Wireless and Mobile Network

DECAP495

Edited by:
Dr. Pawan Kumar

LOVELY PROFESSIONAL UNIVERSITY

Wireless and Mobile Network

Edited By
Dr. Pawan Kumar

Title: WIRELESS AND MOBILE NETWORK

Author's Name: Gagandeep Singh

Published By : Lovely Professional University

Publisher Address: Lovely Professional University, Jalandhar Delhi GT road, Phagwara - 144411

Printer Detail: Lovely Professional University

Edition Detail: (I)

ISBN: 978-81-19929-08-5

Content

Gagandeep Singh, Lovely Professional University

Unit 01: Introduction to Wireless and Mobile Networks

CONTENTS

Objectives

- Understanding the fundamentals of the transmission in networks.
- Analyze the communication of the networks.
- Understanding Protocols and the TCP/IP suite.
- Analyzing the revolution of cellular networks.

Introduction

The most fascinating development in recent times has been in the area of wireless technology, which applies to both networking and telecommunications. The proliferation of wireless technologies, such as mobile phones, satellite services, and now wireless Internet and wireless local area networks, is causing significant shifts in the computer networking and telecommunications industries. Today's counterpart of the wireless telegraph is the cellular or mobile telephone, which enables communication in both directions between two parties at the same time. Technology known as analogue was employed in the initial generation of wireless telephones. Even though the devices were large and the connectivity was spotty, they were able to convincingly demonstrate the inherent ease of mobile communications. Digital technology is used in the construction of the most recent generation of wireless devices. Wireless communications have already made a significant influence and will continue to do so in the future. There have only been a handful of technological advancements that have proven effective in "shrinking" the planet in this fashion. In the next section, we will cover the principles of transmission mediums, as well as briefly discuss the growth of cellular networks and the protocols that are necessary for use in wireless settings.

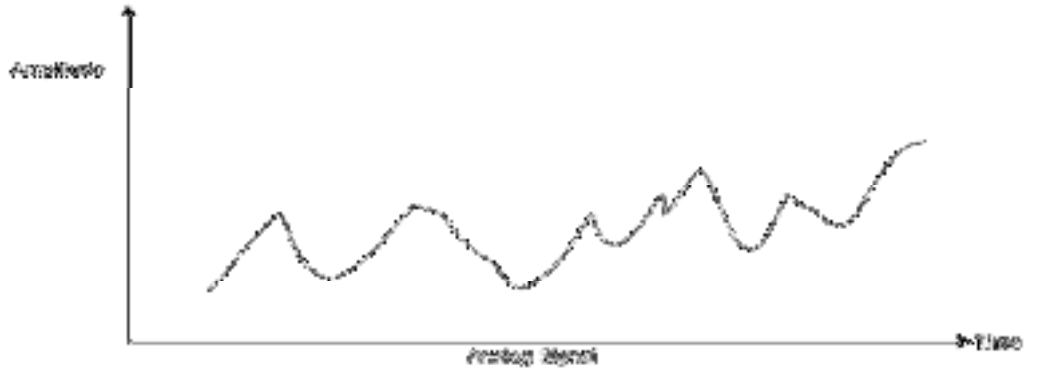
1.1 Transmission Fundamentals

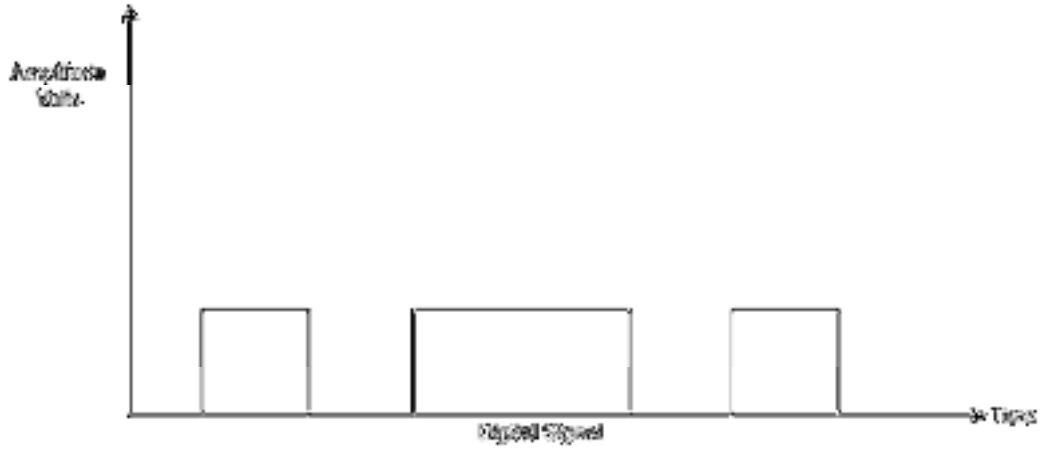
The utilization of electromagnetic signals as a means of transmitting data is the primary prerequisite for the process of data transmission. You may also describe a time-dependent electromagnetic signal as a frequency-dependent signal with discrete frequency components. This

is an alternate way to characterize the signal. It has been shown that a viewpoint on a signal's frequency domain is required for comprehending data transmission a great deal more than one that focuses on the signal's time domain.

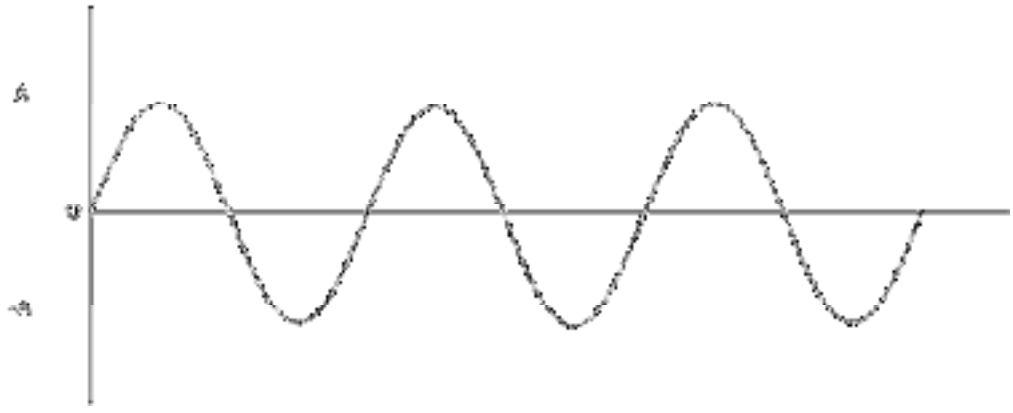
Time Domain Concepts

An electromagnetic signal can be analogue or digital depending on its type. This is a signal that changes over time. An analogue signal is one that has a gradual shift in signal strength over time. To put it another way, there are no gaps or interruptions in the transmission. A digital signal is one in which the signal intensity remains constant for a predefined amount of time before changing to a new predetermined level.





Sine Wave

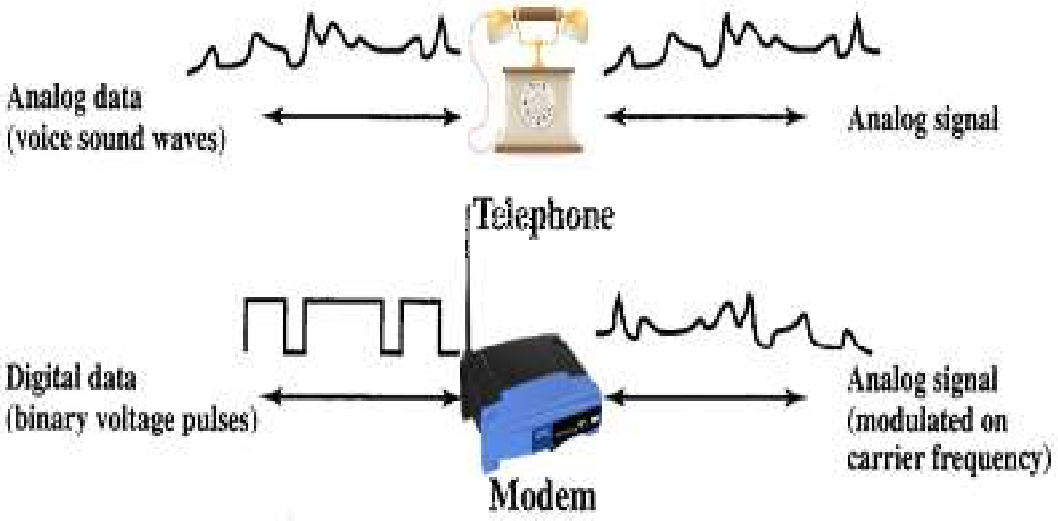


- The **frequency** is the rate in cycles per second, or Hertz (Hz)] at which the signal repeats.
- The **peak amplitude** is the maximum value or strength of the signal over time.
- The **wavelength** (A) of a signal is the distance occupied by a single cycle, or, put another way, the distance between two points of corresponding phase of two consecutive cycles.

Analog and Digital Signaling

Impulses of electromagnetic signals carry information from one location to another. Depending on the signal's frequency, several types of copper wire media, such as twisted pair and coaxial cable, may be utilized to transmit an analogue signal. This is because an analogue signal is an electromagnetic wave that is continually changing. Digital signaling's primary benefits are that, in comparison to analogue signaling, it often has lower costs and is less prone to being disrupted by noise interference. The most significant drawback is that digital transmissions are more susceptible to attenuation than analogue transmissions. This is the case because digital transmissions use more bits per signal. The image that follows is a diagram that illustrates a sequence of voltage pulses that were produced by a source that had two different voltage levels. It also displays the voltage that was received along a conducting medium. When the signal intensity at higher frequencies is attenuated, or lowered, the pulses become rounder and smaller. It should go without saying that the information included in the transmitted signal might potentially be lost due to the attenuation, but just in case:

With the help of a modem, digital data can also be shown in the form of analogue impulses (modulator-demodulator). By modulating a carrier frequency, the modem changes a series of binary (two-valued) voltage pulses into an analogue signal. The resulting signal will have a frequency spectrum that is mostly made up of the carrier, and it will be able to travel through any material that the carrier can travel through. Most modems encode digital data in the voice spectrum, so it can be sent over standard voice-grade phone lines. Because of this, modems are very flexible. At the other end of the link, a modem takes the signal and turns it back into the original data.



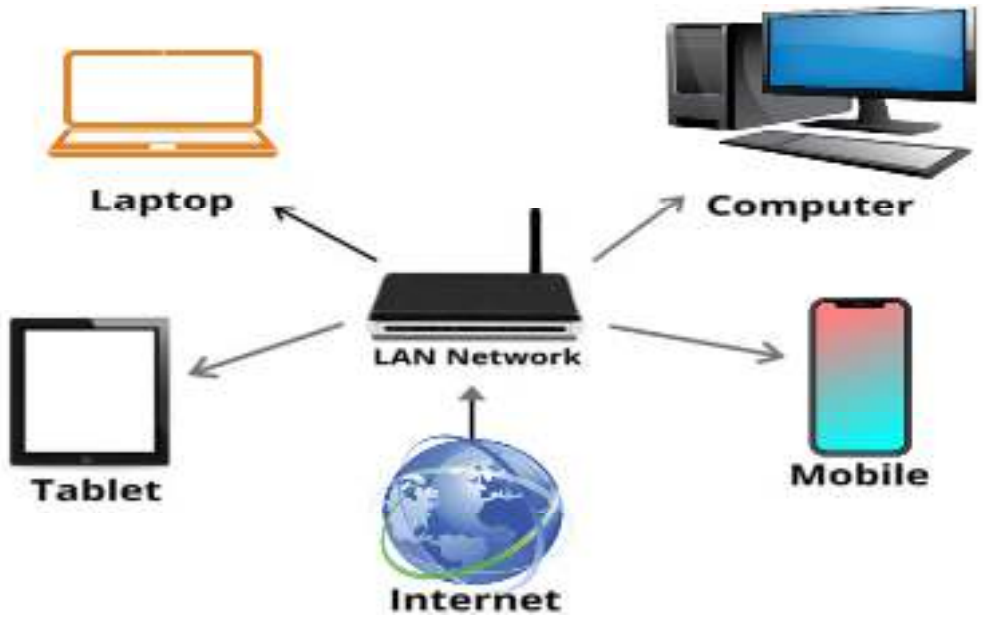
1.2 Communication Networks

The communication networks are basically divided in the three broad categories all of the categories will be discussed in this unit.

- Local area networks (LANs),
- Metropolitan area networks (MANs),
- Wide area networks (WANs)

Local Area Networks

A local area network, or LAN, is a way for devices to talk to each other and share data. In the past, data speeds on local area networks (LANs) have usually been between 1 and 20 Mbps. Even though these data rates are high, they are not enough because there are more and more devices, more and more multimedia applications, and more and more client-server architectures. Because of this, most of the work on LAN development has been on high-speed networks with data rates between 100 Mbps and 10 Gbps.



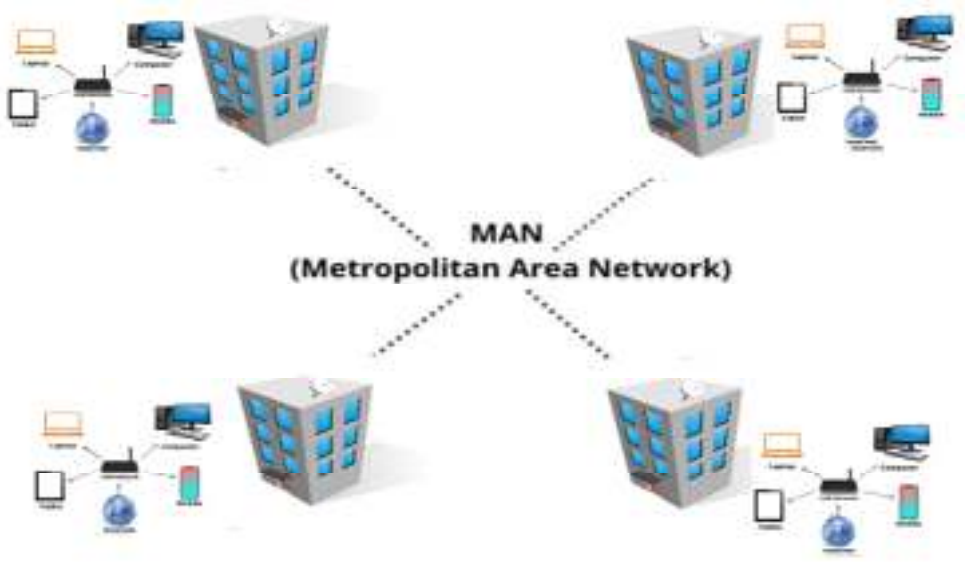
1. The LAN is limited to a small area, like a single building or a group of buildings. Because these two areas are in different places, they have different technical needs.

2. Most of the time, the same company owns both the LAN and the devices that are connected to it.

3. The data rates inside LANs are usually a lot higher than those inside WANs.

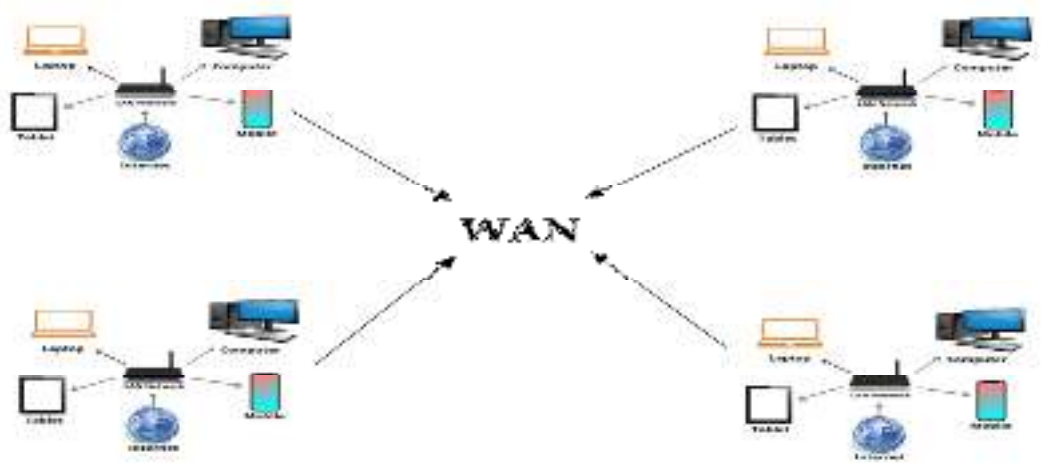
1.3 Metropolitan Area Network

As the name implies, MANs are in the center of LANs and WANs. People are interested in MANs because it has become evident that standard point-to-point and switched network approaches employed in WANs may not be sufficient to fulfill the demands of growing businesses. ATM offers to address a wide range of high-speed demands, but private and public networks that can cover a big area with high capacity at low cost are currently required. On a metropolitan scale, the LAN standards' high-speed shared-medium strategy provides a number of advantages. Even though both LANs and MANs cover some areas, MANs send and receive data quicker and over larger distances. The typical MAN client is someone who lives in a city and requires a large amount of capacity. A MAN is designed to satisfy capacity requirements at a lesser cost and with greater efficiency than using the local phone provider.



1.4 Wide Area Networks

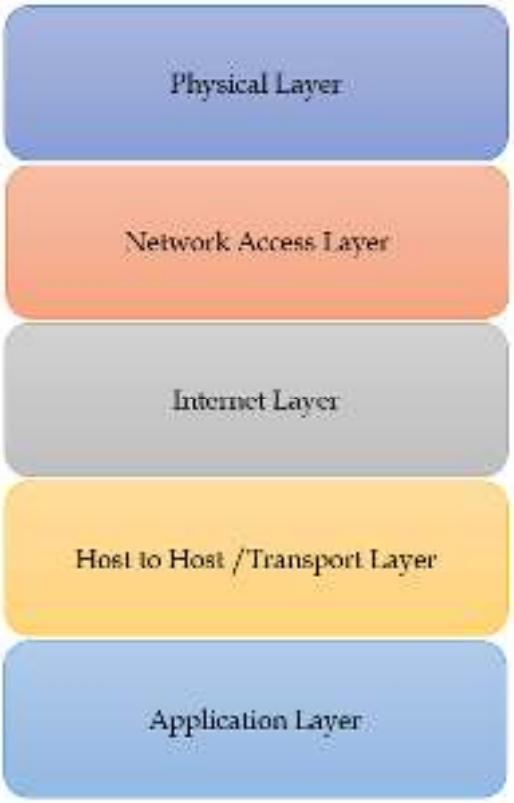
WANs span a broad geographic region, and in some locations they may have to go through public rights-of-way or make use of common carrier circuits. A wide area network (WAN) typically consists of many switching nodes that are connected to one another. Transmissions can originate from any device and be routed through these internal nodes before reaching the device that has been designated as the target. In the past, subscribers were only given a certain amount of bandwidth over their WAN. Data rates of 64,000 bps or lower have traditionally been considered to be the standard when connecting to a data network or a phone network using a modem. Users in the commercial sector have had access to higher rates, and one of the most common services is TL, which operates at 1.544 Mbps. WANs today have far higher data rates than they did in the past as a direct result of the ongoing development of infrastructure comprised of optical fiber, and these services are becoming more generally available. Users are able to connect at rates ranging from 10 to 100 Mbps thanks to a kind of transmission called asynchronous transfer mode, which is utilized by these high-speed WANs (ATM).



1.5 TCP/IP Protocol Architecture

Protocol research and development on the experimental packet-switched network known as ARPANET, which was funded by the Defense Advanced Research Projects Agency, led to the creation of the TCP/IP protocol architecture, which is also commonly referred to as the TCP/IP protocol suite (DARPA). This particular protocol suite is comprised of the many different protocols that the Internet Architecture Board has approved for use as official standards for the Internet. Applications, computers, and networks are the three entities that are responsible for the creation of

communications in general. Layers of TCP/IP The sending of electronic mail and the transfer of files are two instances of usage. The applications that we are discussing are known as distributed applications, and they need the exchange of data between two different computer systems. These applications, along with a wide variety of others, are designed to work on personal computers, which often have the capacity to execute many software packages concurrently. The data that has to be exchanged is sent from one computer to the next through the network, which is made possible since computers are connected to networks. As a consequence of this, moving data from one application to another requires first bringing the data to the computer on which the target application is installed, and then bringing the data within the computer to the application that is intended to receive it. Keeping these considerations in mind, it appears reasonable to segment the effort put into communication into five levels that are relatively independent of one another:

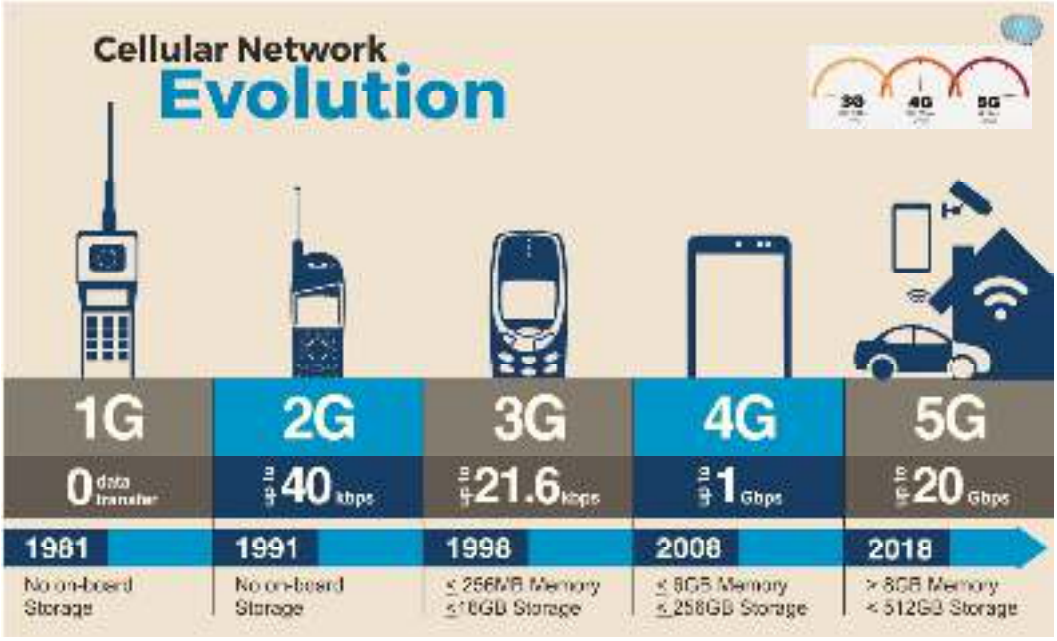


The physical layer is in charge of the actual connection between a device that sends data, like a computer or workstation, and a network or transmission medium. This layer is responsible for defining the qualities of the transmission medium, the types of signals, the data rates, and other important parts of the system. The network access layer is in charge of moving data between an end system (a server, a workstation, etc.) and the network to which it is connected. So that the data gets to the right place, the computer that sends the data needs to tell the network the address of the computer that will receive the data. There's a good chance that the computer sending the data will want to use some of the network's services, like priority. The software used at this layer depends on the type of network being used. There are many standards for circuit switching, packet switching (like ATM), local area networks (like Ethernet), and other types of networks. Because of this, it makes perfect sense to put network access functions on their own layer. So, the parts of the communications software that come after the network access layer don't have to worry about the details of the network that will be used. No matter what kind of network the computer is connected to, the same higher-layer software should work well. The network access layer is in charge of giving two end systems that are connected to the same network access to a network and routing data across that network. When two devices are connected to more than one network, data needs to be able to move between the networks. This is done through procedures. This is what the internet layer does in the system. At this level, traffic is routed across many networks by the Internet Protocol (IP), which is used at this level. The implementation of this protocol is built into both the routers and the end systems. A router is a computer that connects two networks and whose main job is to send data from one network to the other as it moves from the source to the end system. A router connects the system at the source to the system at the destination. Data needs to be sent and received in a secure way most of the time, and this need stays the same no matter what kind of

applications are involved. To put it another way, we would want to know that all of the data will be sent to the application for which it was meant, and that it will be sent in the same order as it was sent. The ways to make sure dependability are almost independent of the types of applications that are used. So, it makes perfect sense to put all of these strategies into a single layer that all programs share. This shared layer, which is also called the transport layer, is called the host-to-host layer. Most of the time, this capacity is provided by a protocol called TCP, which stands for Transmission Control Protocol. Last but not least, the application layer has all of the logic needed to support the different user applications. Each of the many different kinds of apps needs a separate module that is made for that kind of app, like a file-transfer module.

1.6 The Cellular Revolution

This is demonstrated even more clearly by the growth of the mobile phone market. In the year 1990, around 11 million people were making use of it. The current value is in the billions of dollars range. Since 2002, there have been an increasing number of mobile phones in comparison to fixed-line phones all over the world, as stated by the International Telecommunications Union (ITU). This momentum is being driven by newer devices that have built-in digital cameras and the capability to connect to the internet. Cell phones are gaining popularity for a number of different reasons, and this trend is expected to continue. Users are able to carry their mobile phones with them wherever they go, which is one of the primary benefits of using mobile phones. Due to the manner in which they came into being, they are also aware of their physical surroundings. Mobile phones are able to communicate with regional base stations that are always situated in the same physical area. The proliferation of the usage of mobile phones may be attributed to the development of several technologies. The size and weight of the phones have both decreased, and at the same time, the phones now have longer battery lives. The advent of digital technology has not only enhanced reception but also made it possible to make more effective use of a limited spectrum. The cost of mobile phones, along with that of a great many other kinds of digital technology, has recently been on a downward trend. Since 1996, there has been a significant decrease in pricing across the country in areas where there is a high level of competition. In many parts of the world, mobile phones are the only method that may deliver phone service at a price that is affordable. When opposed to digging holes in the ground to lay copper in challenging terrain, setting up base stations is a far quicker and less expensive process. The mobile phone industry is just one facet of the wider cellular revolution. Continuous innovation is being poured into the creation of new wireless device categories. These cutting-edge devices are capable of establishing an Internet connection. They feature personal organizers and telephones, but they also contain access to the internet, instant messaging, e-mail, and other Internet services. Users that operate wireless devices in autos are always able to acquire up-to-date maps and driving directions. In the near future, the devices could be able to call for help in the event of an accident or point the user in the direction of the gas station in the area with the lowest prices. Additionally, there will be a few additional amenities for your convenience. For instance, refrigerators may one day be able to place internet orders for food in order to restock items that have been depleted. Because of voice, many people rushed to connect to wi-fi for the first time. The attention is now being paid to the data. This sector comprises a significant component of the Internet that may function independently of the need of physical cables. The Internet is put to use by people in a wide range of different ways. Wireless technologies, such as smart phones and tablets, do not offer as many ways to display and enter information as stationary devices, such as a personal computer. People will mostly do business with one another and converse with one another, rather than spending extended periods of time surfing. It is possible to customize information to the location of the user of a wireless device since these gadgets can track their position. Users won't have to waste time looking for the information they need because it will be brought to them automatically instead.



1.7 The Global Cellular Networks

There is not a single mobile phone network available at the present. In most cases, a device will only function with one or two technologies out of a large variety, and it will only be able to connect to the network of a single operator. In order to progress beyond this method, further effort in the creation and use of standards is required. The IEEE is currently working on a set of wireless standards that will be applicable to devices that will be manufactured in the future. To accommodate a greater number of users, the new standards will make use of higher frequencies. Because so many first- and second-generation networks have been constructed and put into operation over the course of the previous decade, the implementation of the new standards will also assist in resolving issues that have surfaced as a result of this proliferation of networks. The Advanced Mobile Phone System was the first generation's digital wireless network that proved to be the most successful and widely used in North America (AMPS). The Cellular Digital Packet Data (CDPD) overlay network is responsible for the 19.2-kbps data rate that is provided by this network's data service. Whenever there is a break in the usage of the voice channels, the CPDP takes over and provides the data service. The Global System for Mobile Communications (GSM), the Personal Communications Service (PCS) IS-136, and the PCS IS-95 are the three wireless systems that are considered to be the most significant of the second generation. IS-95 is an example of a standard for code division multiple access (CDMA), whereas IS-136 is an example of a standard for time division multiple access (TDMA) (CDMA). The data service on the GSM and PCS IS-136 is sent across distinct channels at a rate of 9.6 kbps. Plans for International Mobile Telecommunications-2000 are currently being developed by the ITU (IMT2000). With the help of these guidelines, we should be able to create a single network that serves the whole planet. The two-gigahertz frequency band is where the standards are being developed. It will be able to achieve data transfer rates of up to 2 Mbps by utilizing the new standards and frequency spectrum. The process by which mobile devices will connect to the internet must be described in standards, in addition to the frequency utilization, encoding techniques, and transmission protocols that will be specified. Several organizations that are responsible for setting standards as well as industry groupings are collaborating on this endeavor. The Wireless Application Protocol (WAP) Forum is currently working on developing a standard protocol that would enable devices with restricted screen and keyboard capabilities to connect to the internet. The Internet Engineering Task Force (IETF) is currently working on a mobile IP standard, which will modify the widely implemented IP protocol to make it suitable for usage in a mobile environment.

Summary

- In this Unit we have covered the basics of the transmission Fundamentals.
- Time domain concepts were discussed.

- The difference between analogue and digital signals was discussed briefly.
- Discussion on LAN ,MAN and WAN was done with the required details.
- The architecture of TCP/IP protocol was discussed in details.
- How the cellular network has got into the main stream was discussed.

Keywords

MODEM – Modulation and demodulation device

LAN – Local Area Network

MAN – Metropolitan Area Network

WAN - Wide Area Network

ATM – Asynchronous Transfer Mode

ARPANET – Advanced Research Projects Agency Network

TCP/IP – Transmission Control Protocol/Internet Protocol

DARPA – Defense Advanced Research Projects Agency

ITU - International Telecommunications Union

IEEE - Institute of Electrical and Electronics Engineers

GSM - Global System for Mobile Communications

TDMA - Time division Multiple Access

CDMA - Code Division Multiple Access

FDMA - Frequency Division Multiple Access

PCS - Personal Communications Service

AMPS - The Advanced Mobile Phone System

WAP - Wireless Application Protocol

Self Assessment

1. The signal which changes over time is a called

A. Digital Signal
B. Analog Signal
C. Attenuated Signal
D. Clear Signal

2. A type of a signal in which the intensity of the signal is constant for predetermined time is called.

A. Digital Signal
B. Analog Signal
C. Attenuated Signal
D. Clear Signal

3. The rate in cycles per second at which the signal repeats itself is known as

A. Wavelength
B. Frequency
C. Period

D. Cycle

4. The distance occupied by the single cycle of the wave is known to be
A. Period
B. Frequency
C. Wavelength
D. Cycle

5. The biggest drawback of the digital transmissions is that it has more susceptibility to
A. Wavelength
B. Frequency
C. Cycle
D. Attenuation

6. Most of the modems encode the digital data in the form of _____ spectrum.
A. Noise
B. Data
C. Voice
D. Signal

7. _____ network is usually limited to a single building.
A. Local Area Network
B. Metropolitan Area Network
C. Wide Area Network
D. Wireless Area Network

8. The typical MAN client is someone who lives in a city and requires a _____amount of capacity.
A. Small
B. Large
C. Medium
D. Varied

9. _____ is a type of network that is spreaded over a broad geographic region.
A. Local Area Network
B. Metropolitan Area Network
C. Wide Area Network
D. Wireless Area Network

10. The _____ layer is responsible for the actual connection between devices that sends data.
A. Transport
B. Data Link

C. Presentation
D. Physical

11. The network access layer is in charge of moving data between _____ and the network to which it is connected.
12. The _____ layer is also called the host-to-host layer.
13. The very first known network for packet switching was called_____.
14. The maximum strength of the signal over the time is called_____.
15. Usually LAN is owned by a single organization.

