-technologies/
3. Sujihelen, L., Jayakumar, C., & Singh, C. (2017). Detecting Node Replication Attacks in Wireless Sensor Networks: Survey. Indjst.org. Retrieved 17 October 2017, from http://www.indjst.org/index.php/indjst/article/view/54150/58900
4. Introduction to Wireless Networking. (2013). Tutorial-reports.com. Retrieved 17 October 2017, fromhttp://www.tutorial-reports.com/wireless/introduction.php
5. Wireless network. (2017). En.wikipedia.org. Retrieved 17 October 2017, from https://en.wikipedia.org/wiki/Wireless_network
6. How do Wireless Networks Work? - Webopedia Reference. (2008). Webopedia.com. Retrieved 17 October 2017, from https://www.webopedia.com/DidYouKnow/Computer_Science/wireless_networks_explained.asp
7. INTRODUCTION TO WIRELESS NETWORKS. (2017). http://cdn.

ttgtmedia.com. Retrieved 17 October 2017, from http://cdn.ttgtmedia.com/searchNetworking/downloads/wireless_sample.pdf

8. Karim, A., & Tamimi, R. (2006). Security in Wireless Data Networks: A Survey Paper. Retrieved from http://www.cse.wustl.edu/~jain/cse574-06/ftp/wireless_security.pdf
9. Fitzpatrick, J. (2016). The Difference Between WEP, WPA, and WPA2 Wi-Fi Passwords. Howtogeek.com. Retrieved 17 October 2017, from https://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/
10. Types of Wireless Network Security keys; How to secure them. (2017). The Windows Club. Retrieved 17 October 2017, from http://www.thewindowsclub.com/type-wireless-network-security-keys-secure-windows-7
11. Ucisa.ac.uk. (n.d.). UCISA Case Studies on the Use of Wireless Networks. [online] Available at: https://www.ucisa.ac.uk/groups/ng/bestpractice/wirelessstudies.aspx [Accessed 23 Oct. 2017].

INDEX

A

Access point (AP) 36
Advanced Encryption Standard (AES) 85
Advanced Encryption Standards (AES) 194

C

carrier sense, multiple access with collision detect\ 176
Cellular networks 195
Central Regulatory Domain Agent (CRDA) 36
CIA (Common Air Interface 120
Computer Network Exploitation 162

D

Data transmissions 174
denial of service (DoS) 145
Denial of service (DoS) 143, 145
Digital communication 188
distributed denial-of-service (DDoS) 147
Distributed queue dual bus (DQDB) 177
domain name system (DNS) 147
Dynamic frequency selection (DFS) 178

E

Enhanced Data Rates for GSM Evolution (EDGE) 100
Extensible Authentication protocol (EAP) 191
Extensible Authentication Protocol (EAP) 105, 194

F

Federal Communications Commission (FCC) 40

G

global area network (GAN) 20
Global System for Mobile Communications (GSM) 18

H

Health Protection Agency (HPA) 39

I

IEEE (Institute of Electrical and Electronics Engineers) 54
Information Operations 163
InfraRed (IR) 57
International law 163
internet service provider (ISP) 146

L

Local area network (LAN) 11
local area networks (LANs) 98
Location-support system 174

M

media access control (MAC) 184, 185
Media Access Control (MAC) 178
megabits per second (Mbps) 47
mesh network or mobile ad hoc network (MANET) 15
Metropolitan area network (MAN) 11
mobile switching center (MSC) 24
multiple-input and multiple-output, or MIMO 44

O

Open version of Shortest Path First (OSPF) 127
Operationalizing 163
OSI (Open System Interconnection) 125

P

Personal area network (PAN) 11
personal computers (PCs) 54
personal digital assistants (PDAs) 54, 98
Physical node 171, 172, 173
Private authentication 174
public key cryptography (PKC) 185

Q

quality of service (QoS) 178

R

Radio communication design 33
radio frequency (RF) 39
Routing Information Protocol (RIP) 127

S

Single input multiple output(SIMO) 36
Single input single output (SISO) 36
Software Engineering Institute 160

T

TCP (Transmission Control Protocol) 128
Temporal Key Integrity Protocol (TKIP) 85
Transmit power control (TPC) 178
transport Layer Security (TLS) 191

U

United States Computer Emergency Readiness Team (US-CERT) 146
User Datagram Protocol (UDP) 128
User-in-the-loop (UIL) 36

V

Virtual LAN (VLAN) 192
virtual private network (VPN) 192

Virtual Private Network (VPN) 54

W

WEP (Wired Equivalent Privacy) 52
Wide area network (WAN) 11
Wi-Fi Protected Access (WPA) 84, 94, 101, 105, 184
Wi-Fi Protected Setup (WPS) 85, 88, 89
Wired Equivalency Protocol (WEP) 104, 194
wired equivalent privacy protocol (WEP) 189
Wired Equivalent Privacy (WEP) 25, 83, 101, 189, 190
Wireless communication 184, 185, 186, 189, 193
Wireless fidelity (Wi-Fi) 184, 189
wireless local area networks (WLANs) 5, 98, 99
wireless local area network (WLAN) 64
wireless personal area networks (WPANs) 12, 179
wireless sensor networks 169, 172, 179

Wireless Network Security

This book systematically focuses on the field of wireless security in network. All the important areas of wireless communication have been covered in this book. This topic is interdisciplinary in nature. Hence, the related topics covering wireless network and security have been discussed at various points in the book. The books also describe the key issues which are being faced in the wireless communication system as well as in the security system to protect it. The book starts with an introduction to the field of wireless network and security and explains the basic terms as well as the concepts related to it. Subsequently, the history of wireless network and how it has evolved over all the years has been discussed in this book. Various problems related to wireless network communication and security have been explained. Chapter two describes the real-time problems which are already being faced in the wireless network along with the types of wireless devices. How these devices can be used as a medium in the theft of data has also been explained.

Later the security measures in wireless network have been elaborated and challenges in the field of wireless security has been shown. In chapter six, the architecture of wireless network in the terms of OSI model have been elaborated. The next chapter focuses on the attacks to wireless network which are active attack and passive attack and the chapter next to it deals with the measures to prevent these attacks. With the rapid advancement in technology, security measures have also been arranged in the advanced way. In chapter nine, the securing of data through routing protocol has been discussed along with the IEEE standards. In last chapter of the book, the security goals along with the issues related to the wireless communication are discussed.



JOCELYN O. PADALLAN is currently pursuing her Master of Science in Information Technology from Laguna State Polytechnic University, Philippines and has Master of Arts in Educational Management from the same University. She has passion for teaching and has been an Instructor at Laguna State Polytechnic, Los Banos Campus, Philippines.

ISBN 978-1-77361-305-5

ARCLER PRESS