A. True
B. False

16. Digital signals have a high cost of transmission.

A. True
B. False

Answers for Self Assessment

1.	B	2.	A	3.	B	4.	C	5.	D
6.	C	7.	A	8.	B	9.	C	10.	D
11.	End System	12.	Transport Layer	13.	ARPANET	14.	Peak Amplitude	15.	A
16.	B								

Review Questions

1. Write and explain the difference between analogue and digital Signals.
2. Explain how the transmission of digital signal is different from the analogue signals.
3. Compare and contrast the LAN and WAN networks in detail.
4. Explain the TCP/IP protocol Suite in detail.
5. What is the main reason for the expansion of the cellular network?
6. Explain the evolution of the cellular networks in detail.

Further Readings

- Wireless communications & networks by William Stallings, Pearson
- Principles of wireless networks by Kaveh Pahlavan, Pearson
- Fundamentals of wireless networking by Ron price, Mcgraw hill education
- Wireless networks first-step by Jim Geier, cisco press

Web Links

- http://59.51.24.50:8000/wxwl/Wireless_Communications_&_Networking_Stallings_2nd.pdf

Unit 02: Wireless Cellular Networks

CONTENTS

Objectives

- Understanding the Principals of cellular networks.
- Analyze the first-generation analog signals.
- Understanding the difference among TDMA and CDMA schemes.
- Analyzing the revolution third generation systems.

Introduction

It's possible that the emergence of cellular networks was the single most important factor in the sea shift that has place in data communications and telecommunications. The technology behind cellular networks serves as the foundation for mobile wireless communication. People are able to connect even in locations where there aren't many wired networks available. Cellular technology is at the core of many different types of devices, including mobile phones, personal communication systems, wireless Internet, wireless web applications, and many more. The first part of this chapter provides an overview of the fundamental concepts upon which all cellular networks are founded. Following that, we will investigate certain cellular technologies and standards, which have been divided into three generations for the purpose of making them simpler to comprehend. The analog-based components of the first generation are being phased out in favor of digital components in the second generation. Digital systems of the second generation are currently the most widely used technological advancement. Finally, the third-generation of high-speed digital technology has started to become more widely available.

2.1 Principles of Cellular Networks

More individuals may use the accessible mobile radio phone service thanks to the development of cellular radio technology. To use a mobile radio phone before cellular radio, a high-power transmitter and receiver were required. At least 25 channels and a range of at least 80 kilometers are usual for a standard radio system. One way to increase the system's capacity is to use low-power devices with a limited range and a high number of transmitters and receivers. Before we get started, let's examine the cell phone network infrastructure. As a follow-up, we'll dive into the mechanics of how they work.

Cellular Networks organization

To build a cellular network, several low-power transmitters are used, each with a power output of little more than 100 watts. Since this specific sort of transmitter has a limited range, an area can be divided into cells, with each cell having its own antenna. There is a base station for each cell, which contains a transmitter, a receiver, and a control device. As a last note, each cell has an own frequency range. So that there is no crosstalk or interference between adjacent cells, each one is allocated a different frequency. On the other hand, two cells may share the same frequency band if they are physically separated by a large enough distance.

To begin with, you need to think about how the cells covering a region will seem to the eye. Square cells would be the simplest arrangement to explain. There are flaws with this geometry, though. In all, four of the eight neighbors of a d-width square cell are d away, four of the eight neighbors are V2d away, and four of the eight neighbors are V2d away. Ideally, all neighboring antennas should be at the same distance away from a mobile user as they move closer to the cell's boundary. So it's much easier to figure out whether or not a user should be moved to a nearby antenna and which antenna to utilize. A hexagonal layout allows for antennas to be placed at equal distances from each other. As with the hexagon's own radius, the circle's circumference is equal to its own. A hexagon's side length is therefore equal to its radius. Hexagons have six equal-sized corners. D = V3R; this is the formula for the distance, d, that must be traveled from one cell to the center of its surrounding cells. There is no such thing as a completely hexagonal layout in the real world. Signal propagation patterns, topographical contours, and antenna location all affect how close you can get to the optimum signal path.

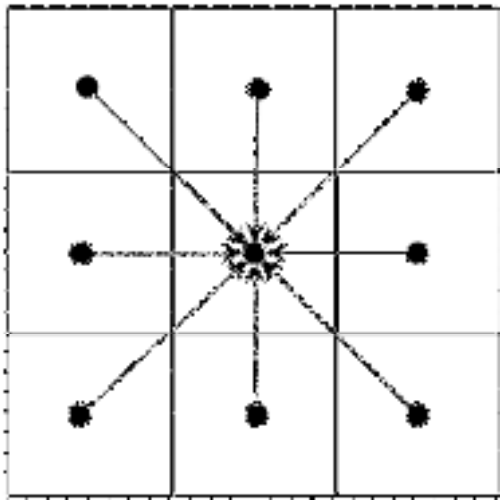


Figure 1 Square pattern

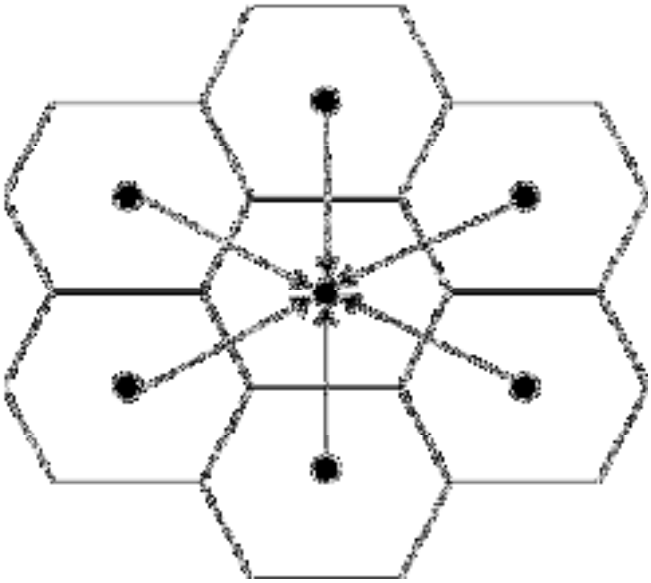


Figure 2 Hexagonal pattern

Reusing the same Frequency Several Times

Every cell in a cellular system comprises a base transceiver. It is carefully managed to allow communication within the cell using a certain frequency band while minimizing the power at that frequency leaving the cell and entering neighboring cells (to the extent that it is practical in the highly variable mobile communication environment). In spite of this, it is not only impracticable but also impossible to use the same frequency range in two adjacent cells. 1 A secondary purpose is to utilize the same frequency band in several geographically diverse cells. As a result, many mobile phones are able to interact concurrently within the same frequency spectrum. Any number of frequency bands may be given to a single cell, with the precise number determined by the expected volume of traffic.

Increasing Capabilities

After some period of time, as more users utilize the system, there may be a buildup of traffic to the point where there is not sufficient frequency bands allotted to a cell to handle its calls. The following are some of the methods that have been utilized in an effort to find a resolution to this predicament:

Adding new channels:

When a system is initially installed in an area, it is relatively uncommon for some of the channels to remain unused. As a result, development and expansion may be controlled and organized through the addition of additional channels.

Frequency borrowing:

In the simplest case, frequencies are taken from adjacent cells by congested cells. The frequencies can also be assigned to cells dynamically.

Cell splitting:

Because traffic and terrain are not always spread out in the same way, there are chances to increase capacity. Cells in areas with a lot of foot traffic can be split up into many smaller cells. In general, the original cells range in size from 6.5 to 13 kilometers. Smaller cells can be broken down further, but 1.5-kilometer cells are getting close to being the smallest size that is practically workable for a global solution (but see the subsequent discussion of microcells). In order to keep the signal in the cell even though the cell is getting smaller, the power level must be lowered. When mobile units move around the coverage area, they move from one cell to the next. This means that the call has to be sent from one base transceiver to the next. This part of the process is called a handoff. As the cells get smaller, these handoffs happen more frequently. The process of dividing cells into smaller parts to make them bigger overall. When the radius gets smaller by a factor of P, the coverage area gets smaller, and the number of base stations needed goes up by a factor of p2.

Cell sectoring

It is a technique that divides a cell into a number of wedge-shaped sectors, each of which has its own unique channel configuration. The vast majority of cells consist of between three and six sectors. Each sector receives a unique subset of the cell's channels, and the base station makes use of directional antennas in order to concentrate its attention on a certain sector.

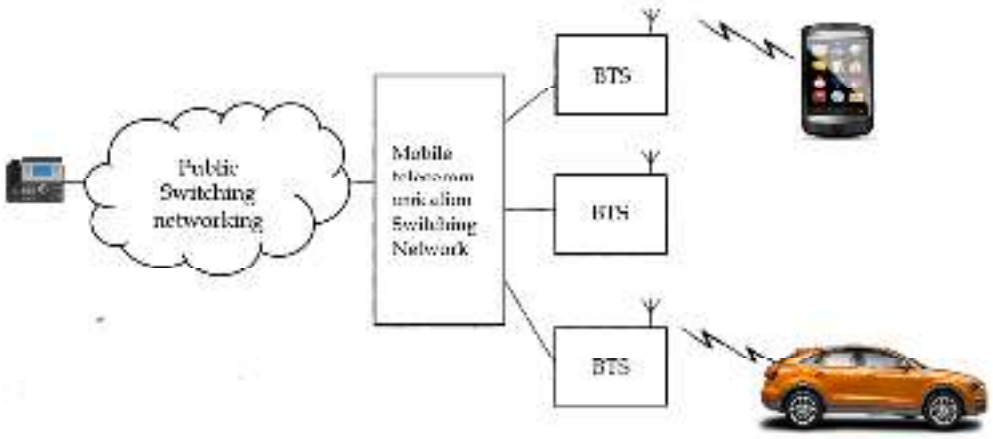
Microcells

These are formed when antennas travel from the highest points of large buildings or hills to the highest points of small structures or the sides of large buildings, and then finally to lamp posts, where they congregate to create microcells. There is a direct correlation between the size of a cell and the amount of power that can be sent between base stations and mobile devices. The smaller a cell is, the less power can be transmitted between them. Microcells can be beneficial in a variety of settings, including crowded city streets, highways, and large public buildings.

Working of cellular system

The base station can be found about in the centre of each individual cell (BS). People are able to communicate with one another on the channels that have been established for that cell thanks to the base station (BS), which is equipped with an antenna, a controller, and a number of transceivers. The controller is responsible for coordinating all calls that take place between the mobile unit and the rest of the network. When many mobile units are active and moving about in the same cell, they are able to communicate to the base station simultaneously if the cell is large enough. Every base

station is linked to a mobile telecommunications switching office (MTSO). Many BSs can be supported by a single MTSO. A wired connection is what is often used to link an MTSO and a BS, but a wireless connection is also a viable option. The Mobile Telephone Switching Office (MTSO) is in charge of connecting calls that are made from one mobile unit to another. Additionally, the MTSO is linked to the public telephone network or the telecommunications infrastructure. Because of this, it is able to connect a mobile subscriber to the cellular network as well as a fixed subscriber to the public network. The MTSO assigns a voice channel to each call, manages handoffs (which will be discussed in further detail later on), and maintains information on payments. Because everything else in a mobile phone network is computerized and programmed, the user's sole responsibility is to initiate or receive calls. Control channels and traffic channels are the two varieties of channels that are available for usage in communications between the mobile unit and the base station (BS). Control channels are used to communicate information about how to connect a mobile unit to the nearest base station (BS), as well as how to establish a call and ensure that it remains active. Users are able to communicate with one another and share data through the usage of traffic channels. The following events typically take place during a call made between two mobile users located inside the control area of a single MTSO.



Initialization of mobile device

When the mobile unit is powered on, it scans the entirety of the system to locate the setup control channel that has the highest strength and then selects that particular one. Cells that operate on a variety of frequency bands constantly transmit signals over a variety of setup channels. The receiver selects the setup channel that has the strongest signal strength and continues to monitor it once it has been selected. Because of this manner, the mobile unit has located the BS antenna of the cell in which it will automatically function, and it is now ready to begin operation. After then, a handshake is performed using the BS in this cell, which involves the mobile unit and the MTSO that is in control of this cell. Discovering who the user is and where they are may be accomplished through the handshake. This scanning method is utilized often as long as the mobile unit is turned on since it may be used regardless of where the mobile unit is located. A new BS is selected each time the unit relocates to a different cell. In addition, the mobile unit is searching for pages, which is something that will be detailed in greater detail later.

Mobile originated call

A mobile unit was the one that initiated the call: A mobile unit initiates a call by transmitting the telephone number of the called unit over a setup channel that has previously been selected. This begins the call. First, the receiver on the mobile unit verifies the information in the forward channel to ensure that the setup channel is not currently active. This information comes from the base station. When the mobile unit detects an idle, it will be able to transmit a message on the appropriate reverse channel (to the BS). The request is then sent to the MTSO via the BS.

Paging

After then, the MTSO will make an effort to establish a connection with the caller unit in order to complete the call. The Mobile Telephone Switching Office (MTSO) will send a "paging" message to one of the base stations in accordance with the number of the mobile unit that has been called (BS). Every base station has its own unique setup channel that it uses to transmit the paging signal.

Call acceptance

The called mobile unit searches for its number on the setup channel that is being observed, and once it locates it, it responds to the BS with its number. After that, the BS will forward the response to the MTSO. The MTSO creates a connection between the base station (BS) that is making the call and the base station (BS) that is receiving the call. At the same time, the Mobile Switching Office (MTSO) selects an available traffic channel inside the cell of each BS and communicates this information to the BS. The BS subsequently communicates this information to the mobile unit. Both of the mobile devices begin receiving transmissions from the channels that have been assigned to them.

Ongoing calls

While the connection between the two mobile devices is being maintained, voice or data signals may be transferred back and forth between the two devices. These signals are transmitted via the base station of each individual device and the MTSO.

Handoff

During a connection, if a mobile unit moves from the range of one cell to the range of another cell, the traffic channel needs to be changed to one that is assigned to the BS of the new cell. This happens when the mobile unit moves out of the range of the first cell and into the range of the second cell. This modification is carried out by the technology behind it without the call being terminated or the user being informed.

The following is a list of some of the additional tasks that the system is capable of doing, although they are not displayed:

Call Blocking

During the stage of the call where the mobile unit initiates it, if all of the traffic channels that are assigned to the nearest BS are in use, the mobile unit will attempt the call a predetermined number of times. A busy tone is played again to the user after a certain number of unsuccessful efforts on their part.

Call termination

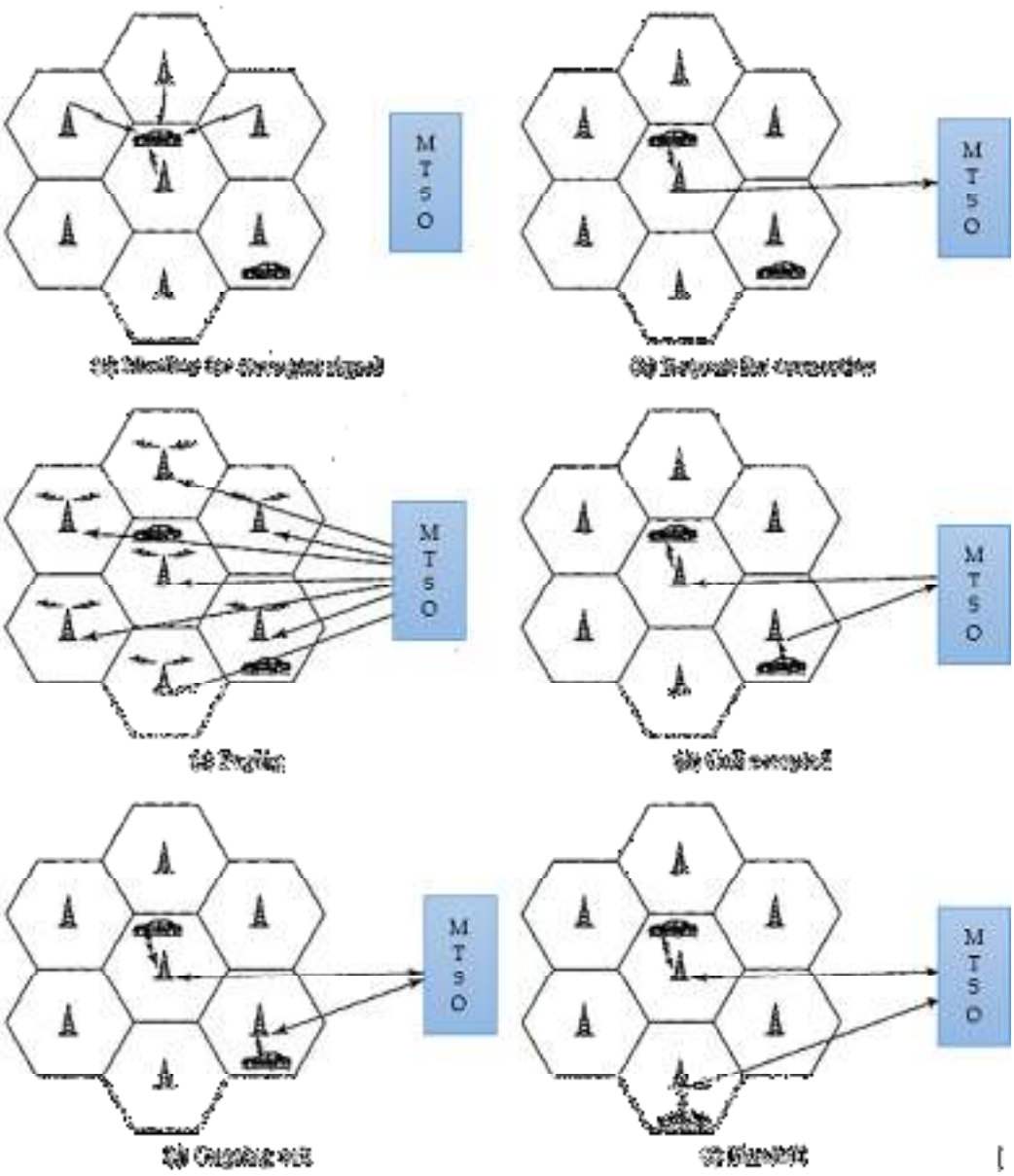
The MTSO is informed as soon as one of the two users hangs up, and at that point, the traffic channels at the two BSs become accessible to be used.

Call Drop

The traffic channel to the user is severed and the MTSO is informed if the base station (BS) is unable to maintain the minimum required signal strength for a certain length of time during a connection owing to interference or weak signal areas in specified locations.

Calls from fixed and remote subscriber

A telephone exchange that is connected to the public switched telephone network is referred to as the MTSO. As a result, the MTSO is able to link a mobile user located within its service area to a fixed subscriber by means of the phone network. Additionally, the MTSO has the ability to link a mobile user located within its service area to a mobile user located outside of its service region by utilizing the phone network or dedicated lines to a distant MTSO.



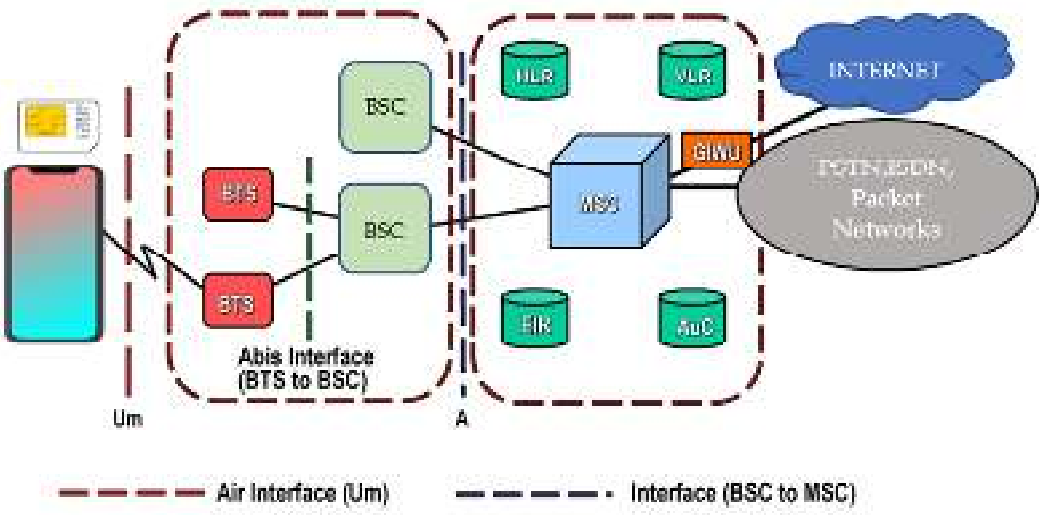
GSM architecture

The fundamental components of the GSM system that is responsible for its functionality. The GSM requirements dictate how the various functional pieces must be connected to one another, and they are the parameters that determine the restrictions at Urn, Abis, and A. Therefore, it is feasible to purchase equipment from a variety of different companies in the expectation that it would be compatible with one another. Other interfaces are also described in the GSM standards; however, we do not need to be concerned with those interfaces at this time. Transfer to another location Through the Urn interface, which is sometimes referred to as the air interface, a mobile station is able to communicate with a base station transceiver that is located in the same cell as the mobile unit. The physical terminal, also known as mobile equipment (ME), can be anything from a phone to a PCS (personal communications service) device. Radio transceivers, digital signal processors, and subscriber identity modules are all components of this device (SIM). A subscriber's identification number, the networks they are permitted to access, encryption keys, and other subscriber-specific data are all saved on a portable device known as a SIM, which is also known as a smart card or plug-in module. Another name for a SIM is a plug-in module. All GSM subscriber units are identical until a SIM card is inserted into one of them. Therefore, a subscriber has only to bring their SIM card with them in order to utilize a broad variety of subscriber devices in numerous countries. Once the subscriber has their desired device, all they need to do is insert their SIM card into the device. In point of fact, the subscriber units will not function without a SIM card, with the

exception of the ability to make some emergency calls. Therefore, rather than the subscriber devices themselves, it is the SIM cards that move around.

The Base Stations each have their own unique subsystem. The components that make up a base station subsystem include a base station controller as well as one or more base transceiver stations (BSS). Radio antennas, radio transceivers, and links to base station controllers are all components of a single base transceiver station (BTS), which is the building block of a single cell. Depending on its location, the maximum distance that a GSM cell can transmit signals is ranging from 100 meters to 35 kilometers. A base station controller, also known as a BSC, has the ability to exert control over one or more base station terminals, or BTS, and, therefore, a large number of cells. Paging and relocating a mobile unit from one cell to another inside the BSS are both responsibilities that fall within the purview of the BSC.

- **Network Subsystem** The network subsystem acts as a connecting point between the public switched telecommunications networks and the cellular network (NS). The Network Switch (NS) manages handoffs between cells that are hosted on separate BSSs; it also verifies the identities of users and their accounts; and it has capabilities that enable mobile users to travel worldwide. The mobile switching center is the most essential component of the network switch. It is responsible for the following four databases, which together form its core:
- **Home Location Register (HLR)**: Both the permanent and temporary databases that make up the HLR are where information on each subscriber who "belongs" to it is stored.
- **Visitor Location Register (VLR):** The location of the subscriber is an important piece of information that can vary in a short amount of time. The VLR that the subscriber is placed in determines where they are placed geographically. A list of subscribers who are physically present in the switching center's service area is kept in the visitor location register. This list may be found in the register. It maintains a record of the subscriber's activity levels as well as other information about the subscription. The system will utilize a subscriber's phone number in order to determine the location of the subscriber's home switching center whenever the subscriber receives a call. The HLR for this switching center contains information on the subscriber's present physical location, which may be accessed at any time. The VLR is what is utilized to initiate a call coming from a subscriber. Even if the subscriber is located inside the coverage area of their home switching center, they will still be shown in the VLR of the switching center. This is done for consistency's sake.
- **Authentication Center (AuC)**: This database is what the system relies on to authenticate users. It maintains the authentication and encryption keys for all of the subscribers' home and guest location registrations, for instance. When a user joins a network, the center is utilized to do identity verification on the user as well as control over who may view the user's data. Because GSM calls are encrypted, their privacy cannot be compromised. The message that is sent from the subscriber to the base transceiver is encrypted using the stream cipher A5, which is employed. On the other hand, landline networks do not record the conversations that take place over them. A3 is a unique form of encryption that establishes your identity and is used to verify it.
- **Equipment Identity Register database (EIR):** The Equipment Identity Register database (EIR) is responsible for keeping track of all of the various pieces of equipment that are located at the mobile station. Additionally, it aids in preserving people's safety (e.g., blocking calls from stolen mobile stations and preventing use of the network by stations that have not been approved).



First Generation Analog

There was analog traffic channels present on the very earliest mobile phone networks, which are today referred to as "first-generation" systems. AT&T's Advanced Mobile Phone Service (AMPS) has been the most widely used first-generation system in North America ever since it was introduced in the early 1980s. South America, Australia, and China are the three countries that implement this approach. AMPS is still in use today despite the fact that it has been mostly superseded by systems of the second generation. In the following paragraphs, we will discuss what AMPS is and how it operates. Details on the range of frequencies The AMPS system is allocated two 25-MHz bands in North America.

Table 1 AMPS parameters

Base Station transmission Band	869 to 894 MHz
Mobile unit transmission band	824 to 849 MHz
Space between forward and reverse channel	45 MHz
Channel Bandwidth	30 kHz
No. of full duplex voice channels	790
No. of full duplex control channels	42
Cell size, radius	2 to 20 Km
Mobile unit max power	3 watts
Modulation, control channel	FSK,8-kHz peak deviation
Modulation, voice channel	FM,12-kHz peak deviation
Data transmission rate	10 kbps
Error control coding	BCH (48,36,5) and (40,28,5)

The first is for transmitting signals from the base station to the mobile unit at a frequency of 869-894 MHz, and the second is for transmitting signals from the mobile unit to the base station at the same frequency (824-849 MHz). Every one of these bands has been cut in half so that they may better compete with one another (i.e., so that in each market two operators can be accommodated). Only up to 12.5 MHz is capable of being sent and received by each operator's system. Each operator has a total of 416 channels available to them because the gap between channels is 30 kHz. Because only 21

of the channels are needed for control, the remaining 395 are available for use in transmitting calls. The bit rate for control channels is 10 kbps, while data channels use this rate. Frequency modulation is the method that is utilized so that analog talks may be sent across the conversation channels. Additionally, control data is transmitted in brief bursts all across the chat channels. This quantity of channels is insufficient for the majority of the world's major markets; hence, it is necessary to either reduce the amount of bandwidth allocated to each discussion or discover a method for making many simultaneous uses of the same frequency. Both of these approaches have been utilized in the past to accomplish a variety of mobile communications-related goals. Reusing frequencies is something that AMPS does.

Operation

A numeric assignment module (NAM) with read-only memory is included in every mobile phone that is capable of using AMPS. The NAM consists of the phone number, which is assigned by the service provider, as well as the serial number, which is assigned by the manufacturer. Both of these numbers are included in the phone. When the user activates their phone, the device communicates its phone number as well as its serial number to the MTSO. The MTSO maintains a registry of lost or stolen mobile devices and can disable those devices by using the serial number. The phone number is utilized by the MTSO for the purpose of billing. Even if the phone is used in a city that is quite a distance away, the user's local service provider will still be invoiced for the service.

The following events take place in the following order [CODC01] when a call is made:

1. To place a call, a subscriber first selects the appropriate option from the menu, dials the desired recipient's number, and then presses the transmit key.

2. The MTSO verifies both that the user is authorized to make the call and that the entered number is valid. Along with the number that was called, some service providers require the user to provide a personal identification number (often known as a PIN) in order to prevent fraudulent activity.

3. The MTSO will then send a message to the user's smart phone informing them of which traffic channels they should utilize in order to send and receive data.

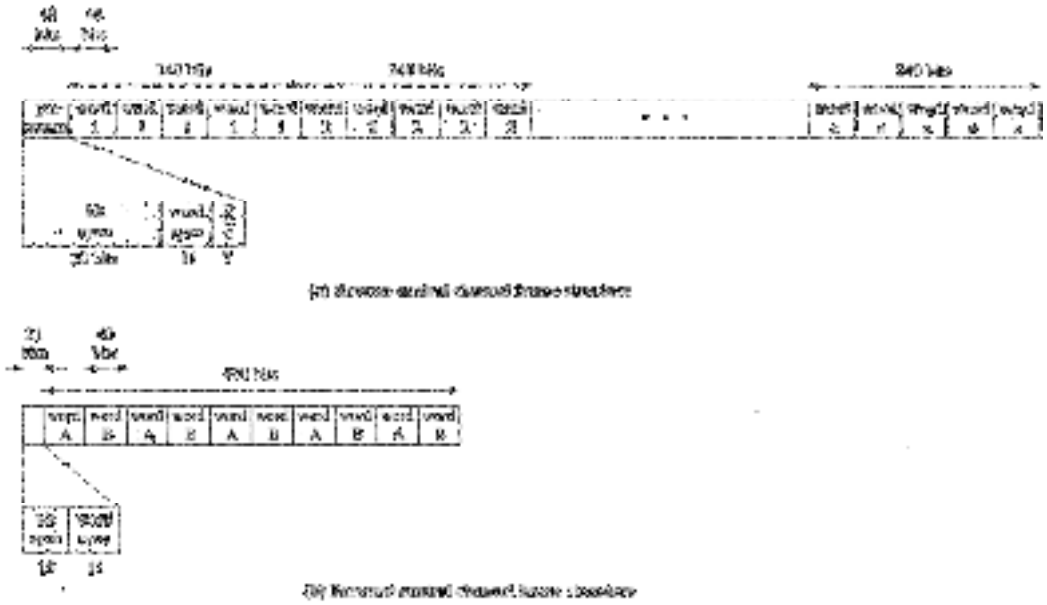
4. The MTSO will then transmit a signal to the individual who is being phoned indicating that their phone is ringing. In the initial ten seconds following the placement of the call, each of these things (steps 2–4) takes place.

5. The MTSO establishes a connection between the two parties and begins the collection of billing information as soon as the person who was phoned picks up the phone.

6. When one of the parties disconnects from the call, the MTSO closes the circuit, makes available any available radio channels, and completes the billing information.

AMPS control channels

Each AMPS service contains a total of 42 control channels, including 21 full-duplex 30-kHz control channels, 21 RCCs connecting the subscriber to the base station, and 21 forward channels connecting the base station to the subscriber. The transmission of digital data takes place across these channels using FSK. Data is transmitted over both channels in chunks that are referred to as "frames." The frame begins with a 48-bit precursor that contains a 30-bit bit sync field with alternating ones and zeros, an 11-bit word sync field (11100010010), and a 7-bit digital color code. In addition, the frame features a word sync field that contains alternating ones and zeros (DCC). In co channel cells, the DCC is utilized to differentiate between the several transmissions. It is the one and only identification for a base station, as well as the address of the destination for an RCC frame. Following the introduction, the body of the frame consists of one to six words of data. Each word is comprised of 36 data bits and is encoded using a condensed form of the BCH block code, which is represented as (n, k, t) =. (63,51,5). . In this abbreviated variant, the 48-bit word is created by adding 12 check bits to the 36 data bits that are already there. To ensure the accuracy of the information, each word is broadcast five times within the same time window. The term is discovered by employing the reasoning of the majority at the base station. When all of the additional labor is taken into account, the data rate is somewhere in the hundreds of bits per second range. Among the types of communications that fall under the RCC umbrella are "Origination," "Page Response," and "Order Confirmation." The FCC frame structure begins with a bit sync that is 10 bits long and a word sync that is 11 bits long. There are two words of data included inside each frame. Each word has its own unique code.



Using BCH and having a total of 28 data bits and 12 check bits. Again, each word is checked for correctness by being said five times. Also, the busy/idle bits that are added to every tenth bit in the frame of each FCC frame tell us about the state of the RCC frame that goes with it (idle or busy). Each FCC frame can be used to get this kind of information. Because of this, the size of the frame as a whole has grown to 463 bits. When the signaling rate is 10 kbps, the data rate is about 1.2 kbps (without taking into account the overhead). The FCC also sends out paging messages and signals for assigning frequencies.

Last but not least, control information can now be sent through a voice channel while a conversation is going on. Either the mobile unit or the base station can send a data burst by turning off the voice FM broadcast for about a hundred milliseconds and then replacing it with an FSK-coded message. These messages are meant to send information that needs to be sent quickly, like a change in power level or a handoff.

2.2 Second Generation TDMA and CDMA

The radio component of a mobile station may only broadcast and listen during the time frame allotted by TDMA. During the remaining time, the mobile station can undertake network measurements by detecting nearby transmitters that operate on a variety of frequencies. Unlike code division multiple access (CDMA), which makes frequency handover difficult, this characteristic allows for inter frequency handover. CDMA, on the other hand, enables handoffs, allowing mobile stations to connect to up to six base stations at the same time.The majority of 2G mobile networks use TDMA, whereas 3G systems use CDMA. TDMA is still used in current systems, despite this. Several users can share a single time slot using universal terrestrial radio access (UTRA) protocols including combined time division multiple access (TDMA), code division multiple access (CDMA), and time division duplex (TDD).

Each cell is assigned a certain number of channels, half of which are reverse and the other half of which are forward, similar to FDMA. To restate, a mobile unit is given capacity on reverse and forward channels that are matched such that full duplex communication can take place. Furthermore, every physical channel is furthermore logically divided into a multitude of communication paths The broadcast is done in a manner that consists of a recurrent series of frames, each divided into a number of time slots. Each for each slot position that occurs during the sequence of frames, a new logical channel is generated.

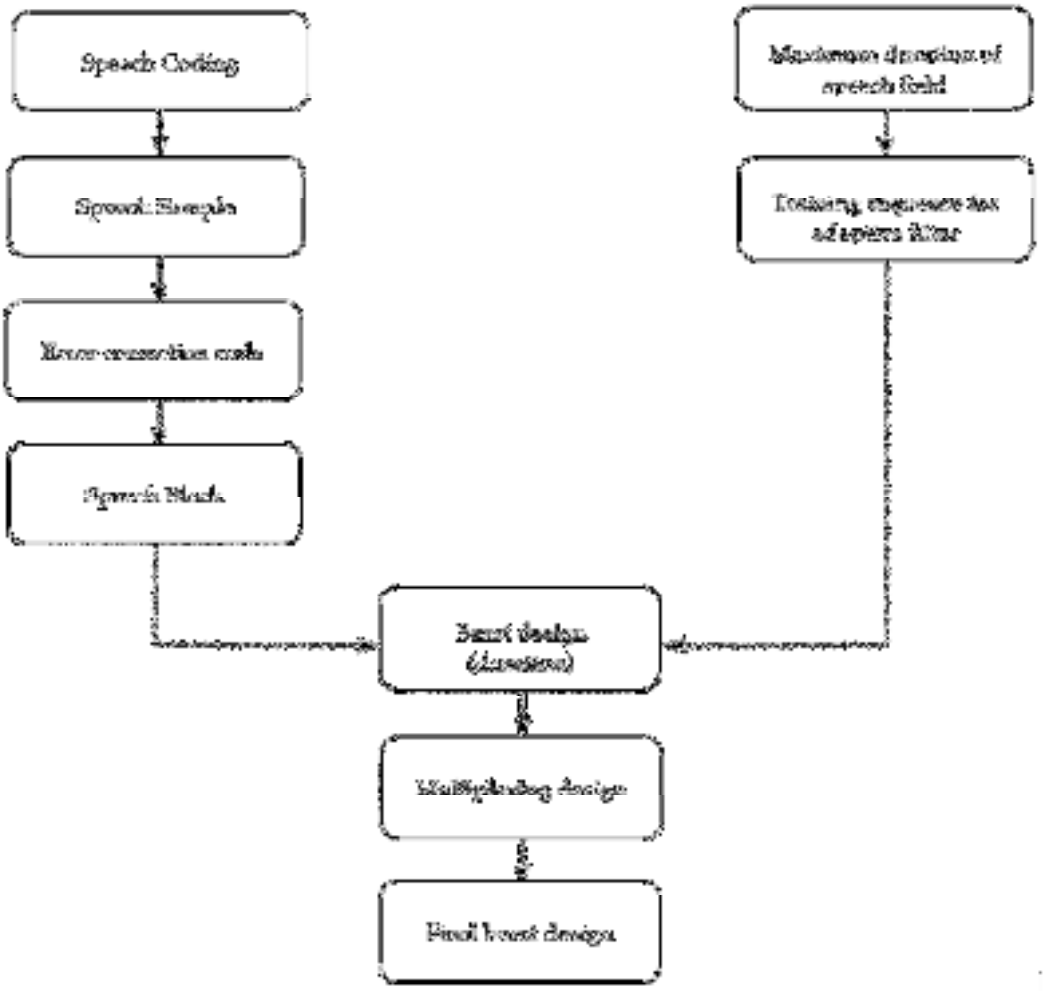
Mobile Wireless TDMA Networks: Design Considerations

Before delving into the specifics of GSM, it's a good idea to review a few key points. By looking at a simple analysis based on one offered in [JONE93], we may make recommendations for general design. Some of the design decisions made for GSM were based on the findings of this study. In broad terms, The purpose of this project will be to establish the duration and make-up of the traffic channel time slot. This will enable for successful voice and data transfer while making optimum use

of the available bandwidth. The radio frequency spectrum Take the following list of expectations into consideration:

- There are eight logical channels in a TDMA frame, which corresponds to the number of time slots. This appears to be the absolute minimum necessary to justify the additional costs associated with multiplexing.
- For there to be enough traffic in a cell, the maximum cell radius (R) must be at least 35 kilometers in rural areas.
- Frequency: Around 900 MHz; this is a popular frequency range for mobile devices applications for radio
- The maximum permissible speed for automobiles is 69.4 miles per hour to accommodate mobile devices (or 250 kilometers per hour) units on trains moving at a high rate
- To avoid an undue increase in latency, the maximum coding delay permitted is roughly 20 milliseconds.
- The fixed network, which may include satellite connection, causes delays. If the delay is more than 20 milliseconds, It becomes difficult to communicate verbally.
- Maximum delay spread (in hilly areas): 10 J.LS; this is the difference in propagation delay between several multipath signals arriving at the same antenna
- Bandwidth: Maximum of 200 kHz (equal to 25 kHz per channel) (the maximum frequency that may be used).

Design consideration for TDMA



Code Division Multiple Access

The following is an explanation of how CDMA works for cellular network systems. Each cell is given a frequency bandwidth that is split into two portions: one for reverse (mobile unit to base station) and one for forward (base station to mobile unit). This is similar to how FDMA works (base station to mobile unit). In order to achieve full duplex communication, a mobile unit will utilize both forward and backward channels. A transmission known as direct-sequence spread spectrum (DS-SS) is used. This type of transmission makes use of a chipping code to increase the data rate of the transmission, which in turn expands the signal bandwidth. Different users are given orthogonal chipping codes, which enables the receiver to recover the transmission of a single unit from many broadcasts and hence enables different access. These codes are distributed to various users.

CDMA is advantageous for cellular networks in a variety of ways, including the following:

- Variations in frequency Because the signal is spread across a broader bandwidth, frequency-dependent transmission faults like noise bursts and selective fading have less of an impact on the signal's quality.
- Resistance to Multipath: In addition to DS-ability SSs, which prevent multipath fading through frequency diversity, CDMA chipping codes exhibit low cross correlation and autocorrelation. This makes them resistant to multipath. Because of this, a signal version that is delayed by more than one chip interval will cause less interference with the dominant signal compared to interference caused by other multipath circumstances.
- Spread spectrum is able to fulfill its goals by utilizing noise-like signals, which means that the code for each user is distinct, so ensuring the user's privacy.
- Degradation of service in a graceful manner: When using FDMA or TDMA, only a certain number of users can access the system at the same time. However, with CDMA, the noise level and hence the error rate rise when more users contact the system at the same time. The system only progressively degrades to an unbearable error rate as more users contact it simultaneously.

It is important to highlight the following drawbacks associated with CDMA mobile phones:

- Self-jamming: Until all mobile users are correctly synchronized, incoming signals from multiple users will not be perfectly matched on chip boundaries. This will prevent any interference from occurring. As a direct consequence of this, the different users' spreading sequences are not orthogonal, and there is some degree of cross correlation between them. Both time division multiple access (TDMA) and frequency division multiple access (FDMA) require that the received signals be orthogonal or substantially orthogonal within the appropriate time or frequency guard bands.
- Near-far problem: The attenuation of signals is lower for those that are closer to the receiver than for those that are further away. It is possible that it will be more difficult to receive transmissions from mobile units that are located further away due to the absence of complete orthogonality. Consequently, power control measures are of the utmost significance in a CDMA system.
- Soft handoff: In order to provide a seamless transition from one cell to the next, the mobile unit must first acquire the new cell before relinquishing the old one, as will be discussed in more detail in the next paragraph. Because it is more difficult than the "hard handoff" utilized by FDMA and TDMA, this technique is referred to as a "soft handoff."

2.3 Third Generation Systems

The goal of the third generation (3G) of wireless communication is to provide fairly fast wireless communications that can support voice, data, video, and other types of media. Through its

International Mobile Telecommunications for the Year 2000 (IMT-2000) initiative, the lTD has defined third-generation capabilities as.

- Voice quality is about the same as that of the public switched telephone network.
- 144 kbps data rate for users in fast cars over large areas.
- 384 kbps data rate for pedestrians standing still or moving slowly over small areas.
- Support for 2.048 Mbps for office use (to be phased in over time).
- Data transmission rates that are both the same and different.
- Both packet switched and circuit switched data services are supported.
- An adaptable interface to the Internet that takes into account the difference between traffic coming in and traffic going out.
- Better use of the spectrum in general.
- Support for a lot of different mobile devices
- Ability to change so that new services and technologies can be added

The trend toward personal telecommunications for everyone and access to communications for everyone is one of the things that drives modem communication technology. The first idea is that a person can easily identify himself or herself and use any communication system in a whole country, across a continent, or even around the world with just one account. The second is the ability to connect to information services from a terminal in a wide range of settings. For example, a portable terminal that works just as well in the office, on the street, and on an airplane. An important part of this change in the way people use computers will be wireless communication. For instance, the GSM cell phone system with its subscriber identity module is a big step toward these goals.

Personal communications services (PCSs) and personal communication networks (PCNs) are names for these ideas of global wireless communications. They are also goals for third-generation wireless. In general, the planned technology is digital and uses time division multiple access or code division multiple access to make good use of the spectrum and have a lot of capacity.PCS handsets are made to be small, light, and use little power. International work is being done to let the same terminals be used everywhere.

Summary

- In this Unit we have covered the underlying principles of cellular networks.
- The concepts behind the first-generation cellular system architecture was discussed.
- The topics of discussion included the time division multiple access and the code division multiple access encodings.
- The services related to the third generation of the cellular network was discussed.
- How the cellular network has got into the main stream was discussed.

Keywords

BTS – Base transceiver system

MTSO - Mobile telecommunications switching office

BS – Base Station

SIM – Subscriber identification module

ME – Mobile Equipment

GSM - Global System for Mobile Communications

IEEE - Institute of Electrical and Electronics Engineers

GSM - Global System for Mobile Communications

TDMA - Time division Multiple Access

CDMA - Code Division Multiple Access

FDMA - Frequency Division Multiple Access

BSC – Base station controller

MSC - mobile switching center

HLR - Home location register

VLR - Visitor location register

AuC – Authentication center

EIR – Equipment identity register

FCC - Forward control frames

RCC - reverse control frames

Self Assessment

1. The communication services offered by first-generation cellular networks fall into one of the following categories:

A. Analog
B. Digital
C. Hybrid
D. All of the above

2. GPRS stands for

A. General packet radio service
B. Global positioning radio service
C. Geological Packet Radio Service
D. None of the above

3. The system which allows the complete bandwidth to each user is called

A. CSMA
B. GSM
C. CDMA
D. FDMA

4. Which mode of communication is called two-way communication

A. Simplex
B. Half Duplex
C. Full Duplex
D. None of the above

5. Out of the following which statement is NOT correct in term of TDMA

A. Discontinuous data transmission
B. Single carrier frequency for single user
C. No requirement of duplexers

D. High transmission rate

6. With the use of handoff technique, it is possible to
A. Minimize the impact of signal fading
B. Optimization of power
C. Maintain the link quality when the user travels from one cell to another
D. None of the above

7. What is the main purpose of creating a cell in the mobile systems
A. Handoff
B. Frequency reusability
C. Modulation
D. Large bandwidth

8. What is the main advantage of 2g cellular network
A. Calling can be done
B. Increased overhead
C. Higher bitrate
D. New services like SMS were included

9. How many channels does FDMA carries _____ phone circuit at a time.
A. Ten
B. Two
C. One
D. Several

10. The FDMA channel has a bandwidth which is _____ compared to other
A. Wide
B. Narrow
C. Large
D. Zero

11. _____ is based on FDMA/FDD.
A. GSM
B. W-CDMA
C. Cordless telephone
D. AMPS

12. BTS stands for_____
A. Before the scenes
B. Basic transmission system
C. Base transceiver system

D. None of the above

13. MTSO stands for
A. Mobile telecommunication system office
B. Managed telecom system operation
C. Mobile transmission switching official
D. Mobile telecommunications switching office

14. It is NOT possible to block a call if we are using a GSM service
A. TRUE
B. FALSE

15. Which register stores the permanent and temporary information about the actual belonging of the subscriber
A. VLR
B. HLR
C. MSC
D. AuC

16. What is the correct AMPS space between the forward and reverse channel
A. 20 MHz
B. 30 MHz
C. 45 MHz
D. 55 MHz

Answers for Self Assessment

1.	A	2.	A	3.	C	4.	C	5.	B
6.	C	7.	B	8.	D	9.	C	10.	B
11.	D	12.	C	13.	D	14.	B	15.	B
16.	C								

Review Questions

1. Write and explain the difference between TDMA and CDMA.
2. Explain how the cellular network operate.
3. Compare and contrast the functionality of BSS and BTS detail.
4. Explain the functionality of GSM service in detail.
5. What is the main reason for using the third-generation cellular network?
6. Explain the evolution of the cellular networks in detail.

Further Readings

- Wireless communications & networks by William Stallings, Pearson
- Principles of wireless networks by Kaveh Pahlavan, Pearson
- Fundamentals of wireless networking by Ron price, Mcgraw hill education
- Wireless networks first-step by Jim Geier, cisco press

Web Links

- http://59.51.24.50:8000/wxwl/Wireless_Communications_&_Networking_Stallings_2nd.pdf

Unit 03: Modulation Techniques

CONTENTS

Objectives

- Understanding the signal encoding concepts.
- Analyzing the differences between the different types of signals.
- Understanding the Digital data analogue signals and Analog data digital signals.
- Analyzing the Analog data analog signals

Introduction

In this lesson, we will go over the fundamentals of analog signaling, which makes use of a carrier signal that is continuous and has a consistent frequency. The frequency of the carrier signal is determined so that it is compatible with the transmission medium that has been selected. Data can be sent by modifying the transmission of a carrier signal in some way. In contrast to digital signaling, which translates a digital or analog source of data into a digital signal. The actual format is chosen to make the most efficient use of the media being transmitted across, and this choice is determined by the encoding technique. The process of modulation refers to the process of encoding source data with frequency onto a carrier signal. Amplitude, frequency, and phase are the fundamental frequency domain parameters that are utilized in all different kinds of modulation systems.

3.1 Signal Encoding Criteria

Before we get started, there are several terms that need to be established. Keep in mind that a digital signal is a series of unique voltage pulses that are irregular in their pattern. Each pulse may be thought of as a separate component of a signal. Before being sent as binary data, each data bit is first transformed into an individual signal element. Bits and signal components are paired with one another in order to create the simplest possible scenario. A voltage level that is higher is used to represent the binary digit zero, while a voltage level that is lower is used to represent the binary digit one. It is also possible to encode digital bit streams using analog signals. A digital bit stream is made up of a series of pulses that have a consistent frequency, phase, and amplitude. It was possible for the data components (bits) and the analog signal elements to precisely match one another. As we shall see in the next section, there may be a correlation between data items and signal components that is either one-to-multiple or multiple-to-one. This is true for both analog and digital signals. The pace at which data are transmitted, measured in bits per second, is referred to as a signal's data signaling rate, or simply its data rate. A bit's duration, also known as its length, is the

amount of time that it takes the transmitter to emit the bit; for a data rate of R, this amount of time = 11R. In contrast, the term "modulation rate" refers to the rate at which the signal level is changed. This will be dependent on the type of encoding, which will be covered in further detail later. The rate of modulation is denoted by the baud unit, which refers to the number of signal components that occur per second.

Before anything else, the receiver has to be aware of the time associated with each bit. That is to say, the beginning and end of a bit must be discernible to the receiver in a reasonable manner. The second step is for the receiver to determine whether the signal level at each bit point is high (0) or low (1). (1). In the course of doing these activities, a sample is taken from each bit position in the middle of the interval. The value is then compared to a threshold. As was proven, noise and other constraints will both contribute to the occurrence of errors. Which aspects of the incoming signal have the most impact on whether or not the receiver successfully deciphers it?

The following three components are absolutely necessary:

- A measurement of the signal to noise ratio
- The rate of data transfer.
- The bandwidth

If we assume that every other variable will remain the same, then the following assertions are true:

- Bit error rate (BERV) grows as data rate rises.
- Bit error rate decreases when signal-to-noise ratio increases.
- An increase in bandwidth makes it possible to increase the data rate.

The manner of encoding is a distinct component that may be utilized to improve performance if desired. The only thing that the encoding system is truly responsible for doing is mapping data bits to signal components. There are many various approaches that may be used. Before getting into further depth about these ways, let's take a time to discuss and evaluate the following approaches to comparing and contrasting the various solutions.

Signal spectrum:

The signal spectrum is comprised of a number of fundamental elements. Because there are fewer components operating at high frequencies, the bandwidth requirements for the transmission are reduced. Additionally, it is highly recommended that there be no component of direct current (dc). When there is a dc component to the signal, there must be a direct physical attachment of the transmission components. This is required. By eliminating the need for a direct current (dc) component, an alternating current (ac) connection may be made using a transformer. This results in improved electrical isolation and less interference. In conclusion, the spectral properties of the signal that is being transmitted are what define the degree to which the transmission will be affected by signal distortion and interference. In point of fact, a deterioration of a channel's transfer function at the band edges is a phenomenon that takes place very regularly. When designing a signal that is appropriate for transmission, the power that is sent should therefore be concentrated in the middle of the transmission bandwidth. In a circumstance like this one, one would expect to see less distortion in the signal that was received. It is possible to generate codes with the purpose of changing the spectrum of the sent signal in order to accomplish this objective.

Clocking:

The receiver is required to be aware of both the beginning and finish of each bit position. This is not a straightforward endeavor. One way that may be used, albeit an expensive one, to synchronize the transmitter and the receiver is to generate a separate clock channel. The alternative would be to provide some kind of synchronization system that is dependent on transmission. Providing you use the appropriate encoding, this is doable.

Signal interference and noise immunity:

There are certain codes that operate better than others when they are exposed to noise. BERs are the standard method for expressing this concept.

Cost and complexity:

In spite of the fact that the price of digital logic is getting cheaper, this facet should not be ignored. In specifically, the cost rises with the signaling rate that must be achieved in order to achieve a specified data throughput. It is going to become clear that some codes genuinely call for a signaling rate that is higher than the data rate.

3.2 Digital Data Analog Signals

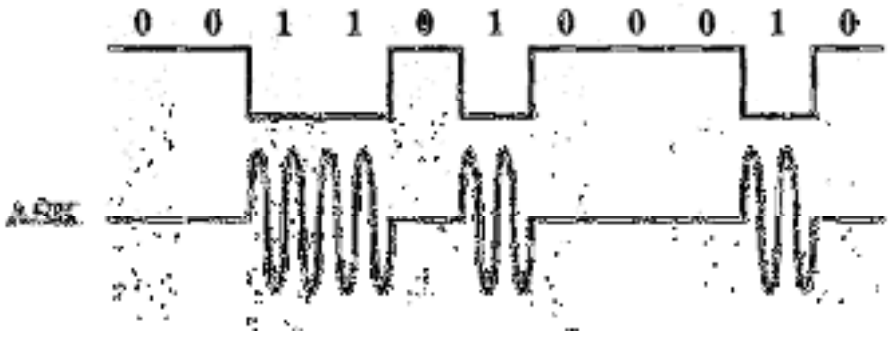
To start, let's take into consideration the possibility of analog signals being utilized in the transmission of digital data. The public telephone network is the location where this transformation is utilized to convey digital data more frequently than any other. The voice-frequency range of the telephone network, which is around 300 to 3400 Hz, was designed to receive, switch, and send analog signals. This was the original intent of the designers. In its current state, it is unable to process digital signals coming from subscriber locations; however, this situation is starting to improve (although this is beginning to change). Connecting digital devices to a network requires the use of a modem, also known as a modulator-demodulator, which is a device that can convert digital data into analog signals and vice versa. For the purpose of the telephone network, modems that produce signals at voice frequencies are deployed. The same core technologies, such as microwave, are utilized for modems that create signals at higher frequencies (e.g., microwave). This section presents a concise summary of different approaches, in addition to a discussion of the various options' varying levels of performance characteristics. We stated that in order to modulate a signal, one or more of the parameters of the carrier signal, specifically its amplitude, frequency, or phase, must be altered. As a consequence of this, amplitude-shift keying (ASK) serves as an example of three main encoding or modulation schemes for the process of transforming digital data into analog signals (ASK),

Amplitude -Shift Keying

The two possible binary values in ASK are each represented by a distinct amplitude associated with one of the carrier frequencies. In most cases, one of the amplitudes is equal to zero, which indicates that one binary digit is represented by the continuous presence of the carrier, while the other is represented by the absence of the carrier. When one bit is transmitted, the signal that is produced looks like this:

$$\text{ASK} \qquad s(t) = \begin{cases} A\cos(2\pi f_c t) & \text{binary 1} \\ 0 & \text{binary 0} \end{cases}$$

Where A is the carrier signal is a modulation technique that can experience sudden shifts in gain and is considered to be fairly inefficient. On voice-grade lines, it is typically only used for transmissions of up to 1200 bits per second. The acronym ASK refers to an approach for transmitting digital data over optical fiber. is suitable for use in light-emitting diode (LED) transmitters. To put it another way, one component of the signal is denoted by a flash of light, whilst the other component of the signal is denoted by the absence of light. Because of a "bias" current that is predetermined in the device, laser transmitters often emit only a little amount of light. This low level represents one signal element, whereas a light wave with a bigger amplitude represents another signal element.



Frequency -Shift Keying

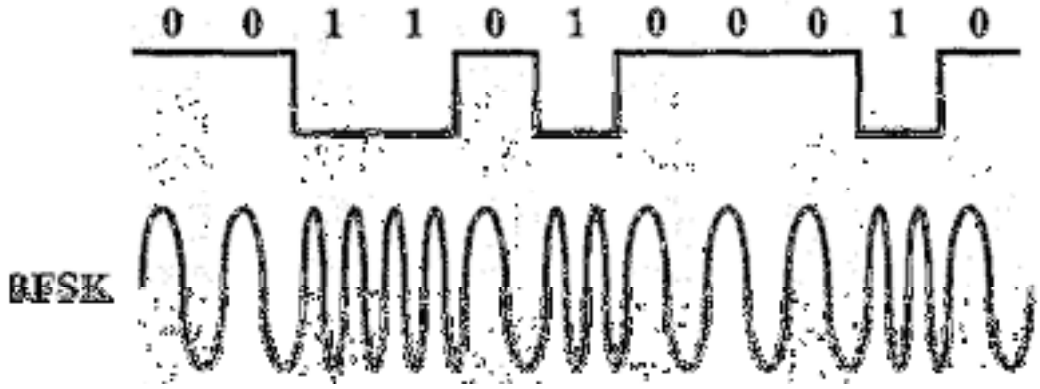
The most common version of FSK is called binary FSK (BFSK), and it uses two separate frequencies that are quite near to the carrier frequency in order to represent the two binary values.

BFSK

$$s(t) = \begin{cases} A\cos(2\pi f_1 t) & \text{binary 1} \\ A\cos(2\pi f_2 t) & \text{binary 0} \end{cases}$$

where 11 and 12 are typically placed equally apart from the carrier frequency fc, but in opposite directions from that frequency.

A voice-grade line is able to transmit sounds with a frequency range of around 300 to 3400 Hz. The term "full duplex" describes the practice of transmitting signals simultaneously in both directions. This bandwidth is split up in order to ensure that full-duplex transmission may take place. The frequencies that are utilized to represent 1 are centered on 1170 Hz, and there is a shift of 100 Hz in each direction (transmit or receive) in either of the two possible directions (transmit or receive). The modem utilizes frequencies that are shifted 100 Hz to each side of a core frequency of 2125 Hz in order to send or receive information in the opposite direction (receive or send). Keep in mind that there isn't much overlapping or interference going on. When compared to BFSK, ASK has a higher rate of error. In most cases, it is deployed over voice-grade lines at speeds of up to 1200 bps. High-frequency applications, ranging from 3 to 30 MHz, are common uses for it (3 to 30 MHz)



Phase Shift Keying

Changing the phase of the carrier signal is how data is encoded in the PSK coding scheme. PSK Two Level Binary phase-shift keying is the simplest method, and it uses two phases to represent the two binary digits. This method is also known as two-level binary phase-shift keying. The following signals are produced whenever one bit is transferred:

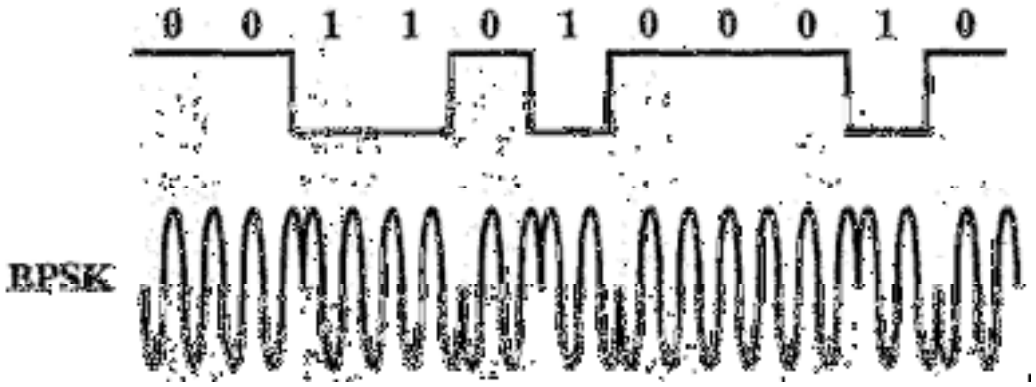
BPSK

$$s(t) = \begin{cases} A\cos(2\pi f_c t) \\ A\cos(2\pi f_c t + \pi) \end{cases} = \begin{cases} A\cos(2\pi f_c t) & \text{binary 1} \\ -A\cos(2\pi f_c t) & \text{binary 0} \end{cases}$$

Since inverting the sine wave or multiplying it by -1 is the same as a phase shift of 1800 (1T), the calculations on the far right can be used. Because of this, the formulation is straightforward. If we have a bit stream and define d(t) as the discrete function that takes on the value of +1 for one bit time if the corresponding bit in the bit stream is 1, and the value of -1 for one bit time if the corresponding bit in the bit stream is 0, then we can describe the transmitted signal as follows: If we have a bit stream and define d(t) as the discrete function that takes on the value of +1 for one bit time if the corresponding bit in:

BPSK

$$s_d(t) = Ad(t)\cos(2\pi f_c t)$$



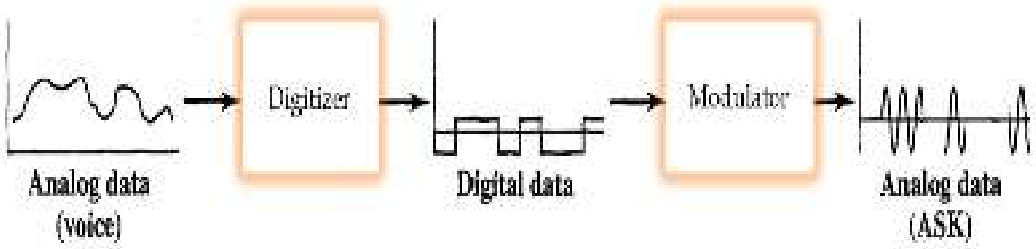
3.3 Analog Data Digital Signal

Translation of analog data into digital signals. In a more technical sense, referring to this as the digitization process, which is the conversion of analog data into digital data, may be a more accurate description of what is going on here. When analog data are converted to digital data, a great deal of potential for occurrences opens up. These are the three that come in first place:

1. The digital information can be sent using NRZ-L if desired.

2 In this particular scenario, the transformation of analog data into a digital signal was a very straightforward process. 2. It is possible to use a code other than NRZL to encode the digital data so that it may be transmitted as a digital signal. As a result, there is a requirement for one more step.

3. The digital data can be converted into an analog signal using one of the many modulation techniques.



Even though the restrictions for transmission (such as the use of microwave) dictate the use of an analog signal, the speech data may be seen as digital data since they have been digitalized. This is because the limits for transmission are analogous to the constraints for transmission. A device known as a codec is one that converts analog data into a digital form suitable for transmission, and then another device known as a coder-decoder retrieves the original analog data from the digital form (coder-decoder). In this part, pulse code modulation and delta modulation, the two most used methods for coding, are broken down and discussed. The section comes to a close with a discussion of performance evaluations made by other organizations.

Pulse Code Modulation

The sampling theorem, which forms the basis of pulse code modulation (PCM), states that if a signal is sampled at regular intervals of time and at a rate that is greater than twice the maximum signal frequency, then the samples will include all of the information that was contained in the original signal. This is because the sampling rate is greater than twice the maximum signal frequency. Reconstructing the function f(t) from this data could require the application of a low-pass filter. On the website for the book, a proof is available to any reader who is interested in purchasing it as a supplemental document. If speech data are limited to frequencies around 4000 Hz, which is a conservative approach for intelligibility, then 8000 samples per second would be sufficient to properly represent the voice signal. However, keep in mind that these PAM samples, which stand for pulse amplitude modulation, are analog. Before these analog samples can be translated to their digital equivalents, each of them needs to be assigned a binary code.

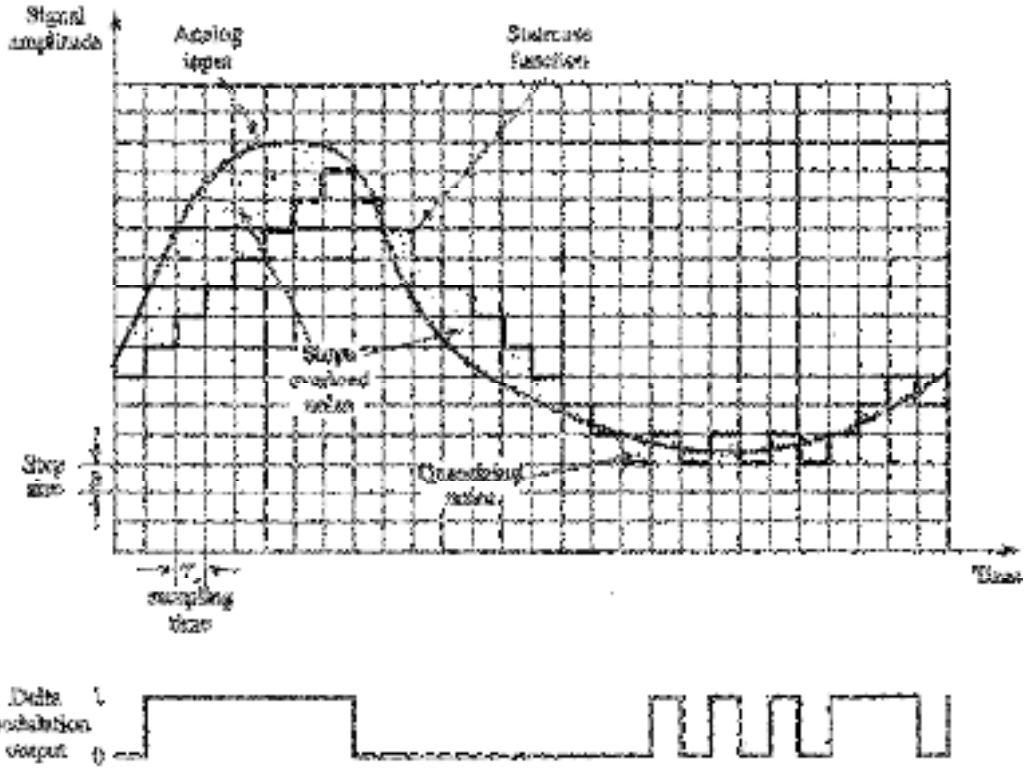
PAM samples are gathered at a rate of 2B, which translates to once per Ts = 1/2B seconds. For the sake of providing an approximation, each PAM sample is quantized into one of 16 levels. After then, it is possible to utilize four bits to represent each sample. However, due to the fact that the quantized values are only approximations, it might be challenging to exactly extract the original signal. Due to the use of an 8-bit sample, which allows for 256 different quantizing levels, the quality of the recovered speech signal is comparable to that which is reached by analog transmission. This is the case since analog transmission also uses 256 different quantizing levels. Note that this suggests that the minimum data rate necessary for transmitting a single voice signal is 64 kbps, which is equal to (8000 samples per second) X (8 bits per sample). As a consequence of this, PCM produces digital output by first converting an analog signal with continuous time and amplitude into a digital signal

Because of the utilization of nonlinear encoding, which is a popular refining approach for the PCM scheme, the quantization levels are not equally spaced with one another. The problem with having identical spacing between samples is that the mean absolute error is the same for each sample, despite the fact that the signal intensity may vary. Therefore, lower amplitude levels have much higher amounts of distortion. When quantizing low-amplitude signals, more quantizing steps should be used, whereas when quantizing high-amplitude signals, less quantizing steps should be used. This will result in a considerable reduction in the total amount of signal distortion. It is possible to achieve the same outcome by uniformly quantizing and then companding the analog signal that is being entered. Companding is a method that narrows the range of strength that a signal can have. This is accomplished by providing weaker signals on input with a larger gain than strong signals. At the output stage, the process works in the reverse direction. Be aware that the input side effect will compress the sample, which will result in a reduction of the higher values in comparison to the lower ones. When there are a set number of quantizing levels, there are therefore more levels that are accessible for lower-level signals. On the output side, the samples are extended by the compressor, which restores the values to their original form from the compressed data. Through the use of nonlinear encoding, the PCM SNR ratio is capable of being significantly improved. Voice signals have shown improvements of between 24 and 30 dB thanks to recent work.

Delta modulation

The PCM's usefulness and complexity have both been improved via the application of a wide variety of diverse approaches. One of the most well-liked alternatives to pulse code modulation (PCM) is delta modulation.

An analog input can be approximated with delta modulation using a staircase function that moves up or down by one quantization level (δ) at each sample interval (Ts), where the original analog waveform is overlaid with the staircase function. The binary nature of this staircase function, in which it either moves up or down by a predetermined amount δ at each sample time, is the primary characteristic that sets it apart from other functions. As a consequence of this, the output of each sample after going through the delta modulation process may be represented by a single binary digit. The derivative of an analog signal, rather than the amplitude of the signal, is what is utilized to approximate a bit stream: A 1 is produced if the staircase function is expected to get more steep throughout the course of the ensuing period; otherwise, a 0 is produced. The staircase function recreates the original analog waveform with as much accuracy as is achievable by allowing the user to choose the direction of the transition (either up or down) that occurs at each sampling interval.



At each sample interval, the analog input is compared to the value that was determined to be the most recent result of the approximation staircase function. In the event that the value of the sampled waveform is higher than the value returned by the staircase function, a 1 is produced; in all other cases, a 0 is generated. As a consequence of this, the staircase is continuously modified in response to the incoming signal. As a consequence of this, the receiver is able to reassemble the staircase function by employing the binary sequence that is produced by the DM process. The staircase function may then be smoothed using an integration approach or by passing it through a low-pass filter in order to provide an analog approximation of the analog input signal. This can be done in order to construct an analog representation of the signal.

Two of the most important factors to consider in a DM scheme are the sampling rate and the size of the step that is assigned to each binary digit δ that must be chosen in order to achieve a satisfactory equilibrium between two distinct types of noise or errors. When the analog waveform is changing very slowly, a phenomenon known as quantizing noise might develop. This noise is getting louder as the number 8 is increased. On the other hand, slope overload noise happens when the analog waveform changes at a rate that is faster than the staircase's ability to keep up with it. This noise is getting louder as there is less of it. It should come as no surprise that increasing the sample rate will result in improved accuracy for the system. The data rate of the output signal does, however, increase as a consequence of this change.

At each sampling time, the analog input is compared to the most recent value of the approximating staircase function. If the value of the sampled waveform exceeds that of the staircase function, a 1 is generated; otherwise, a 0 is generated. Thus, the staircase is always changed in the direction of the input signal. The output of the DM process is therefore a binary sequence that can be used at the receiver to reconstruct the staircase function. The staircase function can then be smoothed by some type of integration process or by passing it through a low-pass filter to produce an analog approximation of the analog input signal.

Performance

It is feasible to achieve high-quality voice reproduction with PCM by utilizing 128 quantization levels and 7-bit coding (27 equals 128). The bandwidth of a voice transmission is often measured in kilohertz (kHz). Therefore, in order to fulfill the requirements of the sampling theorem, one needs collect 8000 samples every single second. According to this, the PCM-encoded digital data will travel at a rate of 8000 times 7 bits per second, which is equal to 56 kbps. Consider the repercussions from the point of view of the amount of bandwidth being used. The frequency range that is occupied by an analog speech signal is 4 kHz. Using pulse code modulation (PCM), it is possible to convert this 4-kHz analog signal into a 56-kbps digital signal. However, in order to

satisfy the Nyquist criterion discussed in Chapter 2, this digital signal could require a bandwidth of around 28 kHz. Signals with a higher bandwidth exhibit variations that are significantly more obvious. For example, a common PCM system for color television uses 10-bit codes, which translates to 92 Mbps for a transmission that has a bandwidth of 4.6 MHz. In spite of these numbers, the use of digital techniques for the transmission of analog data is becoming increasingly widespread. The following are some of the primary factors contributing to this:

Because repeaters rather than amplifiers are being employed, there will not be any additional noise.

- In contrast to analog signals, which are multiplexed using frequency division multiplexing (FDM), digital signals are multiplexed using temporal division multiplexing (TDM), as we will demonstrate in the next section (FDM). TDM does not suffer from the problem of inter modulation noise, in contrast to FDM, which does, as we have demonstrated.
- The transition to digital signaling paves the way for the use of digital switching techniques that are more efficient and hence more desirable.

Summary

- In this Unit we have covered the concepts of the encoding.
- The differences among the variety of signals were discussed.
- The basic understanding behind the functionality of the digital and analog signals along with their transmission concepts
- The comparison of the digital and analog signals was done.

Keywords

ASK – Amplitude- Shift Keying

FSK – Frequency Shift Keying

BFSK – Binary Frequency Shift Keying

PSK – Phase Shift Keying

NRZ – Non Return to Zero

PCM – Pulse Code Modulation

PAM – Pulse Amplitude Modulation

SNR – Signal to Noise Ratio

DM – Delta Modulation

TDM - Time division Multiplexing

FDM - Frequency Division Multiplexing

Self Assessment

1. If Modulating frequency is doubled, the modulation index also becomes doubled the system is called

A. FM
B. AM
C. PM
D. None of the above

2. Modulation is required

A. To transmit electrical signals over an antenna through free space
B. To improve the signal to noise ratio
C. To make the low frequency signals travel long distance
D. All of the above

3. The Process of super imposing information onto a carrier wave is called
A. Communication
B. Transmission
C. Modulation
D. Demodulation

4. Which device can perform the modulation and demodulation
A. Multiplexer
B. Serial Port
C. Modem
D. HUB

5. If there is an increase in the modulation index it leads to increase in bandwidth
A. PM
B. FM
C. AM
D. Both A & B

6. In signal modulation out of the following which is not an advantage
A. Range Increase
B. Reception Quality Enhancement
C. Antenna size increase
D. Adjustment of bandwidth is allowed

7. In the Process of _____ Signals are mixed with the carrier
A. Dispersion
B. Modulation
C. Attenuation
D. Demodulation

8. Out of the following which is NOT an advantage of Modulation.
A. Efficient transmission
B. Reduced interference and noise
C. Overcoming hardware limitations
D. High power transmitters needed

9. Telegraphy uses which of the following techniques most frequently
A. FSK

B. Two tone modulation
C. PCM
D. Single tone modulation

10. When there is a condition of heterodyne on the receiver end the modulation of the signal_____.
A. Decreases
B. Has no change
C. Increases
D. Is eliminated

11. Which of the discrete values of carrier frequency is used for binary data transmission.
A. PSK
B. ASK
C. FSK
D. DSK

12. A signal is a _____ that carries data from one network to another
A. Electromagnetic
B. Electric current
C. Electronic Sign
D. None of the above

13. A signal can be in which form?
A. Audio
B. Video
C. Speech
D. All the above

14. What is modulation?
A. It is a process of converting data into electrical signals optimized for transmission
B. It is a process of converting data into analog signals optimized for transmission
C. It is a signal
D. None of the above

15. Which medium is used in radio transmission?
A. Air
B. Water
C. Space
D. Cable

16. Modulating signal has a reference line up to _____ limit
A. Line with zero

B. The peak of carrier line
C. Modulated highest point
D. Unmodulated highest point

Answers for Self Assessment

1.	D	2.	D	3.	C	4.	C	5.	D
6.	C	7.	B	8.	D	9.	A	10.	B
11.	C	12.	B	13.	D	14.	A	15.	C
16.	B								

Review Questions

1. Write and explain the difference between FSK and ASK.
2. Explain how the ASK is achieved.
3. Compare and contrast the functionality of BFSK and BPSK detail.
4. Explain the process of PCM in detail.
5. What do you understand by delta modulation?
6. Compare and contrast delta and pulse code modulation in detail.

Further Readings

- Wireless communications & networks by William Stallings, Pearson
- Principles of wireless networks by Kaveh Pahlavan, Pearson
- Fundamentals of wireless networking by Ron price, Mcgraw hill education
- Wireless networks first-step by Jim Geier, cisco press

Web Links

- http://59.51.24.50:8000/wxwl/Wireless_Communications_&_Networking_Stallings_2nd.pdf

Unit 04: Spectrum Modulation Techniques

CONTENTS

Objectives

- Understanding the spread spectrum modulation in detail.
- Analyze the frequency hopping spread spectrum .
- Understanding the difference among CDMA and GSM Technology.
- Analyzing the code division multiple access in detail.

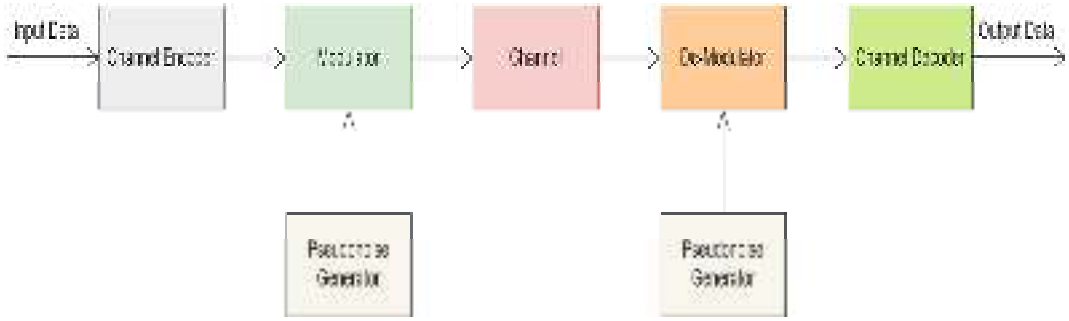
Introduction

As spread-spectrum techniques grow increasingly common, electrical professionals from outside the area are eager for concise explanations of the technology. h Some components could be difficult to understand or articulate, while others might be disregarded. Short-range data transceivers are increasingly employed in satellite positioning systems, 3G mobile telephony, and W-LAN as these technologies advance. Spread-spectrum technologies are also advantageous when radio spectrum is expensive and rare, as when communication needs surpass radio frequency availability.

4.1 Spread Spectrum Modulation

The fundamental components of any spread spectrum system are the same. A channel encoder is a device that takes information as its input and converts it into an analog signal that has a central frequency and a small bandwidth. A spreading code or a Sf reading sequence is an additional series of digits that is added to this signal in order to effect a change. The code used for spreading is generated most of the time using a pseudo noise or pseudorandom number generator; however this is not always the case. Because of this modulation, the signal that will be sent will have a significantly broader bandwidth (also known as spectrum). The same group of numbers is utilized in the process of determining what the signal is at the receiving end. After that, the signal is sent to a channel decoder so that the data may be obtained. This "waste" of the spectrum offers a lot of benefits, including the following:

- It is possible for humans to become used to the many types of noise and multipath distortion. Spread spectrum technology was initially utilized by the military due to its resistance to disruption caused by interference.



- It also has the ability to encrypt and conceal signals for you. Only a receiver that is in possession of the spreading code will be able to decipher the encoded data.
- Multiple users are able to use the same greater bandwidth without causing an excessive amount of disturbance to one another. Cell phone apps make use of this trait by employing a technology known as CDM or CDMA.

4.2 Frequency Hopping Spread Spectrum

In frequency-hopping spread spectrum, often known as FHSS, radio signals are sent in a manner that hops from one frequency to another at predetermined intervals. Because it shifts frequencies at the same time as the transmitter, a receiver is able to pick up the message being transmitted. Those who try to listen in will only hear noises that are beyond their ability to interpret. When someone makes an attempt to jam a signal on one frequency and is successful, just a portion of the transmission is disrupted.

There are several channels that have been reserved specifically for the FH signal. The majority of the time, a channel's carrier frequencies make up its carrier frequencies. The width of each channel and, by extension, the distance between carrier frequencies is typically equal to the bandwidth of the signal that is being sent in. This is because the width of each channel is proportional to the distance between carrier frequencies. For instance, the gap that is used by the EEE 802.11 standard for wireless LAN is 300 milliseconds. The transmitter is only capable of operating on a single channel at a time for a certain length of time. During that period, a certain kind of encoding is utilized in order to convey a particular quantity of bits (or maybe a fraction of a bit, as we will discuss in a later section). A spreading code determines the sequence in which the channels will be used in the transmission. It is possible to tune into a number of stations all at once by using a code that is shared between the transmitter and the receiver.

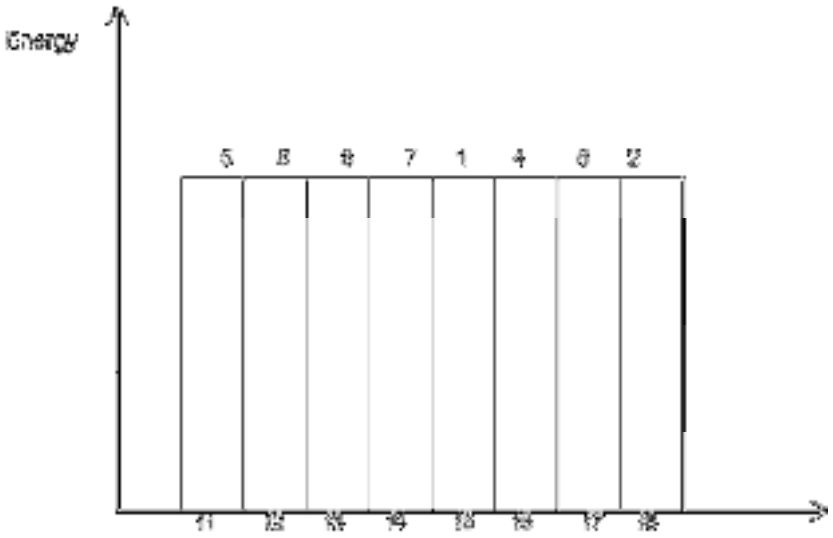


Figure 1 Assigned channels

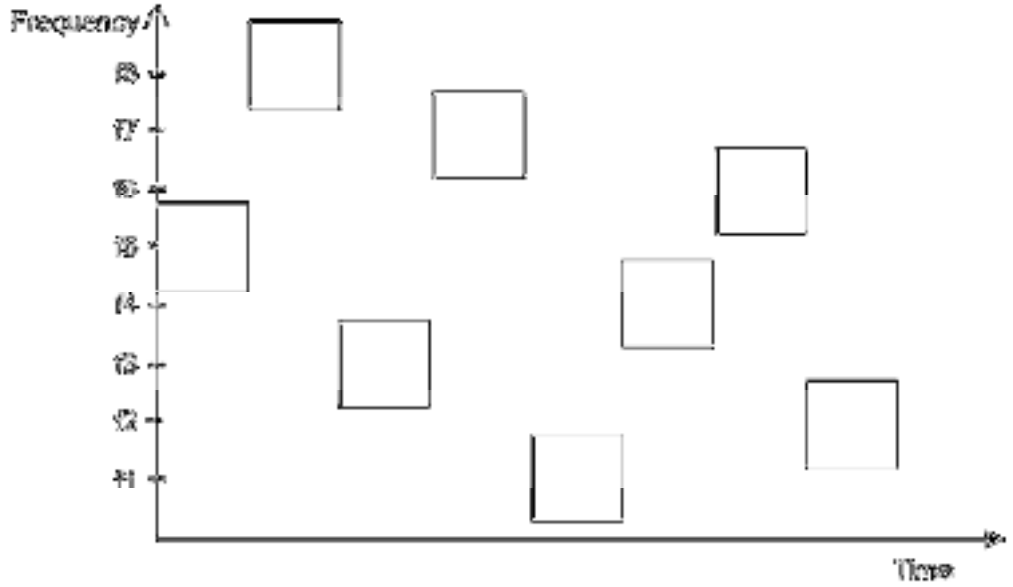
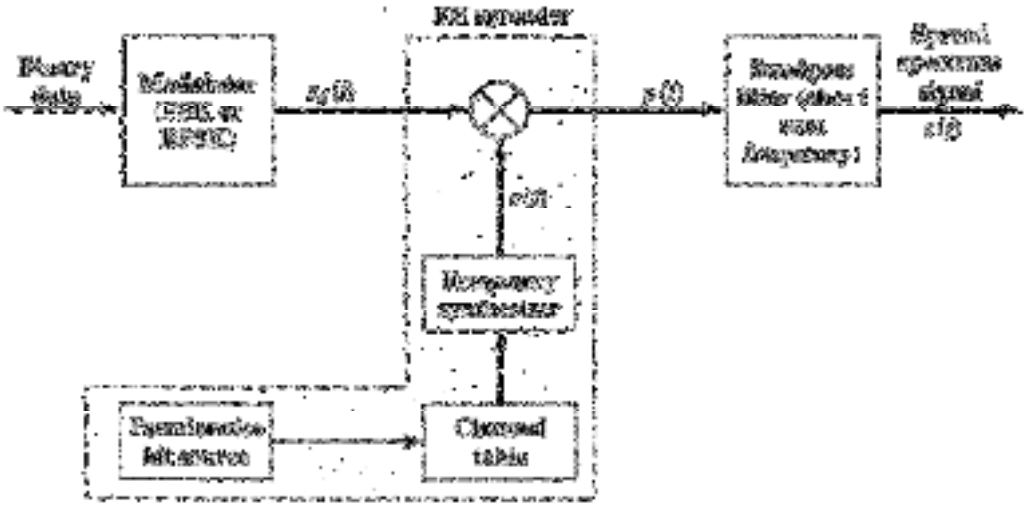
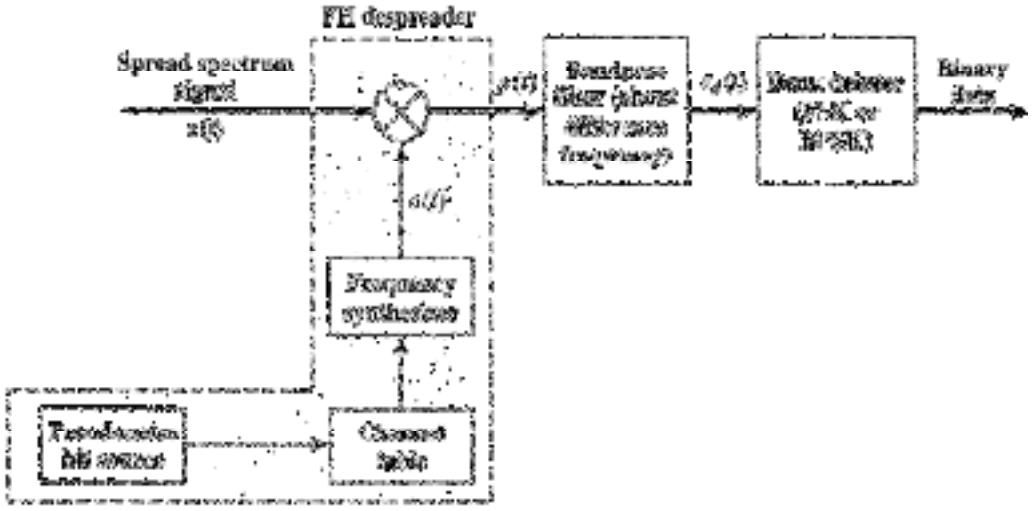


Figure 2 Channel Use

For the purpose of transmitting binary data through a modulator, a digital-to-analog encoding technique, such as binary phase-shift keying or frequency-shift keying (FSK), is utilized (BPSK). The resulting signal, denoted by Sd(t), has a frequency that serves as its basis. The code for distributing information that we were discussing before inserts a key into a table of frequencies that is derived from a source of pseudo noise, sometimes known as "pseudorandom" numbers. Each of the two thousand carrier frequencies is specified by one of the k bits that make up the PN source. A new carrier frequency, denoted by the symbol c(t), is selected at the conclusion of each succeeding time interval (per k PN bits). After then, the signal that was produced by the first modulator is modulated onto this frequency to create a new signal set that maintains the same structure but is now centered on the carrier frequency that was selected. Once the signal with the spread spectrum has arrived, it will be demodulated utilizing the same set of frequencies that were obtained from PN. The data that is still present is remodulated after this step.



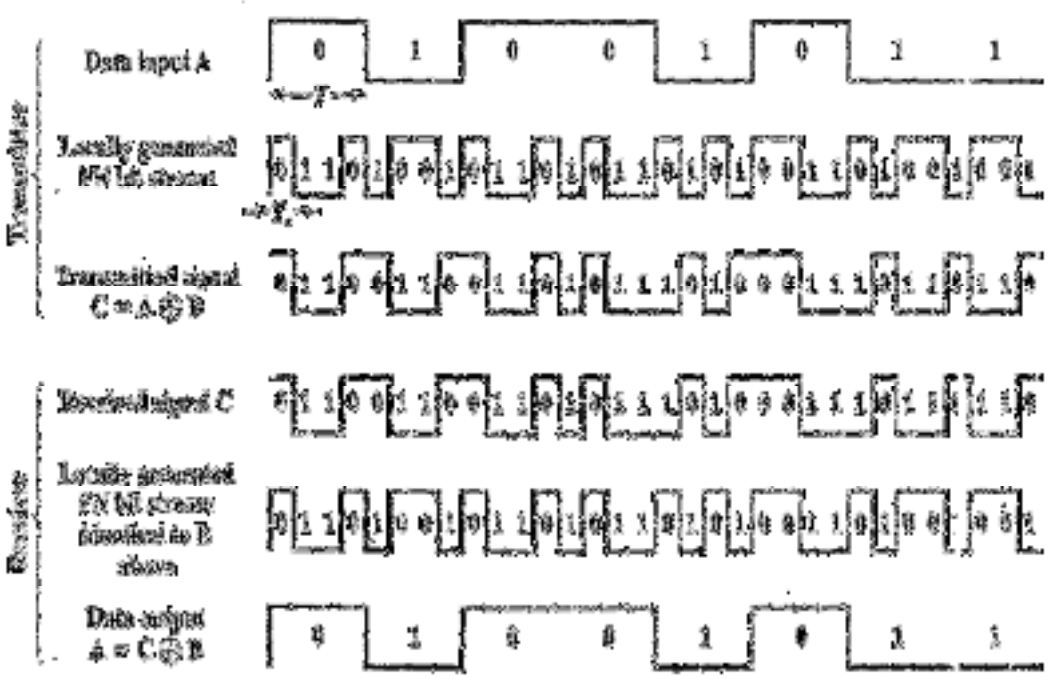


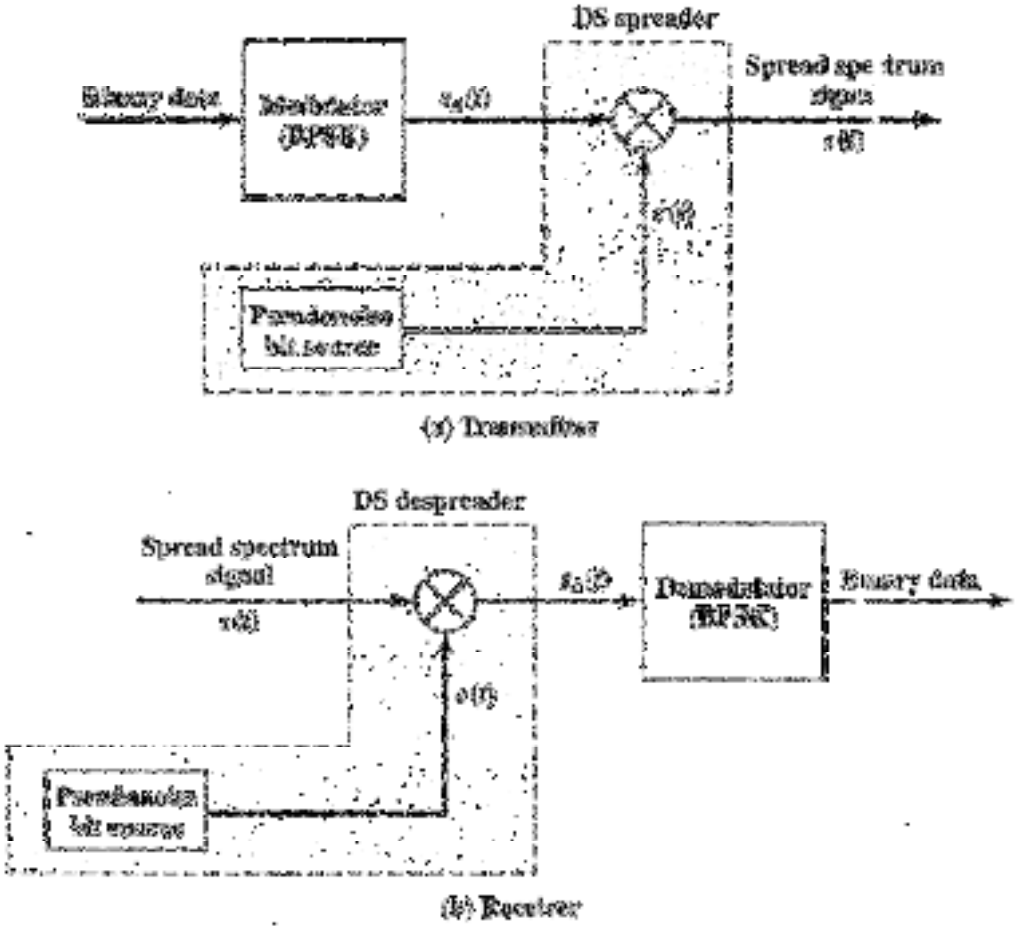
4.3 Direct Sequence Spread Spectrum

In direct sequence spread spectrum, a spreading code makes it appear as though each bit in the original signal is composed of many bits from the signal that is being sent (DSSS). The amount of bits in the spreading code contributes directly to the degree to which the signal is dispersed across a greater frequency range. When compared to a 1-bit spreading code, a 10-bit spreading code may spread the signal over a frequency range that is ten times more extensive. Utilizing an exclusive-OR gate is one method for connecting the digital information stream with the spreading code bit stream in direct sequence spread spectrum transmissions (XOR).

$$0 \oplus 0 = 0 \qquad 0 \oplus 1 = 1 \qquad 1 \oplus 0 = 1 \qquad 1 \oplus 1 = 0$$

When the information bit is set to zero, the combination's spreading code bits are transmitted without any inversion taking place. When the information bit is in the "one" position, the bit is in the "zero" position. The combined it stream has a greater bandwidth than the information stream because it operates at the same data rate as the first spreading code sequence.





4.4 Code Division Multiple Access

The abbreviation for Code Division Multiple Access (CDMA) is "CDMA." This is one of the protocols that may be found in wireless communications of both the second generation (2G) and the third generation (3G) (Code-Division Multiple Access). CDMA, which stands for code division multiple access, is a form of multiplexing that, as its name indicates, allows several signals to share a single transmission channel. The available bandwidth is utilized to its full potential as a result. This technology is implemented in the UHF mobile phone networks that operate at 800 megahertz (MHz) and 1.9 gigahertz (GHz) bands respectively.

Spread spectrum technology and analog-to-digital conversion are both utilized in CDMA transmission (ADC). First, the audio signal is converted into bits and stored digitally. Alterations are then made to the frequency of the signal that is being transmitted in response to a pattern code. This indicates that the signal may be picked up by a receiver only if it has the same code as the transmitter and a frequency response that is identical to the frequency being broadcast by the transmitter. It is much simpler to conceal one's identity when cloning is difficult to do and there are billions of different frequency sequencing sequences that might be used.

The cell architecture of wireless CDMA networks is composed of cell clusters, which work together to form the cell. Mobile units are dispersed across the coverage area of a cell, and each cell that makes up a cell cluster is equipped with a transceiver that has the appropriate amount of transmitting power. Every mobile unit has a transceiver built into it. It functions in a wireless cellular environment thanks to its sensitive receiver and low-power transmitter, both of which are integrated inside the device. Access interference, fading, and multipath propagation are a few of the components that come together to make up the cellular environment.

The near-far effect, also known as the N-F effect, has a significant impact on the quality of service (QoS) provided by CDMA networks. It is a phenomenon that takes place when a user who is located in close proximity to the base station delivers a signal that interferes with and drowns out a signal sent by a user who is located further away. In order to do this, the operators of CDMA

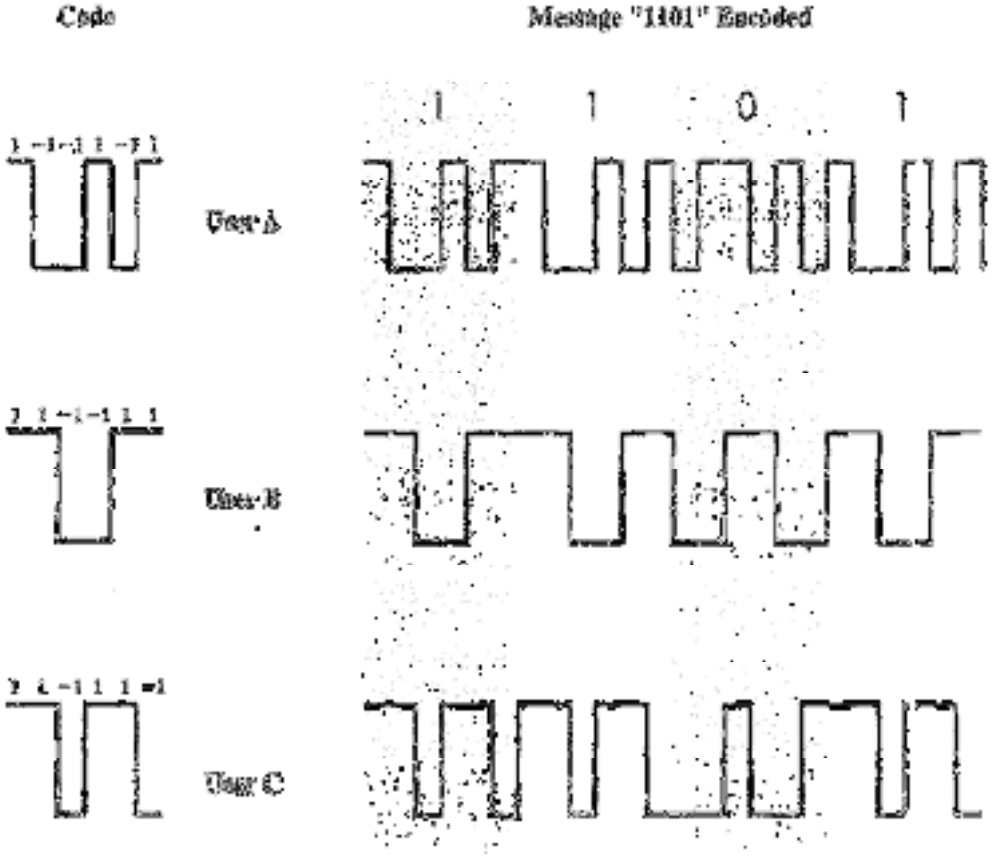
networks make use of receivers that are immune to the N-F effect as well as stringent measures for regulating power.

1.23 MHz is the width that is used for the CDMA channel. Soft handoff is a technique utilized by CDMA networks to ensure that mobile devices have minimal signal degradation as they transition from one cell to another. When digital and spread spectrum are used together, they enable a significantly higher number of signals to be sent across a given amount of bandwidth compared to analog modalities. CDMA is compatible with a variety of different mobile phone technologies, which enables it to support national roaming. The first version of CDMA, also known as CDMA One, was only capable of transmitting data at speeds of up to 14.4 kilobits per second via a single channel and 115 kilobits per second when using all eight channels simultaneously. W-CDMA and CDMA2000 are both capable of sending data at significantly quicker speeds.

The Single-carrier Radio Transmission Technology (1xRTT), Evolution-Data Optimized Release 0 (EVDO Release 0), Evolution-Data Optimized Revision A (EVDO Revision A), and EVDO Revision B are all part of the CDMA2000 family of standards. People frequently get CDMA and CDMA2000, which are two different sets of standards, mixed up. CDMA is a protocol for the physical layer, whereas CDMA2000 is a set of standards that both Verizon and Sprint support.

CDMA, or code division multiple access, is a technique of multiplexing that is used in conjunction with a spread spectrum system. This is how the process goes. The bit data rate, which has a rate of D, is the signal with which we begin our analysis. We break up each bit into k chips according to the user's code, which is a set of rules that is exclusive to that user and cannot be used by anyone else. The chip data rate of the new channel is kilobytes per second (kD chips/sec). For this, we will use a straightforward example4 with the value of k set to 6. It is most straightforward to describe a code as a string of consecutive ones and zeros.

Explanation of CDMA functionality



characterize a code as a sequence of 1s and -1s. shows the codes for three users, A, B, and C, each of which is communicating with the same base station receiver, R. Thus, the code for user A is CA = <1,-1,-1,1,-1,1> . Similarly, user B has code CB =<1,1,-1,-1,1,1> , and user C has Cc = <1,1,-1,1,-1>.

Now that we have that out of the way, let's have a look at what goes down while user A is communicating with the base station. It is likely that the base station is familiar with A's code. We'll assume that the transmission is already timed, so that the base station is aware of when to search for codes in order to keep things as straightforward as possible. If a wishes to transmit a bit value of 1, it will send its code in the form of a. (hip pattern). In the event that a 0 bit has to be transmitted, A will send the complement of its code, which is written as -1,1,1, -1, 1, -1>. (1s and -1s inverted). The receiver located at the base station is responsible for reading the chip patterns. In our simplified model, if the receiver R receives the chip pattern d = [d1, d2, d3, d4, d5] and it is attempting to connect with a user u so that it may obtain the user's code [c1, c2, c3, c4, c5, c6], the receiver then performs the following electrical decoding procedure. Su(d) = (d1 xc1) + (d2 X c2) + (d3 X c3) + (d4 X c4) + (d5 X c5) + (d6 X c6)

The subscript u on S simply indicates that u is the user that we are interested in. Let's suppose the user u is actually A and see what happens. If A :~ends a 1 bit, then dis and the preceding computation using SA becomes

S_A(l, -1, -1, 1, -1, 1) = [1 X 1] + [(-1) X (-1)] + [(-1) X (-1)] + [(-1) X (-1)] + [1 xl] = 6

If A sends a 0 bit that corresponds to d = <-1,1,1, -1,1, ->, we get

S_A(-l, 1, 1, -1,1, -1) = [-1 X 1] + [1 x (-1)] + [1 x (-1)] + [(-1) x 1] + [1 x (-1)] + [1 x (-1)] + [(-1) :(1] = -6

Now that we have that out of the way, let's have a look at what goes down while user A is communicating with the base station. It is likely that the base station is familiar with the code associated with A. We'll assume that the transmission is already scheduled such that the base station is aware of when to search for codes in order to keep things as straightforward as possible. If a needs to transmit a 1, it will send its code in the form of a. (hip pattern). When it is necessary to send a 0 bit, A will send the complement of the code, which is written as -1,1,1, -1, 1, -1>. (1s and -1s turned upside down). A receiver is located at the base station, and it is responsible for reading the chip patterns. If the receiver R gets a chip pattern d = [d1, d2, d3, d4, d5] and is trying to connect with a user u to get u's code [c1, c2, c3, c4, c5, c6], then the receiver performs the following electrical decoding operation. In our simplified version of this scenario, if the receiver R gets a chip pattern d = [d1, d2, d3, d4, d5 If B sends a 1 bit, then d =<1,1,-1,-1,1,1> . Then

S_A(l,l,-l,-l,l,1) = [1 x 1] + [1 x (-1)] + [(-1) x (-1): + [(-1) xl] + [1 x (-1)] + [1 Xl] = 0

As a result, the unwanted signal that was coming from B no longer shows up. If B had given a 0 bit, the decoder would have again given a value of 0 for SA. It's easy to make sure this is true. This proves that SA(SA + SB) = SA(SA) + SA(SB) = SA. If the decoder is linear and A and B send out signals SA and SB at the same time, the decoder will only be able to pick up SA (SA). This is because when the decoder uses A's code, it doesn't pay attention to B. So, if the decoder is linear, SA(SA + SB) = SA(SA) + SA(SB) = SA (SA). If SA(CB) = SB(CA) = 0 in both cases, then the codes of A and B are said to be orthogonal. Even though these kinds of codes are very nice to have, not many people actually have them. When X is bigger than Y, it happens more often than you might think for Sx(Cy) to have a low absolute value. When this happens, it's easy to tell which two situations X and Y are the same and which ones they aren't. SA(Cc) = Sc(CA) = 0 in this case, but SB(Cc) = Sc(CB) = 2. In the second case, the decoded signal would not be affected much by the C signal, but not at all by the O signal. Using a decoder called Su, the receiver can figure out that the signal came from you, even if there are other users broadcasting in the same cell. Even if a user could change things, this is still possible.

In real life, the CDMA receiver can filter out signals from unwanted users by making them look like low-level noise. But the system won't work if there are other users trying to use the same channel as the user the receiver is trying to listen to, or if the signal power of one or more competing signals is too strong, which could be because they are too close to the receiver.

Differentiating Between GSM and CDMA Technology

When trying to move their phones from one cellular network provider to another, the vast majority of consumers become entangled in the argument between the GSM and the CDMA. Because certain carriers' phones can only be made to function on their radio network, they are not compatible with the mobile phone technology used by other networks. Several years ago, incidents like these occurred far more often. Recently, firms that specialize in the production of electronics have begun manufacturing phones that are compatible with both CDMA and GSM networks.

Several-access technologies, such as GSM and CDMA, enable multiple users to connect to the same radio channel at the same time and engage in simultaneous conversation. Each call in CDMA cellular systems is given its own unique code to utilize for encoding the data. After then, they sent all of the calls at the same time. At the other end, receivers take the combined signal and split it up into individual calls before distributing them to the appropriate parties. Every call is converted into digital data using GSM, and then the information is reassembled at a predetermined time for the person who is on the other end of the connection. This takes place on a channel that is shared with others.

Who are the service providers for CDMA? Which of these are GSM standards? GSM is currently utilized in over 200 different nations. Verizon and U.S. Cellular are two of the most prominent carriers in the United States that make use of CDMA technology. T-Mobile and AT&T are both examples of GSM service providers in the United States.

Performance Comparison of GSM and CDMA

In contrast to CDMA networks, GSM networks are capable of simultaneously transmitting voice and data communications. CDMA networks are unable to perform this task. However, this is not the primary reason why individuals favor GSM. A regulation from 1987 mandated the adoption of GSM technology throughout Europe, which served as a significant driving force. Another aspect to consider is that GSM was produced by a consortium of firms working together, whereas the majority of CDMA products were manufactured by Qualcomm. This resulted in GSM phones having lower production and operating costs.

Only two- and three-generation connections can use the CDMA and GSM protocols respectively. In 2010, when the transition to 4G networks started in earnest, carriers immediately embraced Long-Term Evolution (LTE), which is the global standard. As a consequence of this, the distinction between CDMA and GSM is losing some of its significance as GSM-powered devices grow more widespread and CDMA phones become rarer. However, the 2G and 3G networks are still utilized as backups in locations where the signals for 4G LTE are not strong as of yet.

Parameters	**GSM**	**CDMA**
SIM	Required & Removable	Non-Removable & integrated
Voice Quality	High & Good	Poor Quality in congested network
Security	Less secure	More Secure
Spread Spectrum	Applicable	Not applicable
System capacity	Less	3 to 4 time higher than GSM
Frequency reuse	Maximum 3	Maximum 1
Handoff	Hard Handoff	Soft Handoff

Advantages of CDMA technology

- Because it offers a multitude of advantages, CDMA is the most advantageous technology for 3G mobile phones.
- Capacity and security are both improved as a result of this. The ability of CDMA to support ever-increasing network capacity is one of the most important aspects of this line of reasoning. The technique known as code division multiple access, or CDMA, separates the transmission of voice and data packets by making use of a broad variety of frequencies and codes that are exchanged via codes. Through the use of CDMA, a terminal is able to easily communicate with two base stations at the same time. This is due to the fact that CDMA makes a large

amount of information space available, which is gradually becoming more standardized and is appealing to the 3G speed of mobile internet use. The previous connection has been severed, and the new connection has been established in its stead. Handoffs or modifications made from one base station to another base station are made more dependable as a result of this. Every aspect of CDMA has received further attention, which has made it feasible to make the numerous adjustments that are necessary for mobile communications networks.

- Signal congestion on the subscriber's phone is caused by channel pollution, which prevents any one cell site from assuming control of the network. If things continue to grow worse, the sound quality will continue to deteriorate. CDMA does not have the capability to travel worldwide, in contrast to GSM. CDMA does not make it simple to move to or upgrade to another handset since the information about the network service is integrated into the phone itself. This is in contrast to GSM, which allows users to do this by inserting a SIM card into their phone. As of right now, it is only compatible with mobile service providers that utilize the GSM standard, which is why it only provides a limited selection of devices.

Summary

- In this Unit we have discussed the concepts of spread spectrum modulation.
- Frequency hopping spread spectrum and the direct sequence spread spectrum was discussed.
- The basic operation of FHSS and DSSS sending and receiving operations were discussed.
- The code division multiple access was discussed briefly along with the comparison of GSM and CDMA technology.

Keywords

CDMA - Code division multiple Access

CDM - Code division multiplexing

FHSS - Frequency Hopping spread spectrum

LAN - Local Area Network

BPSK – Binary phase shift keying

DSSS - Direct sequence spread spectrum

UHF - Ultra high frequency

ADC - Analog to digital conversion

EVDO - Evolution-Data Optimized Revision

GSM - Global system for mobile communication

Self Assessment

1. A pseudo code generator which creates the K-bit pattern for hopping called is called

A. Hopping

B. Carrier Signal

C. Frequency Synthesizer

D. Pseudorandom noise

2. In the FHSS ,the privacy between the sender and receiver can be maintained if the hopping period is

A. Long
B. Short
C. Zero
D. Infinite

3. The Data rate used in IEEE 802.11 DSSS approach is

A. 2 Mbps
B. 6 – 54 Mbps
C. 5.5 and 11 Mbps
D. 2 and 54 Mbps

4. Is DSSS bandwidth can be increased by replacing every bit with

A. n+1 bits
B. n-1 bits
C. n bits
D. n*1 bits

5. The spread spectrum is used to transmit which type of following data

A. Analog data
B. Digital data
C. Both Analog and Digital
D. None of the mentioned

6. Spread spectrum is a technique used for _____.

A. Encoding
B. Decoding
C. Both Encoding and decoding
D. None of the above

7. Due to spread spectrum it becomes difficult to do _____ of the signals.

A. Interception
B. Jamming
C. Jamming & Interception
D. None of the mentioned

8. Spread spectrum is immune from.

A. Noise
B. Multi-path distortion
C. Noise & Multi-path distortion
D. None of the above

9. For final FHSS signal which filter is used

A. Low pass filter
B. High pass filter
C. Band stop filter
D. Band pass filter

10. IN the CDMA the incoming signal is _____ with the spreading code.
A. Added
B. Multiplied
C. XOR-ed
D. AND-ed

11. In the DSSS the signal is recovered by using the .
A. Low pass filter
B. High pass filter
C. Band stop filter
D. Band pass filter

12. The transmission bandwidth of spread spectrum techniques is equal to the minimum required signal bandwidth.
A. True
B. False

13. The spread spectrum is inefficient for the single user due to its
A. Large transmission bandwidth
B. Small transmission bandwidth
C. Fixed transmission bandwidth
D. Fixed null bandwidth

14. DSSS system spreads the baseband signal by _____ the baseband pulses with a pseudo noise sequence.
A. Adding
B. Subtracting
C. Multiplying
D. Dividing

15. Frequency hopping involves a periodic change of transmission _____
A. Signal
B. Frequency
C. Phase
D. Amplitude

16. FH systems do not have collisions.
A. True

B. False

Answers for Self Assessment

l.	A	2.	B	3.	A	4.	C	5.	C
6.	A	7.	C	8.	C	9.	D	10.	B
11.	D	12.	A	13.	A	14.	C	15.	B
16.	B								

Review Questions

1. Write and explain the difference between DSSS and the FHSS technique
2. Explain how the CDMA and GSM technology different for one another.
3. Compare and contrast the functionality of BFSK and BPSK detail.
4. Explain the CDMA functionality in detail.
5. Elaborate the concept of Spread spectrum Modulation in detail.
6. Explain the FHSS sender process in detail.

Further Readings

- Wireless communications & networks by William Stallings, Pearson
- Principles of wireless networks by Kaveh Pahlavan, Pearson
- Fundamentals of wireless networking by Ron price, Mcgraw hill education
- Wireless networks first-step by Jim Geier, cisco press

Web Links

- http://59.51.24.50:8000/wxwl/Wireless_Communications_&_Networking_Stallings_2nd.pdf

Unit 05: Multiple Access in Wireless System

CONTENTS

Objectives

- Understanding the types of multiple access systems.
- Analyzing the differences between the narrow band and wide band signals.
- Understanding the frequency division multiple access and its variants.
- Analyzing the FDMA in telephony.
- Evaluate the different Multiple access protocols in wireless technology.

Introduction

The adoption of multiple access techniques makes it possible for a large number of mobile users to share the same amount of radio spectrum at the same time. It is necessary to share spectrum in order to achieve a high capacity, which is accomplished by providing the available bandwidth to a number of users all at once. To maintain the system's high level of performance while still achieving the desired level of communication quality, this step must be taken. When possible, it is usually a good idea to give the subscriber the ability to submit information to the base station at the same time as he or she receives information from the base station. By way of illustration, using conventional phone systems, it is possible to both speak and listen at the same time. The ability to do both at once is known as "duplexing," and it is typically required in wireless phone networks. Frequency domain methods or time domain techniques can be utilized to achieve duplexing. The technology known as frequency division duplexing, or FDD, provides each user with two distinct frequency bands. Traffic is sent from the base station to the mobile device via the forward band, while traffic is transmitted from the mobile device to the base station via the reverse band. Each duplex channel in FDD is composed of two simplex channels: one that transmits in the forward direction, and one that transmits in the reverse direction. At order for the subscriber unit and the base station to simultaneously broadcast and receive radio signals on the duplex channel pair, a device known as a duplexer is utilized in both locations. There is never a change in the frequency difference that exists between the forward and reverse channels, regardless of which channel is being utilized. By use time rather than frequency, the technology known as time division duplexing, or TDD, may create both a forward and a reverse link. When using TDD, users of the system share a single radio channel by taking turns in the time domain. Every user is assigned a time slot to utilize the channel, and every duplex channel has a forward time slot as well as a reverse time slot to ensure that communication may occur in both directions. Users at the subscriber unit and the base station may become confused if there is not a significant amount of time between the forward and reverse time slots. In this scenario, users may believe that data is being sent and received at the same time. Demonstrates FDD and TDD approaches. TDD frees

users from the shackles of using two distinct simplex or dedicated communication channels by permitting them to converse on a single channel instead. Because of this, subscriber equipment does not require a duplexer, which makes it easier for users to use.

5.1 Multiple Access Schemes

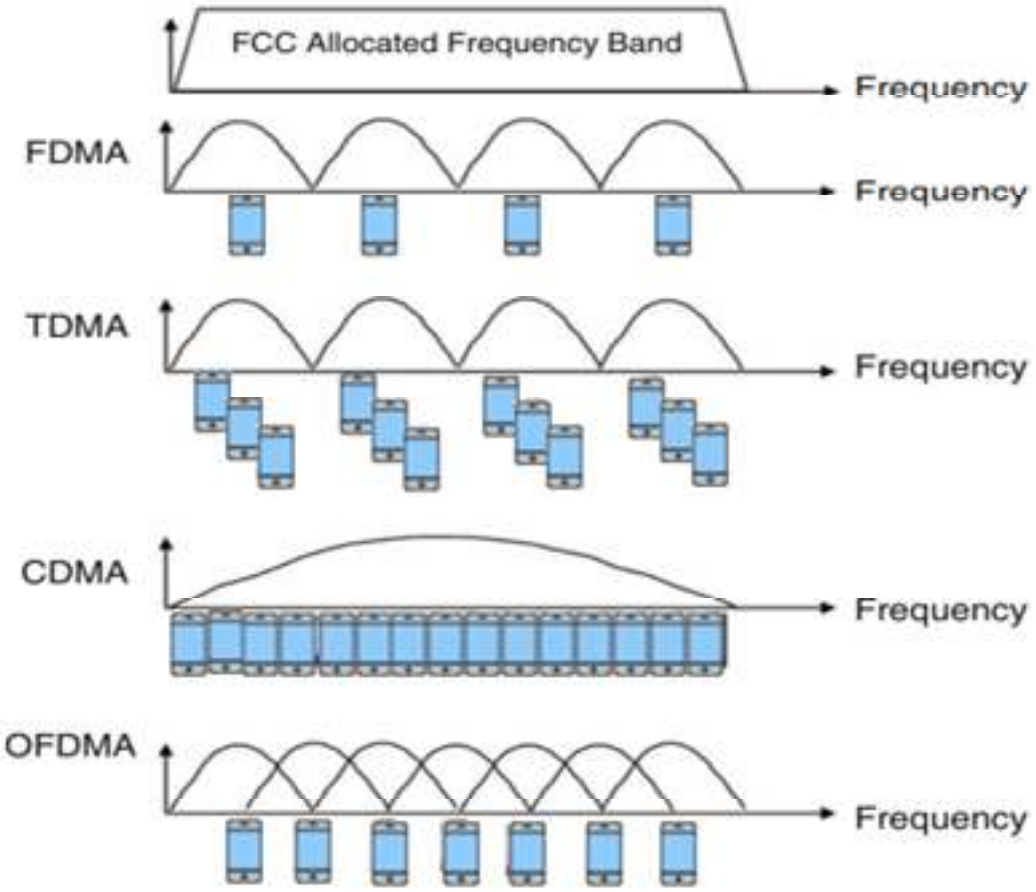
The three primary methods by which a wireless communication system divides and shares the available bandwidth is called frequency division multiple access (FDMA), time division multiple access (TDMA), and code division multiple access (CDMA). On the basis of the manner in which the users are distributed throughout the available bandwidth, these approaches may be subdivided into narrowband and wideband systems. When discussing a multiple access system, the duplexing approach of the system is frequently brought up at the same time as the particular multiple access strategy.

Narrowband Systems

When referring to the bandwidth of a single channel and its predicted coherence bandwidth, the term "narrowband" is used to describe the relationship between the two. The radio spectrum is partitioned into a great number of narrowband channels when a narrowband multiple access system is used. FDD is the method that is utilized for the majority of channel operations. Within the frequency spectrum, the frequency separation between forward and reverse connections on each channel is as wide as it can possibly be made. This not only minimizes interference but also enables each subscriber unit to employ duplexers that are more economically priced and only one transceiver antenna. When FDD is implemented, the system is referred to as FDMA/FDD. This indicates that each duplex channel possesses both a forward and a backward simplex channel. Each user in a narrowband FDMA system is assigned a distinct channel that is not shared with any other users in the immediate area. Narrowband Time Division Multiple Access (TDMA), on the other hand, enables users to share the same radio channel while maintaining a small number of users physically separated in time on a single channel by assigning each user a specific time slot. The vast majority of radio channels for narrowband TDMA systems are typically assigned via either FDD or TDD, and TDMA is utilized to facilitate the sharing of each channel. The acronyms TDMA/FDD and TDMA/TDD are used to refer to both of these types of access systems.

Wideband Systems

In the wideband systems, the transmission bandwidth of a channel is substantially greater than its coherence bandwidth. This is because wideband systems use several channels. Because of this, frequency selective fades only occur in a very small portion of the signal bandwidth at any given time, and multipath fading has a very small effect on the strength of the received signal in a wideband channel. Both of these phenomena are a result of the fact that wideband channels have a much larger signal bandwidth than narrowband channels. In wideband multiple access systems, many transmitters are able to use the same channel all at once without interfering with one another. With spread spectrum CDMA, many transmitters are able to use the same channel at the same time. TDMA, on the other hand, assigns a time slot to each transmitter on the same channel, and it only permits one transmitter at a time to utilize the channel for transmissions. Both FDD and TDD multiplexing are able to be utilized in CDMA and TDMA systems respectively. In addition to frequency division multiple access (FDMA), time division multiple access (TDMA), and code division multiple access (CDMA), there will be two other kinds of multiple access utilized for wireless communications. These two technologies have been given the designations Space Division Multiple Access and Packet Radio.

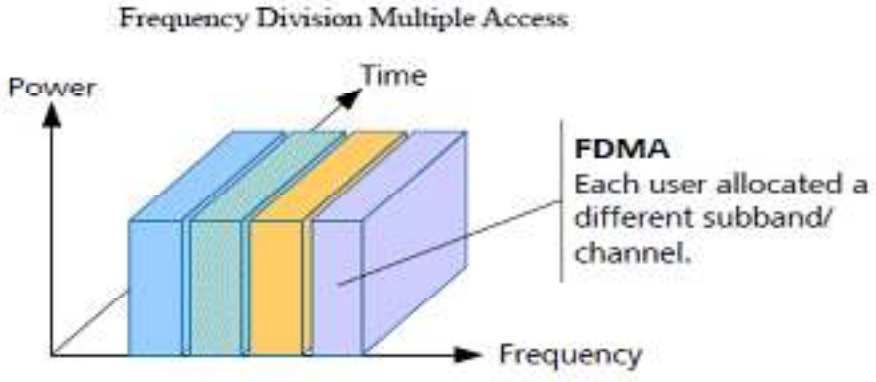


5.2 Frequency Division Multiple Access (FDMA)

Different users are given their own channels while using FDMA, which stands for frequency division multiple accesses. In this scenario, each user has their own frequency band or channel to work with. Users that request service on an as-needed basis are provided access to these channels. During the time that the call is active, no one else will be able to utilize the channel. Each user is assigned a pair of frequencies to utilize in FDD systems; one of these frequencies is referred to as the forward channel, while the other is referred to as the reverse channel. The following is a list of things about FDMA:

- The FDMA channel is only capable of handling a single incoming call at a time.
- An FDMA channel is considered idle while it is not being utilized, and other users are unable to share it or make it larger at this time. In its most basic form, it constitutes a frivolous expenditure of a valuable resource. FDMA, or frequency division multiple access, in which unique frequency bands are allocated to each channel
- Once a voice channel has been selected, the base station and the mobile device will simultaneously transmit signals to one another.
- Because each FDMA channel is only permitted to have one circuit per carrier, the available bandwidths for these channels are not particularly large (30 kHz in AMPS). To put it another way, FDMA is typically implemented in communication systems that have a limited bandwidth.
- In a signal with a narrow bandwidth, the symbol time is significantly greater than the delay spread. Due to the fact that there is very little to no interference between symbols as a result of this, FDMA narrowband systems do not require very much or any equalization.

- Even though TDMA mobile systems are more technologically advanced than FDMA mobile systems, this is starting to change as TDMA's digital signal processing capabilities get better.
- FDMA is different from TDMA in that transmissions can happen at any time. It's different from TDMA because of this. This means that "overhead" functions don't use as many bits as they need to (such as synchronization and framing bits). Because they only have one channel per carrier and need expensive bandpass filters at the base station to get rid of unwanted radiation,
- FDMA systems are more expensive than TDMA systems. Also, the FDMA mobile unit has duplexers because both the transmitter and the receiver work at the same time. This makes base stations and FDMA subscriber units more expensive. For FDMA to work, the RF filtering has to be very strict so that other channels don't mess with it.



Nonlinear Effects in FDMA

In a system that employs frequency division multiple access (FDMA), the antenna at the base station is shared by more than one channel at any given moment. In order to extract the maximum amount of power from power amplifiers and power combiners, they must be operated in a nonlinear fashion very close to or just at their points of saturation. Intermodulation frequencies are caused by nonlinearities, which also contribute to the spreading of signals throughout the frequency domain. It may be difficult for other channels to function properly in FDMA systems if there is interference from undesired radio frequency radiation, often known as IM. Spectrum spreading is the root of the problem that results in interference between channels that are located in close proximity to one another. Intermodulation results in the generation of harmonics, which you do not want. Harmonics created outside of the mobile radio frequency can disrupt the operation of neighboring services. On the other hand, harmonics that are created inside the band cause interference for users of other wireless systems. The Advanced Mobile Phone System (AMPS), which was the first analog cellular network in the United States, was built on FDMA/FDD as its underlying technology. A single user makes use of a single channel during the duration of a conversation. This channel is really composed of two simplex channels that are frequency duplexed with a 45 MHz split. When one mobile user's call concludes or is transferred to another, the channel becomes available for usage by another mobile user. Because each user has their own channel, AMPS allows several users to use it at the same time without interference from one another. The voice signals that are sent from the base station to the mobile device are done so through the forward channel. The voice signals that are sent from the mobile device to the base station are transmitted over the reverse channel.

Key Points to remember about FDMA

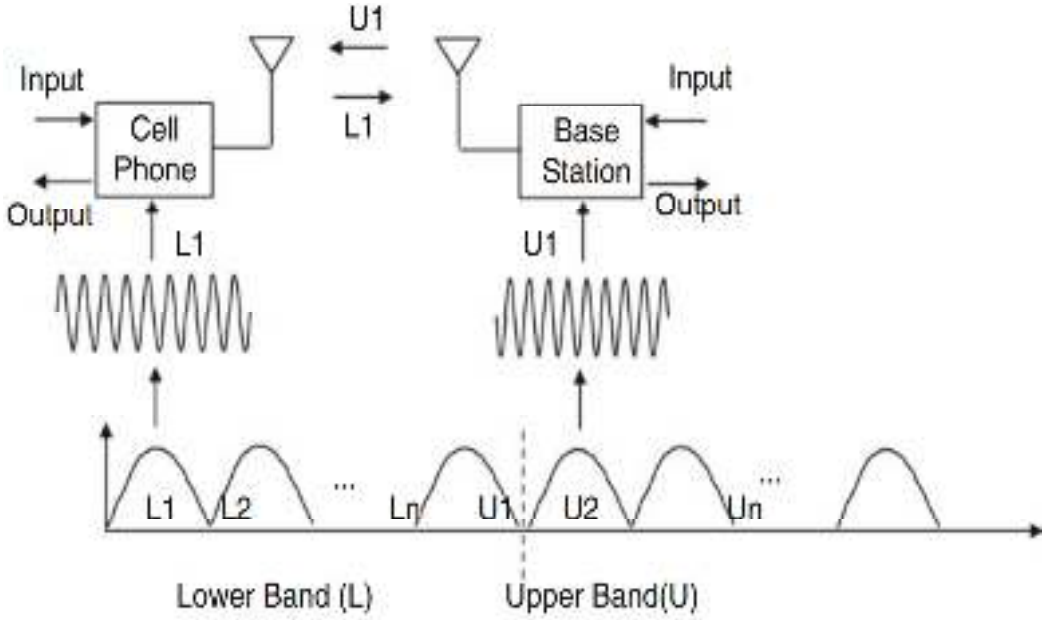
- The user is assigned a particular frequency. One user is serviced by a single channel in an FDMA network at any given moment.
- It is required that users remain on the channel for the whole of the call.
- In the event that the quality of the transmission link deteriorates, the controller will switch the system over to another channel.

- FDMA is inefficient with bandwidth since it can only manage voice traffic; this is despite the fact that it should be simple to install. It is incapable of processing any other kinds of data.
- The FDMA protocol is currently the most widely used method for accessing networks, particularly for satellite communication. It had widespread application in the early telephone and wireless communication systems, particularly those that supported simultaneous conversations between several users.

During a call, one carrier frequency is utilized from the lower band, and one carrier frequency is utilized from the upper band. The radio in the mobile device operates at a lower frequency, while the radio in the base station operates at a higher frequency. Whenever a call is made with this technique, there are always two channels in use. It is essential to be aware that the mobile device operates on lower frequencies since the strength of the signal decreases as the frequency increases. Due to its limited power output, the radio in the mobile phone must operate at lower frequencies than those used by the base station. The first-generation (1G) cellular communication system, also known as AMPS (advanced mobile phone system), makes use of a technique known as frequency-division multiple access (FDMA) so that more than one person may use their phone at the same time.

FDMA Technique

A carrier frequency from the upper band and a carrier frequency from the lower band are both used during a call. The mobile radio operates at a frequency in the lower band. The base station radio operates at a frequency in the upper band. When using this strategy, the call will continuously utilize both of the available channels. Lower frequencies are employed in mobile communication because of the logarithmic relationship between the propagation decay rate and frequency. Mobile phones must operate at lower frequencies since their transmit power is far lower than that of base station radios. Frequency division multiple access (FDMA) technology was utilized by the advanced mobile phone system (AMPS), also known as the first-generation (1G) cellular communication system, to enable simultaneous use of the network by numerous users.



FDMA-FDD

The FDMA-FDD technique divides all of the channels that are usable into two distinct bands: the bottom band and the upper band. After that, we pair them off using the following procedures: Ln Un, L1U1, L2U2, You can see that FDD makes use of two distinct frequencies in the picture that is shown above. One of these frequencies is used for uploading, while the other is used for downloading. In between these two frequencies is a guard band. Therefore, even when both broadcasts are taking place at the same time, there won't be any interference. The FDMA-FDD technique is the name given to this particular approach. The following is a simplified explanation of how FDMA-FDD communication is utilized by the 1G cellular systems:

- The carrier frequency (U1) from the upper band is altered by the base station, and the resulting signal is transmitted to the mobile phone. Either an analog signal or a digital signal may be utilized in its place as the input modulating signal.
- The mobile device, which has the same carrier frequency as the base station, will, after a brief interval of waiting, receive the modulated carrier from the base station. The mobile then modulates a separate carrier frequency (L1) from the lower band and transmits it back to the base station in response. After that, it demodulates the carrier in order to regain access to the information signal.
- The procedure will continue to run until one of the transmitters hangs up the call at the base station. When the base station receives the modulated signal from the mobile device, it first demodulates the signal before retrieving the data.

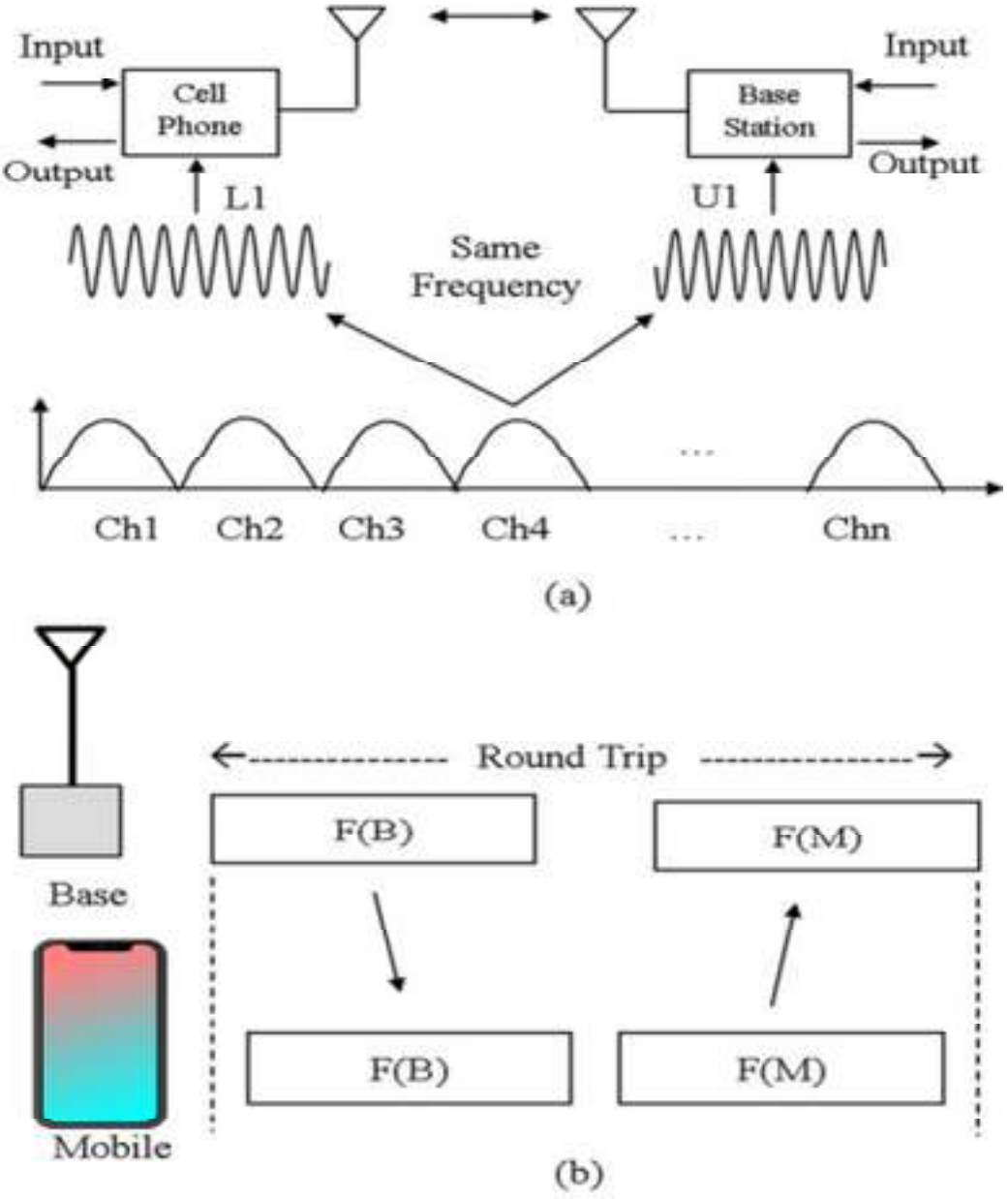
The diagram provides a high-level overview of how an FDMA radio operates when set to FDD mode. A call uses two carrier frequencies at the same time when it is being carried out in this mode of operation, one from the lower band and one from the higher band (for example, L1 U1). The radio in the mobile device operates at a lower frequency, while the radio in the base station operates at a higher frequency. Mobile devices often operate at lower frequencies since the rate at which a signal degrades is logarithmically dependent on the signal's transmission frequency. Because the transmit power of mobile phones is significantly less than that of base station radios, mobile phones are constrained to operate at lower frequencies than base station radios. The AMPS (Advanced Mobile Phone System) cellular communication system of the first generation (1G) utilized a multiple access technology known as FDMA (Frequency Division Multiple Access).

FDMA-TDD Technique

In FDMA-TDD, the uplink and the downlink share the same FDMA frequency so that they may communicate with one another simultaneously. The time required for transmission in both directions is typically on the range of milliseconds (ms). According to this strategy, the mobile device listens in whenever the base station broadcasts, and the base station listens in whenever the mobile device transmits. This is accomplished by placing the data into what is known as a "Frame," which is a collection of numerous time periods all grouped together. A data packet that contains synchronization bits, digital text, digital video, and digital audio is associated with each time slot (sync. bits). Frames are guaranteed to be perfectly synchronized with one another through the utilization of sync bits. The sample frame and the TDD transmission system are both depicted in the figure below.

According to the frame length, which is often expressed in milliseconds and serves as the basis for the calculation of the round-trip delay Td: (ms). The guard time (tg) and the propagation delay are both affected by the technology as well as the propagation distance (tp).The concept of an FDMA radio that is also capable of TDD operation. Both ends of the call make use of the same FDMA frequency throughout the duration of the call when utilizing this strategy. As can be seen in the accompanying photograph, the structure of the frame makes it feasible for this to occur. According to this strategy, the mobile device listens in whenever the base station broadcasts, and the base station listens in whenever the mobile device transmits. This makes efficient use of the available bandwidth due to the fact that the whole connection only makes use of a single carrier frequency.

The flow of traffic in both directions isn't even in cell phone communication technologies such as OFDMA and LTE (4G). When using the FDD approach, the quantity of data that is sent in either way can be dynamically altered on the fly. There is a technique to schedule things using dynamic control that enables high-speed data to be delivered over the downlink while low-speed data is sent over the uplink. This is possible since the downlink and uplink both use the same bandwidth. In TDD, the downlink is provided with an increased number of time slots that are used to transmit more data. TDD, or time division duplexing, is utilized in 4G wireless networks in the same manner as WiMAX and LTE are. The schematic of FDD-TDD with a single FDMA channel can be found down below.

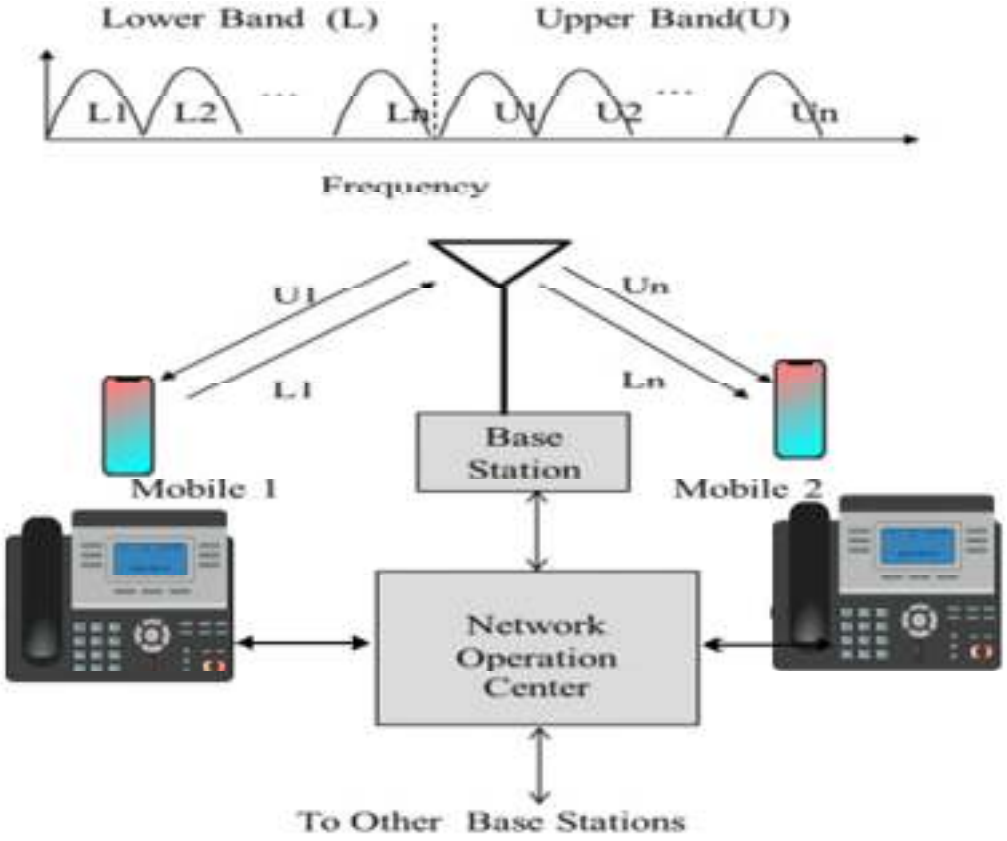


5.3 FDMA Cellular Telephony

A duplex or full-duplex communication technique underlying cellular communication. Duplex communication, often known as two-way communication, allows for simultaneous conversation between two parties. The cellular communication system of the first generation, often known as 1G, was created using the FDMA-FDD approach, and the figure that follows explains how the system operates.

Because of this, each mobile device is provided with a pair of channels, one from the lower band and the other from the higher band, so that it is able to send and receive information simultaneously. The responsibility for distributing channels lies with the network operating center (NOC). The NOC additionally has connections to both a landline and other cellular base stations in addition to these connections. It is clear from looking at the photo that several users can share the same base station. A guard band sits between the two frequencies that are associated with each user; one frequency is used for uploading, while the other frequency is used for downloading. The result is that there won't be any interference, despite the fact that both broadcasts are happening at the same time.

This approach is referred to as FDMA due to these factors. The technique known as FDD is utilized in the 1G Cellular FDMA-FDD communication system. This is the foundation upon which 1G mobile phone systems are built, such as GSM in Europe and AMPS (Advanced Mobile Phone System) in North America (Group Special Mobile). As a direct consequence of this, a brand new era of communication via mobile phones got underway.



Summary

- Multiple accesses may be implemented in a wide variety of various sorts of systems.
- Examining the similarities and differences between signals that operate on narrow and broad bands.
- Being knowledgeable with frequency division multiple access and the various applications that may be found for it.
- There is consideration being given to utilizing FDMA within the field of communications.

Keywords

CDMA - Code division multiple access

CDM - Code division multiplexing

FHSS - Frequency Hopping spread spectrum

LAN - Local Area Network

BPSK – Binary phase shift keying

DSSS - Direct sequence spread spectrum

UHF - Ultra high frequency

ADC - Analog to digital conversion

GSM - Global system for mobile communication

NOC – Network operating center

FSK – Frequency Shift Keying

BFSK – Binary Frequency Shift Keying

FDM - Frequency Division Multiplexing

FDMA/FDD – Frequency division multiple access/ frequency division duplexing

Self Assessment

1) Multiple access may be implemented in a wide variety of various sorts of systems.

A. Examining the similarities and differences between signals that operate on narrow and broad bands.

B. Being knowledgeable with frequency division multiple access and the various applications that may be found for it.

C. There is consideration being given to utilizing FDMA within the field of communications.

D. Conduct an analysis on the various protocols used for wireless multiple access.

2) In satellite communication the channels for telephone communication uses

A. TDM

B. FDM

C. FM

D. AM

3) The FDM and analog multiplexing technique is used for combining

A. Analog signals

B. Digital signals

C. Both analog and digital signals

D. None of the above

4) The power combiners operating at the maximum power efficiency are non-linear. These nonlinearities generate the IM frequency which phenomena is associated with

A. OFDMA

B. FDMA

C. TDMA

D. CDMA

5) What is the guard band ?

A. The spectrum acquired by the noise between the signal

B. The small unused bandwidth between the frequency between the channels that avoid interference

C. Bandwidth allotted to the signal

D. The channel spectrum

6) Which of the underlying transmits the large chunk of data over closely spaced data streams.

A. OFDM

B. ASK

C. DSSS
D. FSK

7) The cross talk might occur due to_____
A. Interception
B. Jamming
C. Jamming & Interception
D. Imperfect filtration

8) The FDMA channel carries _____ phone circuit at a time.
A. Ten
B. Two
C. One
D. Several

9) The bandwidth of FDMA channel is _____.
A. Wide
B. Narrow
C. Large
D. Zero

10) The symbol time in FDMA system is _____ and this inter symbol interference is_____.
A. Large, high
B. Small, low
C. Small, high
D. Large, low

11) Out of the following which preposition is not true for FDMA system when compared to the TDMA system?
A. Low complexity
B. Low cell site cost
C. Better RF filtering
D. Narrow bandwidth

12) During the call users can share same channel in FDMA.
A. True
B. False

13) Which one out of the following uses FDMA/FDD.
A. GSM
B. W-CDMA
C. Telephone
D. AMPS

14) Which technique divides all of the channels that are usable in two distinct bands .
A. CDMA

B. FDMA

C. FDD

D. TDMA

15) Which of the following is a undesired RF radiation?

A. Intermodulation frequency

B. Intermediate frequency

C. Instantaneous frequency

D. Instrumental frequency

16) The free channels in FDMA can be used by other users.

A. True

B. False

Answers for Self Assessment

l.	C	2.	D	3.	A	4.	B	5.	B
6.	A	7.	D	8.	C	9.	B	10.	D
11.	B	12.	B	13.	D	14.	C	15.	A
16.	A								

Review Questions

1. Write and explain the FDMA technology in detail.
2. Explain how the narrowband systems in detail.
3. Compare and contrast the functionality narrow band and wide band systems.
4. Explain the FDMA-FDD functionality in detail.
5. Elaborate the concept of FDMA-TDD in detail.
6. Explain how the FDMA is used in mobile telephony.

Further Readings

- Wireless communications & networks by William Stallings, Pearson
- Principles of wireless networks by Kaveh Pahlavan, Pearson
- Fundamentals of wireless networking by Ron price, Mcgraw hill education
- Wireless networks first-step by Jim Geier, cisco press

Web Links

- http://59.51.24.50:8000/wxwl/Wireless_Communications_&_Networking_Stallings_2nd.pdf

Unit 06: Multiple Access Technology

CONTENTS

Objectives

- Understanding the Time division multiple access.
- Analyze the code division multiple access.
- Understanding the difference among TDMA,CDMA and SDMA technology.
- Analyzing the code division multiple access in detail.

Introduction

Time division multiple access (TDMA), a digital transmission method, enables numerous users to use a single radio-frequency (RF) channel without interfering with one another. Each user is given a unique time slot inside each channel to accomplish this. It is accomplished with the use of technology. A single channel may carry three separate signals thanks to the digital transmission method known as TDMA. Time division multiple access (TDMA), the current cellular network standard, splits a single channel into six time slots, with each signal using two of those slots. This translates into the ability to make three times as many calls as with a modern mobile phone service (AMPS). There is a set amount of time allotted for each caller to leave their message.

The wireless sector began investigating the prospect of digitizing the analog network to expand it around the end of the 1980s. This research project was initiated in the late 1980s. The best technology for both current 800-MHz cellular markets and brand-new 1.9-GHz markets was determined by the Cellular Telecommunications Industry Association to be TDMA in 1989 as opposed to Motorola's frequency division multiple access (FDMA), which is now known as the narrowband analog mobile-phone service narrowband standard. The CTIA determined that it would be preferable to allow carriers make their own technology decisions in light of the escalating technological competition between Qualcomm and code division multiple access (CDMA) and the reality of the European GSM standard. The two primary RF spectrum division and competition technologies are TDMA and CDMA. Spread-spectrum technology called the Code Division Several Access (CDMA) system enables simultaneous use of multiple frequencies. Each digital packet sent by CDMA is encrypted using a key specific to that packet. A CDMA receiver will only function

with that key, and it will be able to locate and distinguish the accompanying signal. TDMA and its variants are currently the most widely used technology worldwide. This is so because it has been accepted by the North American Digital Cellular, the Japanese Digital Cellular (JDC), and the European Standard GSM (NADC). On the other hand, whether TDMA or CDMA is superior has been a hot topic of discussion in the wireless industry for the past few years. The TDMA system was designed to be flexible enough to be utilized everywhere, from a hand-held device in a city center office to a mobile user traveling quickly on the highway. Additionally, the system is capable of supporting a variety of end-user services, including phone, data, fax, short message services, and broadcast message transmission. With its adaptable air interface, TDMA offers excellent capacity and coverage, complete mobility support, and the potential to accommodate a variety of user demands.

6.1 The Advantage of TDMA Technique

The usage of digital technology is required for every method of multiple access. The transition to digital technology has made its way into the public phone infrastructure. For the purposes of transmission across the backbone, all analog calls are transformed to the digital format. There are several advantages to using digital transmission rather than analog transmission, including the following:

- It reduces the amount of bandwidth used and makes it simple to link devices that employ PCS (personal communication systems).
- It is difficult to figure out.
- It maintains great speech quality over long distances.
- On average, it can function with less power from the transmitter.
- It has a number of disadvantages.
- It enables the use of receivers and transmitters that are more compact and less expensive.
- It protects the confidentiality of your voice transmissions.

6.2 Functionality of TDMA Technology

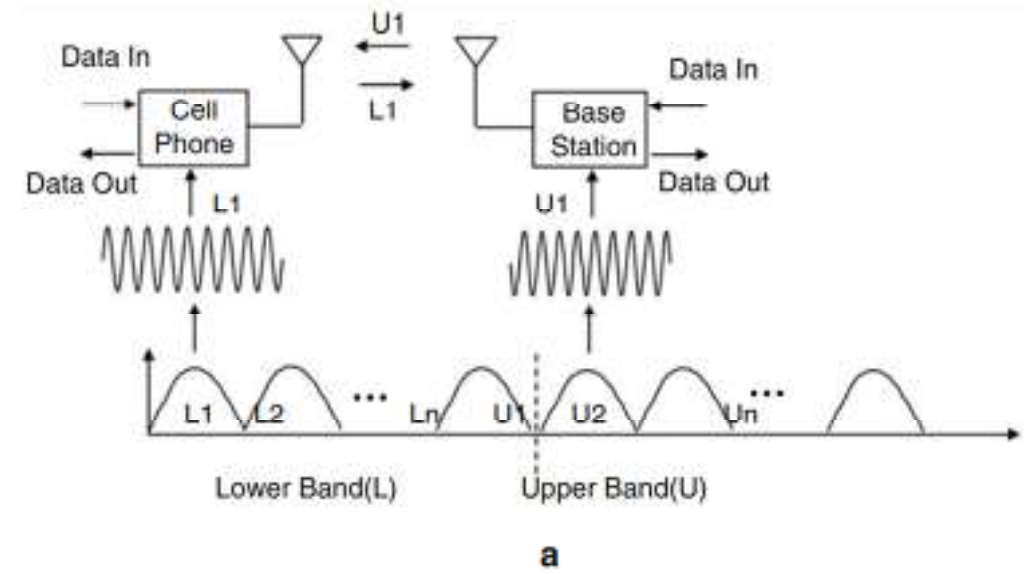
In order for time division multiple access (TDMA) to be effective, the audio stream must either be digitized or divided into a number of packets that are each millisecond long. After utilizing one frequency channel for a brief period of time, it then switches to utilizing another. The transmission of digital samples from a single transmitter allows it to simultaneously occupy various time slots and bands. In TDMA, there are three users sharing the same carrier frequency of 30 kHz. The European Digital Standard GSM and the Japanese Digital Standard Personal Digital Cellular Both Use TDMA as Their Access Mechanism TDMA is the access method that is utilized by both of these Digital Standards (PDC). Because it possesses a number of qualities that are necessary for a system to function well in an advanced cellular or PCS environment, TDMA was selected as the mode of operation for all of these standards. Today, TDMA is a method that is utilized commercially and is integrated into a variety of different systems. If they are segmented into digestible chunks, assigned time slots, and presented in timed bursts that are all in rhythm with one another, all four speeches can be aired on a single channel. The method is carried out once again following the conclusion of the conversation that took place during time slot number four. The implementations of time division multiple access (TDMA) in IS-54 and IS-136 immediately boosted the capacity of cellular frequencies. This was accomplished by dividing a 30-kHz channel into three time slots and permitting three separate users to make use of it at the same time. Because of the way things are set up right now, it is possible to raise the capacity by a factor of six. The capacity should eventually be close to 40 times that of analog technology after hierarchical cells, smart antennas, and adaptive channel allocation is implemented.

6.3 TDMA Technique

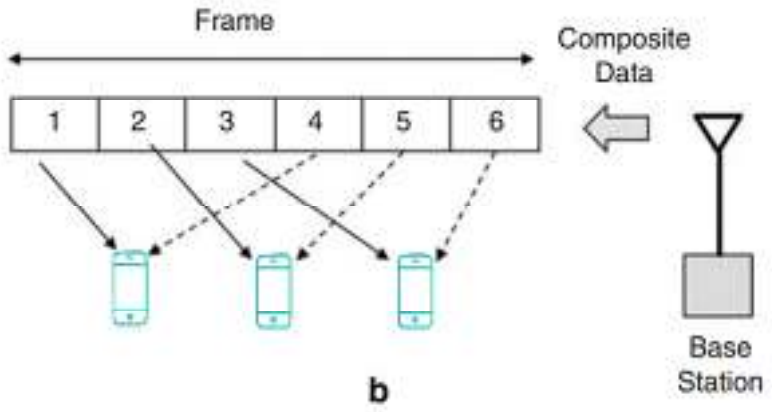
FDMA is further developed into TDMA, which stands for time division multiple access. In TDMA, each FDMA channel is utilized simultaneously by a number of users, one at a time. This is in contrast to FDMA, in which each user takes their turn. This approach makes use of two FDMA channels at the same time during a call; one is taken from the lower band, while the other is taken

from the upper band. Numerous mobile devices communicate with one another by using the lower band frequency. Additionally, the radio at the base station uses the same frequency for the upper band at the same time. The call continues to be active throughout both channels and is transferred between them both. The synchronization is carried out by making use of a one-of-a-kind frame structure, whereby a frame is understood to be a collection of time slots. The 2G Time Division Multiple Access (TDMA) frame structure provides each time period with a cell phone in North America. The time slots on the frame total to six, and each user is given control over two of them. When one mobile is utilizing a channel, this indicates that the other mobiles are not using that channel at the same time. Therefore, TDMA synchronization is required in order to both recover lost data and prevent collisions.

TDMA is superior to FDMA in a number of respects, including the fact that it is less susceptible to interference and noise, that it makes communication more secure, that it grants greater control and flexibility, and that it permits the use of an increased number of channels. Additionally, it enables the FDMA standard to continue to be implemented on the TDMA platform while maintaining the utilization of the same RF spectrum.



a



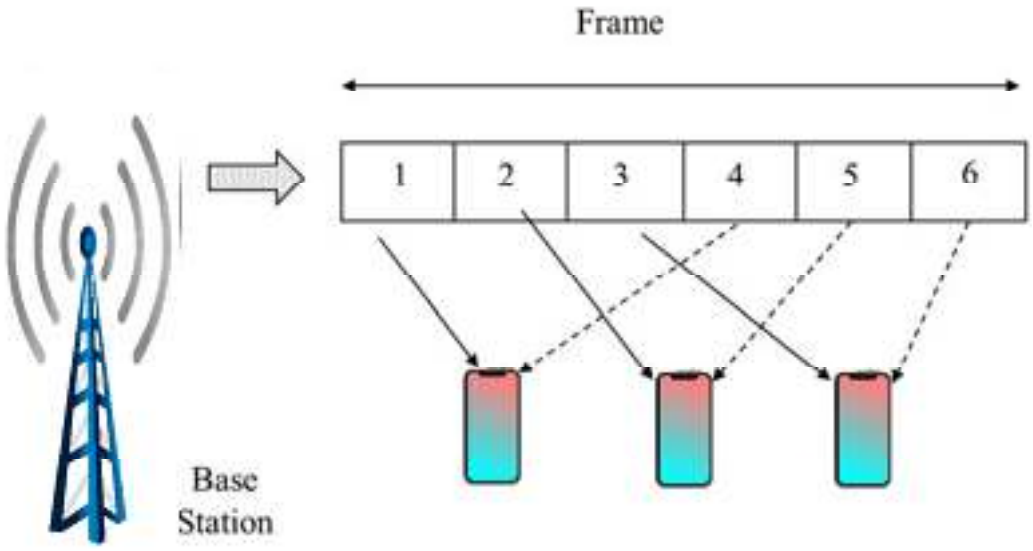
b

Frame Structure of TDMA

The TDMA air connection utilizes a frame structure that is 40 ms long and is partitioned into six time slots that are 6.667 ms each. There are 162 symbols in each of the six time slots, and there are 324 huge bit intervals in each of them (one symbol equals one and a half bits of information). a diagram showing the construction of a TDMA frame used for a forward connection (from base to mobile). In TDMA-3, the time slots are grouped into pairs, such as 1-4, 2-5, and 3-6, and a separate mobile is assigned to each pair. Because of the way that this system is set up, each of the three mobile devices may make independent use of the 30 kHz channel. A rate 1/2 convolutional encoding with interleaving is utilized in the TDMA-3 forward connection. Following the application of a /4 DQPSK modulation by the base station to the data bit stream traveling at 48.6

kbps, each mobile device receives data at a rate of 16.2 kbps. After the RF signal is received, it must first be demodulated and then decoded before the original data can be retrieved. The fact that this is a radio channel makes it difficult to obtain the data because of fading, noise, and interference. Therefore, it is possible that the information will become more inaccurate with time. Even if error control coding makes a significant effect, the carrier-to-interference ratio (also known as C/I) is still the factor that determines how well a system performs. The TDMA-3 reverse link performs actions that are diametrically opposed to those of the forward link.

If each frame takes 40 milliseconds to complete, then. Each user transmits data at a rate of 16.2 kbps, and the frame's six time slots are able to accommodate the data from a total of three users.



To find a suitable multiplexing structure We have three users and six time slots. Therefore we can assign two time slots/user:

- User-1: Time slot 1 and 4
- User-2: Time slot 2 and 5
- User-3: Time slot 3 and 6

6.4 The Advantages of TDMA

In addition to making transmissions more effective, Time Division Multiple Access (TDMA) provides numerous other advantages over standard mobile phone technology. To begin, it is simple to employ for both the transmission of data and the exchange of voice communications.

- You can transfer information at speeds ranging from 64 kbps all the way up to 120 Mbps using TDMA (expandable in multiples of 64 kbps). This enables operators to provide services such as personal communication, such as fax, voice band data, and short message services (SMS), in addition to programs that need a significant amount of bandwidth, such as multimedia and videoconferencing.
- TDMA users are separated in time, they won't be impacted by other simultaneous transmissions even if they occur simultaneously. Spread-spectrum techniques, on the other hand, are susceptible to interference from several users who are transmitting at the same time and are using the same frequency band. This makes spread-spectrum techniques less desirable.
- TDMA also allows for a longer battery life and greater speak time for the user because the phone only communicates between one-third and one-tenth of the time when a conversation is taking place.

- As cell sizes continue to decrease, TDMA deployments generate significant cost savings on base-station equipment, as well as space and maintenance costs.
- The only technology that can effectively employ hierarchical cell structures (HCSs) with pico, micro, and macro cells is called time division multiple access, or TDMA.
- Converting an analog system into a digital one may also be done in the most efficient and cost-effective manner with this method. Because HCSs allow for its coverage to be altered, the system may be tailored to various traffic and service requirements.
- Because of this technology, it is now feasible to get system capabilities that are greater than 40 times AMPS at a cost that is fair. Because it is compatible with FDMA analog systems, TDMA makes it feasible to utilize dual-mode phones with compatible service. This is because of TDMA's ability to function with FDMA analog systems.

The following are some of the perks that come along with having dual band 800/1900 MHz:

Customers on a TDMA 1,900 channel have the ability to switch to and from a TDMA 800 MHz channel and an analog AMPS channel using dual-mode, dual-band phones. Service providers can use the same switch for both 800 MHz and 1900 MHz services. Customers get the same apps and services regardless of which band they use. Because of this, it is now feasible for the networks operating at 800 MHz and 1900 MHz to function together without experiencing any difficulties.

6.5 The Disadvantages of TDMA

The fact that each user is assigned a specific time slot is one of the frustrating aspects of TDMA. On the other hand, users who travel between cells do not have a predetermined amount of time to complete their task. It is possible that a call will be terminated if all of the time slots in the subsequent cell have already been used. In the same manner, if a user is in a cell that has reached its capacity for time slots, they will not hear a dial tone when they try to make a call.

Another issue is that TDMA is susceptible to distortion caused by multipath interference. The path that a signal takes from a tower to a phone might take many distinct forms. It's possible that it collided with a few different objects along the way, which might have led to complications.

Allowing the system a predetermined length of time to complete its tasks is one solution to this problem. The system will be developed to be able to receive, handle, and process a signal within a predetermined length of time. After a predetermined amount of time has elapsed, the system will stop paying heed to the signal. The capacity of a system to deal with frequencies from several paths determines how sensitive it is. The interference caused by these multipath signals is difficult to manage even at a thousandth of a second. All cellular structures, regardless of whether they are made up of vast or tiny groups of cells, have their own unique challenges when it comes to propagation. Because it frequently occurs near the margins of the cell, which are locations where reflection and refraction have the potential to attenuate or eliminate a signal, multipath signal loss is particularly detrimental to macro cells.

6.6 CDMA Technology

Direct Sequence The information is sent via a method called Spread Spectrum using CDMA. CDMA can trace its roots all the way back to the 1940s, which was the decade in which this method of transmission was conceived for the first time. As the capabilities of electronics technology improved, they were increasingly put to use in covert military communications. This is due to the fact that the broadcasts appear to be noise, are challenging to comprehend without the appropriate codes, and are difficult to prevent.

There was a sea change in the way people communicated via mobile phones in the 1980s. During that time period, Qualcomm was engaged in research and development of DSSS transmissions. They started to consider utilizing this as the foundation for a cellular multiple access system, most commonly known as CDMA.

US network operators Nynex and Ameritech, along with Qualcomm, collaborated to develop the first experimental CDMA system so that the concept could be examined and evaluated in practice.

Later on, the team size increased as a result of Motorola and AT&T (now known as Lucent) combining their resources in order to expedite the development process.

Therefore, the beginning of the process of defining CDMA might begin in the year 1990. A standards group was established with the assistance of the Cellular Telecommunications Industry Association (CTIA) and the Telecommunications Industry Association (TIA) (TIA). After that, this committee came up with the first CDMA system standard, which they referred to as IS-95 and which was eventually made public as IS-95-A the next year.

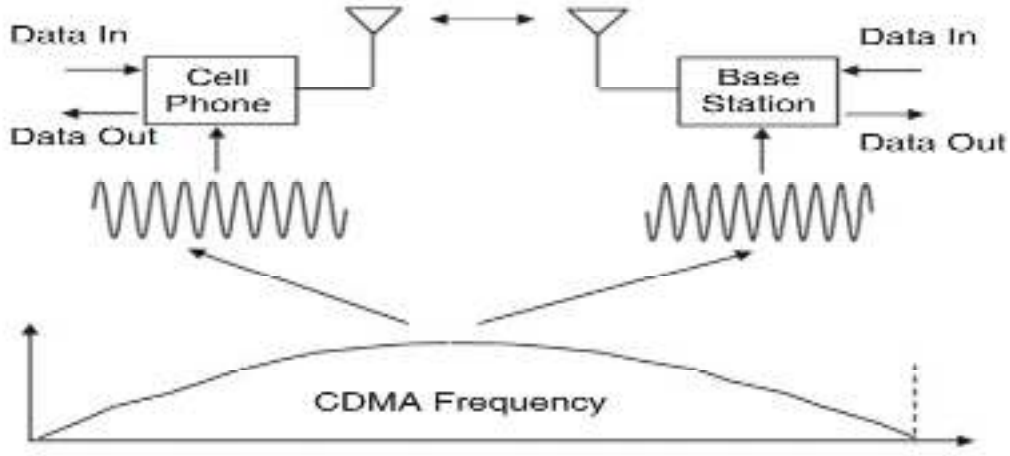
It is possible for more than one individual to use the same carrier frequency simultaneously while using CDMA (code division multiple access). In this scenario, several users share a single carrier frequency, and each user receives their own distinct orthogonal code to use with the shared frequency. Each user is able to communicate with every other user without any difficulties as a result of orthogonal coding. CDMA may also be referred to by its other term, spread spectrum technology. In order to accomplish this goal, every information bit is multiplied by an n-bit orthogonal code. In this method, the operation that corresponds to multiplication is referred to as an Exclusive OR (EXOR) operation. The letter W is produced when bit 0 of the binary code is added to the orthogonal code for four bits (01101), which produces the code.

0 EXOR (0101) = 0101

This is the orthogonal code reproduced due to exclusive OR operation. Moreover, the bit rate is also multiplied by a factor of four, thereby spreading the spectrum by a factor of four as well. Similarly, when the binary bit 1 is multiplied by the same orthogonal code, we obtain

1 EXOR (0101) = 1010

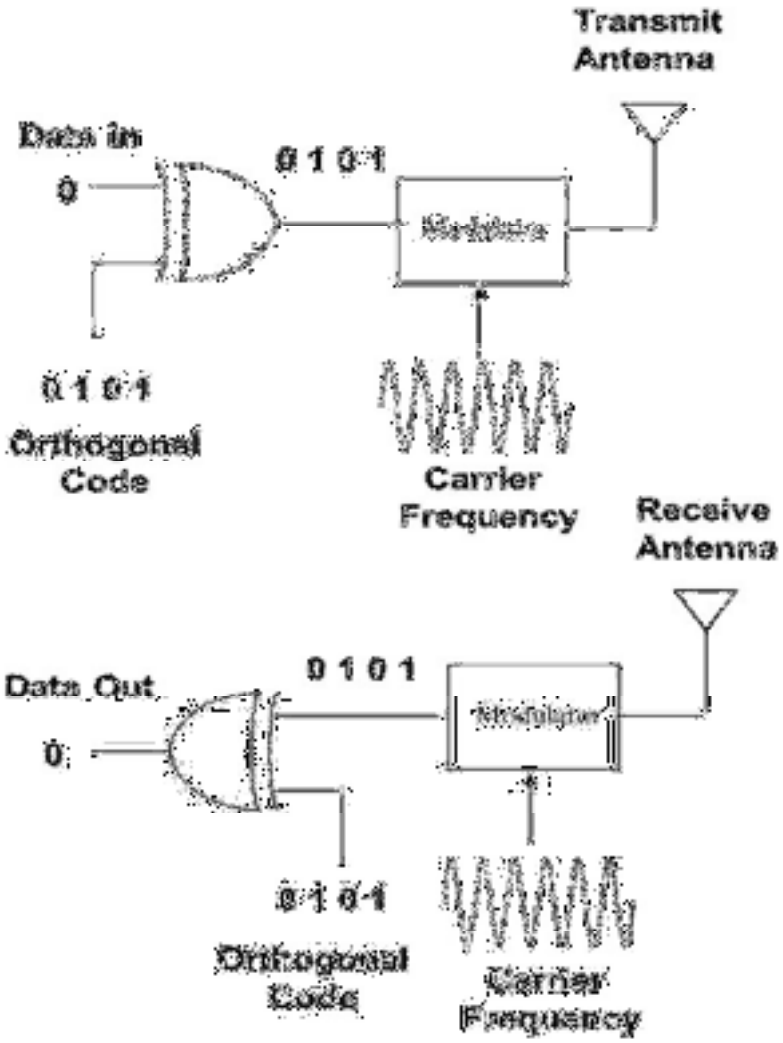
This is the inverse of the orthogonal code. This code is also known as antipodal code. The spectrum is also spread by a factor of four. Therefore, when an information bit is multiplied by an n-bit orthogonal code, the spectrum is spread by a factor of n, enabling multiple users to share the same spectrum at the same time. For this reason a large bandwidth is assigned for CDMA radio



Consider, for example, a 4-bit orthogonal code CDMA radio using the sequence 0101 as its code. When the binary bit 0 is multiplied by the four bits that make up the orthogonal code, the result is the orthogonal code, which serves as a substitute for the bit 0 of the information. At this point, the modulator alters the carrier frequency by applying the orthogonal code, and then the signal is sent through the antenna. The receiver is able to determine the orthogonal code 0101 after it has detected the modulated carrier frequency and demodulated it. Because the exclusive OR gate makes use of the same orthogonal coding, we are able to assert that

(0101) EXOR (0101) =0000

This demonstrates the initial binary value, which is 0 (also written as 0). It is possible to get at the antipodal code for bit 1 by multiplying the binary bit 1 by the same four-bit orthogonal code. This results in the value 1010. Now that the antipodal coding has been applied, the modulator will alter the carrier frequency before sending the signal out through the antenna. The signal is modulated, and the receiver may pick up on it.

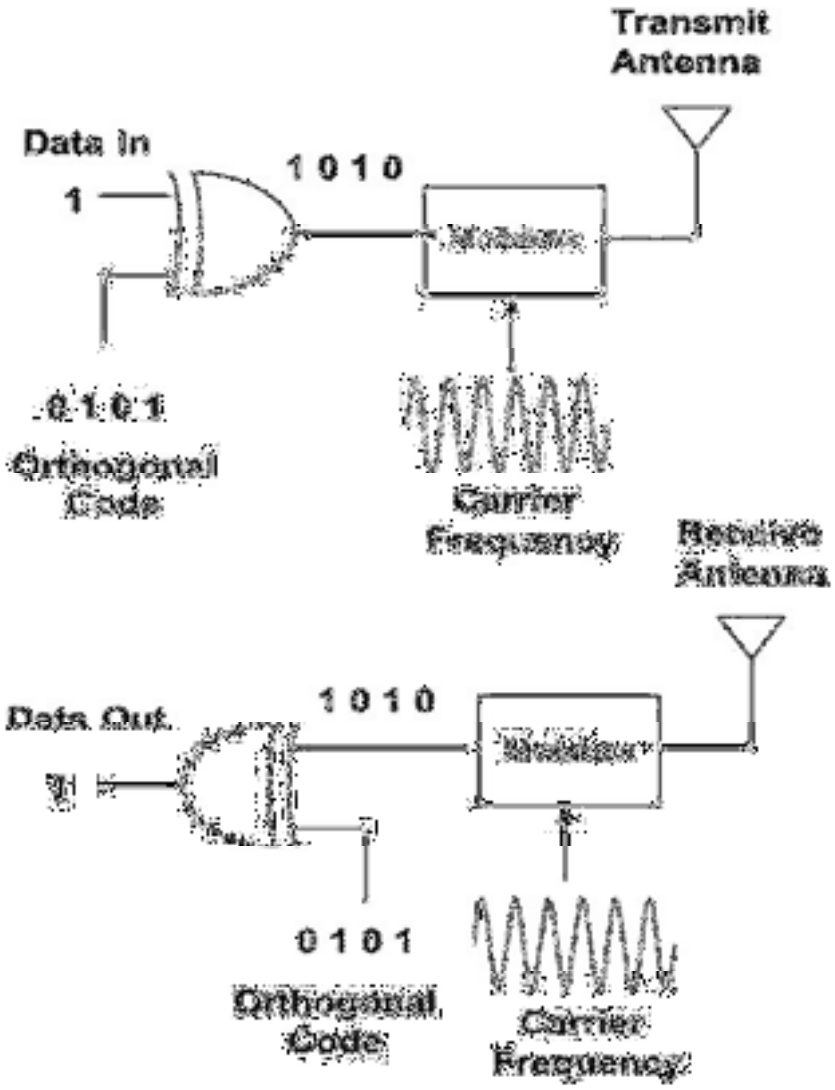


Transferring 0 bit

carrier frequency, demodulates, and recovers the antipodal code 1010. Since the exclusive OR gate also uses the same orthogonal code, we obtain

(0101) EXOR (1010) =1111

That means the first binary number is 0, or 0.0. Multiplying Bit 1 by the same four-bit orthogonal code yields the code 1010. The antenna receives the signal after the modulator modifies the carrier frequency using an antipodal coding. The modulation can be deciphered by the receiver.



Transferring 1 bit

6.7 The Main Features of CDMA Systems

- Users of the CDMA system have the ability to use either TDD or FDD while still sharing the same frequency.
- The capacity of CDMA has a somewhat flexible upper limit.
- As more individuals utilize the CDMA system, the performance of the system will deteriorate.
- When utilizing a CDMA system, the receiver end has difficulty determining whether the signal is close by or further away.
- If the signal is dispersed across a large enough range, multipath fading can be attenuated to some degree.
- CDMA is a technique that reduces the amount of interference.
- Increases in reuse rates have been seen.
- Utilizing a co-channel cell is CDMA. Making use of the spatial variety can assist make it feasible to have smooth handoffs.
- There is a great deal of information available on the channels. Because of this, the symbol duration is kept to a minimum, and the delay spread is maintained at a level that is lower than

the channel delay. The reception quality can be improved with a rake receiver by accumulating a copy of the required signal that was transmitted at a later time.

- A wireless network device will utilize the CDMA protocol in order to communicate. It is the most frequent strategy, and due to the fact that it can be employed in so many different situations, it is utilized worldwide.
- It is capable of supporting an unlimited number of users, in contrast to TDMA full form and other regular mobile phone equipment.
- Hard hand-offs are problematic for TDMA as well as FDMA networks. In order for CDMA systems to function properly, the hard handoff must be replaced with the "soft handoff," which is an approach that makes logical sense.
- The number of customers that can be handled by CDMA is an excessive amount higher in comparison to that of TDMA or FDMA, which are both plagued with issues.
- CDMA ensures the security of its signal transmissions by using a one-of-a-kind code to encrypt each user's data transfer.

Differentiating Between GSM and CDMA Technology

When trying to move their phones from one cellular network provider to another, the vast majority of consumers become entangled in the argument between the GSM and the CDMA. Because certain carriers' phones can only be made to function on their radio network, they are not compatible with the mobile phone technology used by other networks. Several years ago, incidents like these occurred far more often. Recently, firms that specialize in the production of electronics have begun manufacturing phones that are compatible with both CDMA and GSM networks.

Several-access technologies, such as GSM and CDMA, enable multiple users to connect to the same radio channel at the same time and engage in simultaneous conversation. Each call in CDMA cellular systems is given its own unique code to utilize for encoding the data. After then, they sent all of the calls at the same time. At the other end, receivers take the combined signal and split it up into individual calls before distributing them to the appropriate parties. Every call is converted into digital data using GSM, and then the information is reassembled at a predetermined time for the person who is on the other end of the connection. This takes place on a channel that is shared with others.

Who are the service providers for CDMA? Which of these are GSM standards? GSM is currently utilized in over 200 different nations. Verizon and U.S. Cellular are two of the most prominent carriers in the United States that make use of CDMA technology. T-Mobile and AT&T are both examples of GSM service providers in the United States.

Performance Comparison of GSM and CDMA

In contrast to CDMA networks, GSM networks are capable of simultaneously transmitting voice and data communications. CDMA networks are unable to perform this task. However, this is not the primary reason why individuals favor GSM. A regulation from 1987 mandated the adoption of GSM technology throughout Europe, which served as a significant driving force. Another aspect to consider is that GSM was produced by a consortium of firms working together, whereas the majority of CDMA products were manufactured by Qualcomm. This resulted in GSM phones having lower production and operating costs.

Only two- and three-generation connections can use the CDMA and GSM protocols respectively. In 2010, when the transition to 4G networks started in earnest, carriers immediately embraced Long-Term Evolution (LTE), which is the global standard. As a consequence of this, the distinction between CDMA and GSM is losing some of its significance as GSM-powered devices grow more widespread and CDMA phones become rarer. However, the 2G and 3G networks are still utilized as backups in locations where the signals for 4G LTE are not strong as of yet.

Parameters	GSM	CDMA
SIM	Required & Removable	Non-Removable & integrated
Voice Quality	High & Good	Poor Quality in congested network
Security	Less secure	More Secure
Spread Spectrum	Applicable	Not applicable
System capacity	Less	3 to 4 time higher than GSM
Frequency reuse	Maximum 3	Maximum 1
Handoff	Hand Handoff	Soft Handoff

Advantages of CDMA technology

- Because it offers a multitude of advantages, CDMA is the most advantageous technology for 3G mobile phones.
- Capacity and security are both improved as a result of this. The ability of CDMA to support ever-increasing network capacity is one of the most important aspects of this line of reasoning. The technique known as code division multiple access, or CDMA, separates the transmission of voice and data packets by making use of a broad variety of frequencies and codes that are exchanged via codes. Through the use of CDMA, a terminal is able to easily communicate with two base stations at the same time. This is due to the fact that CDMA makes a large amount of information space available, which is gradually becoming more standardized and is appealing to the 3G speed of mobile internet use. The previous connection has been severed, and the new connection has been established in its stead. Handoffs or modifications made from one base station to another base station are made more dependable as a result of this. Every aspect of CDMA has received further attention, which has made it feasible to make the numerous adjustments that are necessary for mobile communications networks.
- Signal congestion on the subscriber's phone is caused by channel pollution, which prevents any one cell site from assuming control of the network. If things continue to grow worse, the sound quality will continue to deteriorate. CDMA does not have the capability to travel worldwide, in contrast to GSM. CDMA does not make it simple to move to or upgrade to another handset since the information about the network service is integrated into the phone itself. This is in contrast to GSM, which allows users to do this by inserting a SIM card into their phone. As of right now, it is only compatible with mobile service providers that utilize the GSM standard, which is why it only provides a limited selection of devices.

6.8 Space Division Multiple Access

Spatial separation Multiple access is a method for making use of the same group of cellular phone frequencies within the confines of a certain service region. In mobile communication systems, it is a common component. If there is sufficient space between two cells or tiny regions, then they are able to make use of the same frequencies (called the reuse distance). By concentrating the signal into a series of tiny beams, SDMA improves both the capacity of the system and the quality of its transmissions. By utilizing smart antennas with beams that aim in the general direction of the mobile station, SDMA makes it possible for more than one customer to get service in the same

geographic region. Mobile stations that are located outside the range of these focused beams almost never experience interference from other mobile stations that use the same radio frequency as them but are connected to a different base station. This is because the interference comes from other mobile stations that use the same radio frequency as them. There is a possibility that the radio frequency will have a greater base station range because of the way the beams are curved. As a result of this component of SDMA, base stations are able to disperse less energy while simultaneously covering a wider region with radio waves. Because of the beam's low width, it is also able to achieve more gain and exhibit superior clarity.

In conventional designs for mobile phone networks, the base station transmits radio signals without being aware of the location of any mobile stations within the cell. When using SDMA technology, the manner in which radio signals are sent varies according to the location of the mobile station. The SDMA architecture prevents vital network resources from being utilized more than once in locations where mobile devices are not currently being used at this time.

The primary advantage of SDMA is that it permits several simultaneous transmissions on the same frequency. When constructing the network, it is important to bear in mind the reuse distance so that interference is reduced to a minimum. This is true even if many mobile stations use the same frequencies. Mobile wireless devices benefit from increased bandwidth and range, as well as improved spectral efficiency, thanks to a cutting-edge technology that has multiple antennas. Because they are unable to pinpoint the location of the mobile device, conventional cell phone base stations disperse power in all directions. This not only results in power being wasted, but it also disrupts the function of neighboring cells and makes it more difficult to differentiate between weaker incoming signals and noise and interference. By modifying the base station's radiation pattern with the help of technology known as smart antennas, it is possible to optimize the transmission and reception capabilities of each user's device. This is accomplished by determining the location of mobile devices in space using smart antenna technology. The base station is able to successfully steer a beam or spot of radio frequency (RF) power toward or away from each user by rapidly altering the phase of signals coming from many antennas. In contrast to MIMO, single-input multiple-output (SIMO) only requires one antenna per client device. This might result in cost savings for equipment at client locations (CPE). WiMAX and LTE on mobile devices are both ideal candidates for the SDMA-based private wireless broadband networks. See also smart antenna in this regard.

Summary

- In this Unit we have discussed the concepts of spread spectrum modulation.
- The unit discussed about the TDMA , CDMA and SDMA.
- The basic operation of TDMA and CDMA sending and receiving operations were discussed.
- The advantages and disadvantages of CDMA and TDMA were discussed.

Keywords

CDMA - Code division multiple access

CDM - Code division multiplexing

FHSS - Frequency Hopping spread spectrum

LAN - Local Area Network

TDMA - Time division multiple access

SDMA – Space division multiple access

DSSS - Direct sequence spread spectrum

UHF - Ultra high frequency

ADC - Analog to digital conversion

EVDO - Evolution-Data Optimized Revision

GSM - Global system for mobile communication

Self Assessment

1. The earliest versions of TDMA effectively analog wireless carrying capacity.

A. doubled

B. tripled

C. quadrupled

D. None of the above

2. FDMA allocated _ users per channel.

A. 1

B. 3

C. 6

D. 10

3. The basic cost for a TDMA base station is____.

A. $300,000

B. $150,000

C. $100,000

D. $80,000

4. Allows handoff to/from an analog AMPS channel.

A. CDMA

B. TDMA

C. SDMA

D. FDMA

5. What technology has the longer handset battery life?

A. TDMA

B. CDMA

C. SDMA

D. FDMA

6. _____enable users access to PCS–like services

A. TDMA

B. CDMA

C. both

D. neither

7. _____Technology depends on sending a unique key to a receiver.

A. TDMA

B. CDMA

C. SDMA

D. FDMA

8. Greater security is offered by_____.

A. Spread spectrum
B. Narrow spectrum
C. Broad spectrum
D. Dispersed spectrum

9. The most widely deployed digital technology at the present time is ____.
A. TDMA
B. CDMA
C. FDMA
D. SDMA

10. ETDMA allocates bandwidth_____.
A. Statically
B. Dynamically
C. Extensively
D. Proficiently

11. The spread spectrum is used to transmit which type of following data
A. Analog data
B. Digital data
C. Both Analog and Digital
D. None of the mentioned

12. Spread spectrum is a technique used for _____.
A. Encoding
B. Decoding
C. Both Encoding and decoding
D. None of the above

13. Due to spread spectrum it becomes difficult to do _____ of the signals.
A. Interception
B. Jamming
C. Jamming & Interception
D. None of the mentioned

14. Spread spectrum is immune from.
A. Noise
B. Multi-path distortion
C. Noise & Multi-path distortion
D. None of the above

15. For final FHSS signal which filter is used

A. Low pass filter

B. High pass filter

C. Band stop filter

D. Band pass filter

16. The transmitter of frequency hopping system is fed with encoding scheme such as

A. Frequency shift keying

B. Binary phase shift keying

C. Frequency & Binary phase shift keying

D. None of the mentioned

Answers for Self Assessment

1.	B	2.	A	3.	D	4.	B	5.	A
6.	C	7.	B	8.	A	9.	A	10.	B
11.	C	12.	A	13.	C	14.	C	15.	D
16.	C								

Further Readings

- Wireless communications & networks by William Stallings, Pearson
- Principles of wireless networks by Kaveh Pahlavan, Pearson
- Fundamentals of wireless networking by Ron price, McGraw hill education
- Wireless networks first-step by Jim Geier, cisco press

Web Links

- http://59.51.24.50:8000/wxwl/Wireless_Communications_&_Networking_Stallings_2nd.pdf

Unit 07: Mobile Adaptive Computing

CONTENTS

Objectives

- Understanding the Mobile computing concepts.
- Analyzing the transparency concepts in mobile computing.
- Understand the concept of application understanding.
- Analyze the concepts of data dissemination and delivery.

Introduction

How does computing while traveling actually work? What are some of the various facets that it entails? Computing systems that are mobile are essentially distributed systems that communicate with other computers through the usage of a network. Wireless communication is required for mobile devices that are able to communicate with one another. There are a wide variety of wireless networks available today, as well as a large number of books that have been written specifically for mobile communication. This book focuses solely on the most fundamental aspects of mobile communication and nothing more. However, in this chapter, we'll discuss why it's reasonable to communicate via mobile devices. What are the key distinctions between mobile computing and mobile communication? People need to be able to communicate with one another in order for distributed computing to be successful. There are great deals of mobile computing jobs that are impossible to complete without mobile connectivity. However, this is not the conclusion of the matter. Mobile communication does not always give a solution.

To be able to send and receive signals or packets is not the only challenge that must be overcome; there are many more complex issues that must be resolved. The innovative ways in which we are able to communicate through our mobile devices are the aspect of mobile computing that most piques our attention. What other applications may there be for this? Consider the software that is currently in use. A significant number of these programs are not very good at adapting to our changing requirements. Take for instance that we are looking for somewhere to have lunch online and that we are interested in going to an Italian restaurant. When we put "Italian restaurant" into a search engine like Google, what kinds of results might we expect to see? We frequently get a great deal of information, much of which is irrelevant to our work. The identity of the user or the location from which they are doing a search is irrelevant to modern search engines. People looking for

Italian food might search for restaurants in Tempe or in the area around Arizona State University. When you pose a question, you are at liberty to provide as much specific information as you see fit. But wouldn't it be great if the applications could tell where you were or, more broadly, what was going on around you and utilize that knowledge to make up the results of the search engine based on what they found? The fact that these programs are aware of what is going on around them will unquestionably assist us in getting more done.

7.1 Mobile Adaptive Computing

Let's consider a different use, like watching movies on the internet, for example. Let's say you're driving some where and you want to watch a movie. There is a significant difference between wired communication and wireless communication. When you are connected to a wire, both you and the application you are using have access to a certain amount of bandwidth. After the beginning of the program and the beginning of the movie, you will be able to view it with decent service (QoS). (Given that it is now possible to watch content online, this is becoming less accurate.) Despite this, it is anticipated that this will take place very soon.) However, in wireless communication, the bandwidth is often split among a number of users in a manner that dynamically shifts depending on the circumstances. This indicates that there is no available bandwidth that is specifically designated for usage. The amount of wireless bandwidth that is really accessible varies, despite the fact that your application might be able to reserve a specific amount of that bandwidth. This is because of the way that wireless technology operates. There are adjustments being made on both the short and the long term. The question that has to be answered is how the app ought to react to these changes. It's possible that the program will always react in the same way, regardless of what you observe. The alternative approach to this problem is to adapt your behavior to the kind of film you are now viewing. Take, for instance, the scenario in which you are watching a movie that features a significant amount of action. By converting the video from full color to black and white or decreasing the quality, the program may make more efficient use of the available bandwidth. If, on the other hand, you are now viewing an interview with Bill Gates, the show may simply switch to audio streaming at that point. Regarding this topic, there are a few essential points that should be mentioned. These choices are made on the basis on the contents of the video, and the client as well as the server could be engaged in the process (the client needs to inform the server that it no longer wants the video frames, only the audio). We are going to investigate the several ways in which the architecture of computer (software) systems may be altered to make them more mobile. As we will see, a significant number of the alterations are performed in order to facilitate an easier adaptation of systems to shifting environmental and system parameters, such as the availability of resources and the location of the system. Getting information to people whenever and wherever they are is the primary focus of mobile computing, which is a larger phrase for computing everywhere.

Understanding ways to circumvent the constraints imposed by mobile devices is another component of mobile computing. Personal digital assistants, sometimes known as PDAs, and laptop computers, for instance, both feature displays that are very tiny and run on battery power. One of the most pressing issues is figuring out how to conduct computing in a manner that is more efficient use of energy. Although Moore's law holds true for processing speeds, it is not anticipated that the capacity of batteries will continue to double at a constant pace. This is because the technology behind batteries is not advancing as rapidly as the technology behind CPUs. When designing systems for solitary computers or distributed networks, one does not have to be concerned with these kind of issues. In distributed systems, it is possible that you may need to troubleshoot issues such as a malfunctioning server or a severed network link. On the other side, there is almost never an issue with energy. When it comes to mobile systems, energy is treated as a resource in the same way that processing power and memory are. Therefore, in the same manner that conventional operating systems are responsible for managing processes and memory, we now need to devise methods for managing the resources associated with energy. When it comes to mobile computing, it's possible that various computers will have varying levels of capability. In order to accommodate the fact that separate devices have their own unique characteristics, it is necessary to have an underlying software entity for each activity that includes more than one device. The term "middleware layer" refers to this particular piece of software. The ability of a wired device and a mobile device to communicate with one another may also be enabled by the presence of a middleware layer. It is possible that mobile clients will become interested in learning about new services as they travel from one administrative domain to another. What about protection or confidentiality? It is fairly simple to eavesdrop on wireless conversations since those conversations take place over a "open" connection. It may appear as though standard cryptographic

procedures may be utilized to ensure the safety of wireless communication. The most significant obstacle, however, is that these risk-free strategies were developed for wired networks, which means that they involve a significant amount of processing and communication. In an effort to reduce these expenses, security procedures have been designed that are extremely simple to circumvent. In the next chapters, we will investigate the many security protocols that are utilized by mobile networks.

7.2 Adaptability—The Key To Mobile Computing

The process of evolution has led to the rise of humans to the top of the food chain. We have unquestionably accomplished this goal by being able to respond effectively and rapidly across a wide variety of contexts. Because of our ability to adapt, you may find us in every environment, from the ice caps of the Arctic to the sands of the Sahara. How do individuals adjust their lives to account for the fact that they live in such a variety of locations? Is it possible that any of these strategies may be implemented on the computers that we have today? Those of us who make frequent use of computers frequently wish that they were more robust and better equipped to adapt to our various requirements and circumstances. There is a wide variety of ways in which problems might arise with computer systems and applications. The worst-case scenario is when there is no discernible cause for their failure to make it. When you install new software, another program that you think has nothing to do with the new one suddenly stops functioning. Aside from that, there are occasions when we merely want our computers to behave appropriately and proactively depending on how we have previously used them. Work has to be done on systems in order to make them resilient and adaptable. We have maintained our position at the absolute pinnacle of the food chain for an extremely extended period of time. The computer that we use today is not even close to being 100 years old, yet it has been around for quite some time.

The purpose of mobile computing is to make it possible to continue working on your computer and chatting with other people even when you are moving around. This objective may be accomplished through the use of mobile devices. In order to make this a reality, amongst other things, there is a need for advancements to be made in the areas of security, privacy, resource allocation, pricing, and billing. Any answer to an issue that arises with mobile computing needs to be flexible enough to accommodate the rapid shifts in computing and communication environments that might occur. When it comes to mobile computing, one of the more recent ways to evaluate performance is based on how effectively a system can accommodate shifts in the surrounding computing environment while maintaining the continuity of its activities. Consider what would take place if, while a video streaming software was running on your computer, you moved from the service area of one access point to that of a different access point. Now, the video stream's packets should be automatically transmitted to the new access point so that the video stream may be received without interruptions and without a reduction in the quality of the stream's image. This may mean that the mobile client obtains a new IP address in the IP network of the new access point and then informs the server about the new address so that the server can send the packets to the new address. This occurs in a network that uses Internet Protocol (IP), which stands for Internet Protocol network. Dealing with this issue can be done in a variety of more effective methods. The most important thing to understand about this situation is that the underlying system needs to carry out a series of predetermined actions in order to keep the connection active and, in this particular instance, to prevent the video stream from pausing while you view it. In essence, the system needs to be able to adjust to various shifts in the surrounding environment, including the configuration of the network as well as the resources and services that are at a user's disposal for communication and processing. Is that, on the other hand, sufficient? In particular, the prior strategy for adaptation did not take into consideration either the requirements of the applications or the role that they played in the process of adaptation. Is this method of adapting, which does not affect the way in which apps function, sufficient to meet the aims of mobile computing?

7.3 Transparency

The capacity of a system to conceal from users some aspects of how it functions internally is referred to as its level of transparency. The development of computer systems that are capable of varying degrees of transparency has taken up a significant amount of time and effort in the field of distributed computing research. The following are some illustrations of this phenomenon:

- The capacity of a system to hide differences in the presentation of data on various computers and the path to take in order to access a certain resource is referred to as access transparency.
- The capacity of a system to conceal the location of a resource is referred to as location transparency. Name transparency, which guarantees that the name of a resource does not reveal its precise location, is connected to location transparency through a user's mobility. Location transparency is also tied to the concept of name transparency (which ensures that no matter which machine a user is logged onto, she should be able to access resources with the same name).
- The capacity of a system to conceal the breakdown of a component and its subsequent recovery is referred to as failure transparency.

It is possible to view mobile computing systems as a form of distributed system, and attempts may be made to establish "mobility transparency," which would incorporate the many types of transparency that we have already discussed. This would, in essence, be in favor of flexibility that is not dependent on the application. But is this a goal that can be achieved, or even one that should be desired, while developing mobile computing systems and software? Let's take a more in-depth look at the components that make up the mobile computing environment and what each of those components represents in this sense.

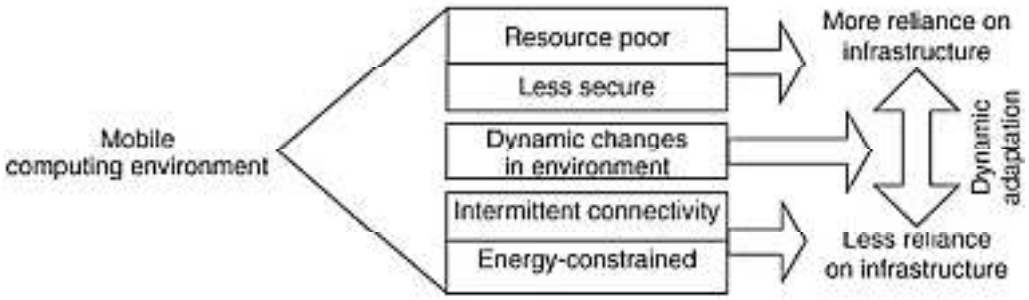
7.4 Issues in mobile computing environments

The limitations of a standard desktop workstation or PC-based distributed computing system are distinct from those of a mobile computing environment (MCE), which has its own unique characteristics. Among all of these, the following ones stand out the most:

- It is possible that portable computers will have less power than their equivalents that are permanently installed. According to Moore's law, which states that hardware technology is always growing better and better, it is nearly guaranteed that a laptop that is purchased today will be more powerful than a desktop computer that was purchased a year or even a few months ago. However, portable computers require a source of power, and battery packs are frequently utilized in this capacity.
- Batteries can only store a certain amount of energy, therefore they either need to be replaced or charged often to maintain their capacity. The first choice will cost you more money, while the second choice will cost you less but will make it more difficult to move around because the computer will need to be plugged in order to be charged. Because of this, the hardware and software that goes into portable computers are designed to consume less energy and have a longer run time when powered by their batteries. For instance, central processing units (CPUs) in mobile computers are designed to consume less energy, which results in a slower rate of calculation for various things.
- Mobile gadgets are less trustworthy and secure. Because their owners bring them with them everywhere they go, the risk that they may be misplaced or stolen is significantly increased. It is possible for there to be a large amount of variation in both the performance and reliability of a mobile connection with regard to bandwidth and latency. They are also more likely to be used in a harsh or disrespectful way, such as when a youngster tosses his father's PDA during a rage tantrum. This is an example of how they are more likely to be used in this manner. Disconnections are common occurrences, whether they are deliberate or unintentional. Both the time and the location of a user's connection may have a significant impact on the bandwidth available to them.

As a result of this, both the quality and the availability of the resources are subject to continuous change. It is essential to reevaluate the development process for mobile apps and systems in light of the characteristics of a mobile computing environment that have been discussed above. More

systems should be designed to rely on fixed infrastructure rather than mobile devices because there aren't sufficient resources and mobile devices aren't as reliable as they once were. However, the fact that there is a possibility of disconnections and poor connections demonstrates that systems shouldn't depend too heavily on the fixed infrastructure. Additionally, the status of mobile devices shifts with time because of the fact that they are transported from location to location (or even if they are not). The manner in which mobile devices perform their functions ought to be modified so that, according to the circumstances, they can depend more or less on fixed infrastructure. The picture that follows illustrates how essential it is to make impromptu adjustments when working in a mobile computing environment.



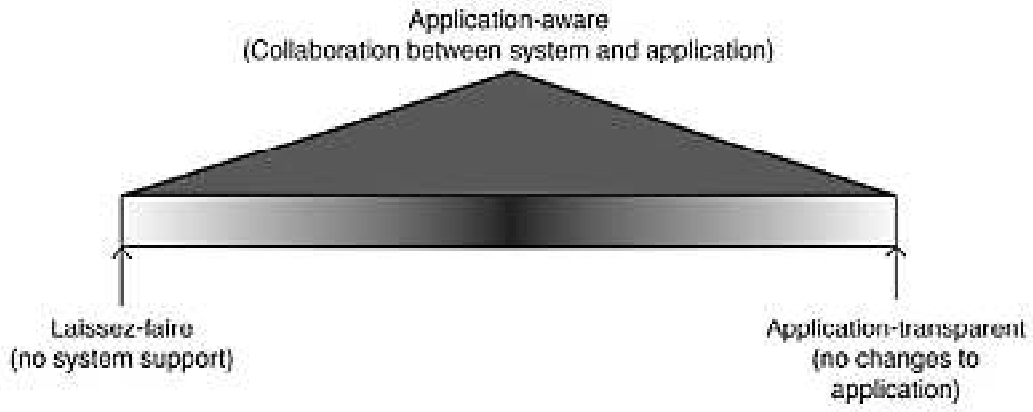
7.5 Application-Aware Adaptation

Which of the following should be responsible for adaptation: the system, the app, or both? The two most extreme approaches to the design of adaptable systems are application-transparent design, in which the system does all of the adaptation, and laissez-faire design, in which the system does nothing to help. Both of these approaches have their place in the design of adaptable systems. Because it places an excessive amount of responsibility on the person developing the application, the strategy of "let's do nothing" is plainly a poor choice. The sorts of adjustments that can be performed are not constrained in any way by the assistance provided by the underlying system. The following illustration demonstrates, however, that the tactic of making application instructions as explicit as possible is not sufficient on its own. Consider two distinct television shows that make use of several forms of media. In one of them, you participate in a video conference by using your phone. In the other, you see a live video broadcast on your phone that is coming from a server located in another location. Consider what would come up next in this scenario. The first scenario involves moving from a location in which your software is able to operate because there is sufficient bandwidth to a location in which there is insufficient bandwidth for it to execute. Your laptop will have a significantly shorter amount of time before its battery dies in the second. In both scenarios, there is a shift in the total amount of a resource. In each scenario, what are you hoping to accomplish with your computer system or application?

It's possible that the functionality of the system or application won't change, regardless of whether or not the program is transparent to the application (user). However, the correct response could be different depending on the kind of program that is now being executed. For instance, a system that does not adapt may be unable to take any action in the first scenario, allowing the audio and visual quality to deteriorate unchecked. In the second scenario, the software may only issue a caution to the user without providing any direction about how they should proceed with the problem. In a system that is adaptable, there are a variety of possible behaviors that it might exhibit. For instance, the system could attempt to perform anything in either or both of these scenarios. However, the system does not take into account the type of program that is running when it makes its adjustments. In the first scenario, the system could make an attempt to modify itself by requesting that the server or other peers begin delivering video of a lower quality, which consumes less bandwidth. In the second scenario, the system could make an effort to reduce its overall energy consumption by dimming the screen's lighting (besides warning the user of the lower battery power level). You might alternatively make use of an approach that is far more adaptable and in which the system communicates with the user or the application in order to determine how to adjust.

The application-transparent method has the system behind it do all of the adaption work instead of the application. On the other hand, under the strategy known as application-aware, the application collaborates with the software that runs on the system. The system provides information on the availability of the resources that may be utilized at this location. The software will make use of this

information to determine how to adapt in response to the quantity of resources that are now accessible. Each app offers a number of different ways to make adjustments.



7.6 Mobility Management

Mobility management is one of the most essential components of a GSM or UMTS network, and it is primarily responsible for ensuring that mobile phones are able to function properly. Mobility management makes an effort to locate subscribers in order to provide them with the ability to receive phone calls, SMS messages, and other services on their mobile devices. bringing the method of discovering a location up to date Both GSM and UMTS are types of radio networks that are constructed from a variety of cells, also known as base stations. Each base station extends across a sliver of land that is a component of a bigger geographic area that is assigned its own one-of-a-kind number. A cellular network is able to cover a significantly broader area when all of these base stations' radio signals are combined and broadcast simultaneously. A location area or routing area is the collective name for a collection of base stations. A mobile device can inform the cellular network of any changes to its position by using a mechanism known as the location update method. The use of mobile devices is required in order to look for area codes. When a mobile device discovers that the area code for its current location has changed since the time of its most recent update, it sends a location update request to the network along with information about its current location and its Temporary Mobile Subscriber Identity so that another update can be performed (TMSI). There are a few different channels via which a mobile device can share its most recent location information with the network. It is possible for the network to request an IMSI attach or IMSI detach location update whenever a mobile device is switched on or off. In addition, every mobile device has to report its position by refreshing its GPS data at regular intervals according to a schedule that has been previously established. A random location update is required whenever a mobile device travels when it is not currently engaged in a phone conversation. At addition, this is necessary for a stationary mobile phone that may switch to receiving service from a cell in a different location. This is because there is a gradual decrease in the strength of the signal. Therefore, a subscriber is provided with a stable network connection, is able to be reached through phone, and is free to roam around anyplace within the coverage area.

When a subscriber is paged to deliver a call or SMS but doesn't answer, they are marked as absent in both the MSC/VLR and the Home Location Register (HLR). This occurs when the subscriber is marked as absent in the Mobile Switching Center/Visitor Location Register (MSC/VLR) (Mobile not reachable flag MNRF is set). The HLR will be updated the next time the mobile updates its position, and the flag that indicates that the mobile is inaccessible will be removed at that time.

TMSI

The majority of the time, the Temporary Mobile Subscriber Identity is the piece of information that is transferred from the phone to the network (TMSI). The VLR arbitrarily assigns a TMSI to each mobile device in the vicinity as soon as the device in question is powered on. Because the number is associated with a specific location, it must be updated whenever the mobile device is moved to a new location. A mobile device's TMSI can also be updated at any moment by the network that it is associated with. It does this rather frequently in order to prevent listeners on the radio interface from locating the subscriber and following him or her. Because of this, it is often difficult to differentiate one phone from another, with the exception of when the phone has just been turned on for the first time or when the information contained within the phone is incorrect for some

reason. After that, the network will be required to get the "international mobile subscriber identifier" from every country in the globe (IMSI). The IMSI is only transmitted as infrequently as is practically practicable to avoid drawing attention to it and allowing it to be traced.

ROAMING

One of the most important ways that cellular networks manage mobility is through the practice known as roaming. When a user of a mobile phone leaves the region that is serviced by their home network, they have the option of automatically using a visiting network to make and receive calls, transmit and receive data, and access other services, including their home network's data services. You may do this task, which is referred to as "roaming," by using a communication terminal or by simply entering your subscriber name on the network that you are now utilizing. When it comes to the nuts and bolts of mobile communications, roaming is made possible by the procedures of mobility management, authentication, authorization, and invoicing.

LOCATION AREA

The term "location area" refers to a collection of base stations that have been strategically positioned in close proximity to one another in order to boost the overall signal strength. Base Station Controllers, also known as Base Station Controllers (BSCs) in GSM and Radio Network Controllers, also known as RNCs in UMTS, are the brains of the base stations. They are typically shared by tens or even hundreds of base stations in a given area. The Base Station Controller is responsible for the allocation of radio channels, the collection of measurements from mobile devices, and the transfer of connections from one base station to another. There is a special number that is referred to as a "location area code" that is assigned to each individual location area. Each base station, which in GSM is referred to as a "base transceiver station" (BTS) and in UMTS as a "Node B," is responsible for broadcasting the geographic area code at predetermined intervals. Within a GSM network, mobile phones are unable to communicate with one another without first traveling via BTSs. A mobile phone using a UMTS network will be unable to connect to anything in the network if it is unable to reach a Node B.

ROUTING AREA

The routing area in the PS domain functions in the same way as the location area. Generally speaking, a "location region" will be divided up into "route areas." Mobile phones that are connected to GPRS make use of something called a router zone. The "bursty" data transmission services, such as wireless internet/intranet and multimedia services, are ideally suited for GPRS's capabilities. It is sometimes named GSM-IP ("Internet Protocol") since it will link clients directly to Internet Service Providers (ISP) (ISP). It is essential to be aware of the precise location of the mobile device since packet communication occurs in brief bursts and more paging messages are anticipated for each mobile device in comparison to the more conventional circuit-switched traffic. The process of switching from one location area to another is referred to as a "location area update," and it is quite comparable to the process of switching from one routing area to another. The most notable distinction is that the component in question has been given the name "Serving GPRS Support Node" (SGSN).

TRACKING AREA

The tracking area is the LTE counterpart of the location area and the routing area. [Case in point:] A collection of cells is what's known as a tracking area. The user equipment allows for the creation of lists of tracking areas, also known as TA lists, which serve as a method for organizing tracking areas. When the user equipment (UE) reaches a tracking area that isn't already in its TA list, the tracking area is updated. This might happen on a frequent basis. Operators are able to provide unique TA lists to each individual user equipment (UE). This may prevent peaks from occurring in certain circumstances. It is feasible, for instance, that not all of the UEs worn by passengers on a train will update the tracking area at the same time. When looking at things from the perspective of the network, the Mobility Management Entity is the component that is in play.

HANDOVER

The process of shifting a mobile phone from one cell to another is referred to as "handover." The handover ought to take place for the reasons that are listed above.

1) When a mobile station leaves the coverage area of a base transceiver station (BTS), the signal strength gradually decreases until it is no longer strong enough to send.

2) The amount of interference causes an increase in the number of errors.

3) The quality of the radio connection deteriorates with time.

4) When there are an excessive number of individuals in a single cell, part of the MS will be shifted to cells that have less people in them.

The term for this is termed "balancing the load."

5) When the size of the cell is reduced, there will be an increased number of handovers.

Call drops, which are often referred to as cutoffs, are something that should not occur as a result of handover.

7.7 Data Dissemination and Management

There are many different mechanisms that may be used to transfer data in mobile computing, including as push-based mechanisms, pull-based mechanisms, hybrid mechanisms, and selective tuning techniques. Each of these mechanisms has their own advantages and disadvantages. In the next paragraphs, we'll have a more in-depth discussion regarding the various methods. Many new information-based applications have been developed as a result of the continuous improvement in technology related to communications as seen by the growth of the internet, the development of mobile and wireless networks, and the accessibility of high bandwidth in residential settings. In many of these applications, data is sent from a very small number of data producers to a relatively large number of data consumers. The term for this practice is "data dissemination." The process of transmitting and pushing data that has been created by a group of computers or broadcasting data that has been obtained via audio, video, and data services is known as data dissemination. The information is transmitted to the mobile devices. It is possible to choose, modify, and cache the essential data items on a mobile device, allowing application software to make use of the data later on. Software designed for mobile computing has a number of challenges, two of the most significant of which are determining how to make the most efficient use of available wireless bandwidth and determining how much power a given battery can store. The use of broadcast channels appears to be a viable option for resolving both of these issues with wireless data transfer. It is possible for an unlimited number of mobile users to acquire information supplied across broadcast channels simultaneously, which results in a more efficient use of bandwidth.

Communication Asymmetry

Systems that are built on disseminating information have a key weakness that makes it difficult for individuals to communicate with one another. To put it another way, the data volume and communication capacity of the upstream route are significantly lower than those of the downstream route, which connects clients to servers (from clients-to servers). The distribution of content is inherently an asymmetric process, regardless of whether it takes place through a symmetric medium like the internet or an asymmetric one like a cable television (CATV) network. This is because both types of media have their own inherent advantages and disadvantages. Therefore, in the not too distant future, it will be essential to make use of procedures and system architectures that are able to function well with asymmetric applications. It is impossible for a computer system that is fixed in one location and a mobile device to connect in the same way. A device receives a predetermined amount of bandwidth for its use. This occurs because there are a large number of devices connected to the network. The amount of data transfer capacity available downstream from the server to the device is significantly more than the amount of data transfer capacity available upstream from the device to the server. This is due to the fact that mobile devices have limited power resources, as well as the fact that higher data transmission rates maintained for longer periods of time need the devices to use more power. In GSM networks, the maximum speed at which data may be delivered uplink or downlink is 14.4 kbps. This limit applies to both directions. The symmetry of the transmission may be preserved because to the fact that GSM is only utilized for voice communication.

Classification of Data-Delivery Mechanisms

Information may often be transmitted from wireless data applications in one of two primary ways: point-to-point access or broadcast. Connection that is point-to-point is not nearly as interesting as broadcast connectivity. It is possible for a data item to fulfill all open requests for it at the same time with only a single broadcast. Therefore, broadcast is available for usage by an unlimited number of people. There are three distinct methods for broadcasting: hybrid, on-demand (often referred to as "pull-based"), and "push-based." During a push-based broadcast, the server may choose to send out transmissions of information using either a periodic or an a periodic broadcast program (generally

without any intervention of clients). A hybrid broadcast makes use of both push-based broadcasting and on-demand data transmission, both of which operate together to make the most efficient use of both of these methods. When using on-demand broadcast, the server will give out information dependent on the number of clients that are still requesting it. When mobile computers obtain information using point-to-point connections rather than through monitoring broadcast channels, the amount of battery power that is consumed by the device is reduced. Sending data can be done in one of three distinct ways: push-based (using the publish-subscribe mode), pull-based (using the on-demand mode), or hybrid (hybrid mode).

Push-based Mechanisms

The data records are retrieved from many distributed computing platforms by the server, and then they are sent to the client. Examples include things like current events, forecasts of the weather and market values, as well as sources of traffic or advertising. In the technique of data delivery known as push-based data delivery, as seen in the picture, a server or computer system is responsible for transmitting the data records that originate from a collection of distributed computing systems. Without the user's knowledge or consent, data recordings are transmitted to mobile devices. The publish-subscribe mode, which is also known as "push mode," is the process by which material is sent to users who have subscribed to a push service. When a user subscribes to have a query performed on a data record, the inquiry is considered to be a perpetual query until the user cancels their subscription to the service. It is also possible for users who are not subscribers to have data pushed to them.

The following is an explanation of the operation of push-based mechanisms:

1. For the information that will be pushed, a structure of records is selected. The flexible multi-level approach provided by an algorithm enables data items to be transmitted in the same way or in a different way depending on the amount of importance they have.
2. A mechanism that is adaptable is used to push data at regular intervals. To conserve bandwidth, all that is required is a single push. However, pushing at regular intervals is essential because it enables devices that have been disconnected the opportunity to save the data until it is delivered again. This is why it is so vital.
3. Adjustments are made to the downlink bandwidth with the assistance of an algorithm (for pushes). The majority of the time, more bandwidth is allocated to recordings that have a greater number of customers or improved access alternatives.
4. A stop-push mechanism is also utilized when a gadget is relocated to another cell when it is being moved.

Advantages of Push based mechanism

1. The transmission of data services to a large number of devices all at once is made feasible by push-based technologies.
2. The majority of the time, the service is not disrupted when it receives requests from mobile devices.
3. The use of these techniques helps prevent server overload, which can occur when a large number of devices make a request for the same thing at the same time.
4. The consumer is provided with information that he would not have had access to in any other way, such as a forecast of upcoming traffic congestion and the weather for the next several days.

Pull-based Mechanisms

The data records are obtained by the user's device or computer system either from the application database server maintained by the service provider or from a collection of computers located in various locations. A few instances of this would be servers that store music albums, ringtones, movies, and actions related to bank accounts. The server only provides a limited response to mobile devices when they request records to be retrieved. When a server decides to deliver just portion of the data packets in response to a request from a client, this action is referred to as a "selective response." This may occur after the server has identified, verified, or checked the client's

subscription account. Pull mode is also referred to as the "on-demand mode." In the pull-based data delivery system illustrated in the following graphic, a device pulls (or asks for) data records from a server or computer system that are produced by a set of distributed computing systems. These data records are then delivered to the device.

The following is an explanation of how pull-based processes function:

1. The quantity of bandwidth that is consumed on the uplink channel is impacted by the number of pull requests that are made.
2. A conclusion is arrived at regarding the pull threshold. Because of this restriction, the total number of pull requests that may be made in a given period of time is capped. This determines how frequently the server needs to restart.
3. A method has been developed that makes it impossible to remove the device from a cell once it has been transferred to another cell. This ensures that the gadget cannot be misused. The subscription either expires or is transferred to the cell network of the new service provider when the device switches service providers.

Advantages of Pull based mechanism

1. Pull-based processes ensure that the device does not get any data that the user does not request, as well as any data that is undesirable or unneeded. Instead, the device only receives the relevant data that the user has requested.
2. Pull-based strategies perform the best when the server is not busy and can reply to requests from many devices within the allotted period of time. This is the ideal scenario.

Hybrid Mechanisms

The transmitting of data via a hybrid technique utilizes both pushes and pulls to move the data. The hybrid mechanism is also known as the interleaved-push-and-pull (IPP) mechanism. Both names refer to the same thing. The devices submit pull requests for records that aren't typically pushed by the front channel through the back channel. The front channel is responsible for transmitting the interleaved responses to pull requests using the techniques that are displayed as broadcast disks. The application server or database server of the service provider, as well as a set of distributed computing systems, are the sources from which the user's device or computer system retrieves and transmits data records. The clearest illustration of this would be a strategy for marketing music recordings and increasing their sales. Marketing makes people want to purchase the album, which in turn makes mobile devices make people want to purchase the record. A device "pulls" (makes a request) from a server, and the server combines the replies it receives with the "pushes" of data records it receives from several distributed computing systems. A technique of data transmission based on both push and pull requests.

In order for hybrid mechanisms to be effective, they need to be able to:

1. There is one path for moving forward by pushing from the front and another for moving forward by pulling from the back.
2. The amount of bandwidth that is available is divided and adjusted between the two channels based on the number of active devices that are pulling data from the server and the number of devices that are requesting data pulls from the server.
3. An algorithm has the ability to reduce the level of planned pushes that is the slowest repeatedly. Lower-level data records that are considered to be of less relevance might have longer push intervals within a broadcasting scheme.

Advantages of Hybrid Mechanism

Can Offer You there are Significantly Fewer Requests That Have to Wait in Line, and There Are Fewer Interruptions to the Server

Keywords

GSM - Global system for mobile communication

UMTS - Universal mobile telecommunication service

TMSI – Temporary mobile subscriber identity

IMSI – International mobile subscriber identity

GPS – Global positioning system

MSC - Mobile switching center

VLR - Visitor location register

HLR - Home location register

MNRF - Mobile not reachable flag

BTS - Base transceiver system

RNC - Radio network Controllers

ISP – Internet service provider

SGSN - Serving GPRS support Node

LTE - Long term evolution

UE - User Equipment

CATV - Cable television network

SIM - Subscriber identity module

Self Assessment

1. Which of the following usually stores all user-related data that is also relevant to GSM mobile systems?

A. VLR
B. HMR
C. CMR
D. SIM

2. In which one of the following codes with specific characteristics can be applied to the transmission?

A. CDMA
B. GPRS
C. GSM
D. All of the above

3. In the Cellular Network, on which of the following, the cell's shape depends?

A. Political conditions
B. Social Conditions
C. Environnent Condition
D. None of the above

4. The capacity of a system to hide differences in the presentation of data on various computers and the path to take in order to access a certain resource is referred to as _____.

A. Data transparency
B. Position transparency
C. Access Transparency
D. None of the above

5. What kind of Protocol is used to provide Internet access from mobile?

A. TCP/IP
B. ISD
C. WAP
D. HTTP

6. What is the full form of SIM?

A. Station Identity Module
B. Subscriber Identity Module
C. System Identity Module
D. None of the above

7. Which of these is a GSM supplementary service?

A. SMS
B. Call forwarding
C. Emergency number
D. All of the above

8. The full form of the term "HLR" is:

A. Home Location Register
B. Home Live Register
C. House Location Register
D. None of the above

9. The drawbacks of all the Mobile Devices and Wireless Devices are:

A. It requires a big source of power
B. It has smaller keypads
C. It rapidly consumes power
D. All of the above

10. Both _____ and _____ are types of radio networks that are constructed from a variety of cells, also known as base stations

A. GPRS, CDMA
B. GSM, CDMA
C. TDMA, UMTS

D. GSM , UMTS

11. The process of shifting a mobile phone from one cell to another is known as_____.

A. Shifting
B. Handover
C. Mobility
D. None of the above

12. The quantity of bandwidth that is consumed on the uplink channel is impacted by the number of _____.

A. Push requests
B. Confirmation requests
C. Unknown requests
D. Pull requests

13. The transmission of data services to a large number of devices all at once is made feasible by _____technologies.

A. Push -based
B. Pull -based
C. Hybrid-based
D. Analysis-based

14. _____ is the piece of information that is transferred from the phone to the network.

A. IMEI
B. TMEI
C. TMSI
D. IGRI

15. Hybrid mechanism of request allows to have fewer requests on the network.

A. TRUE
B. FALSE

Answers for Self Assessment

1.	D	2.	A	3.	C	4.	C	5.	C
6.	B	7.	B	8.	A	9.	D	10.	D
11.	B	12.	D	13.	A	14.	C	15.	A

Review Questions

1. Explain in detail the concept of Handover in GSM technology.

2. Classify and explain the various data delivery models.
3. What do you understand by the term transparency in mobile computing?
4. Discuss in detail the issues in mobile computing environments.
5. What do you understand by the term adaptability?

Further Readings

- Wireless communications & networks by William Stallings, Pearson
- Principles of wireless networks by Kaveh Pahlavan, Pearson
- Fundamentals of wireless networking by Ron price, McGraw hill education
- Wireless networks first-step by Jim Geier, cisco press

Web Links

- http://59.51.24.50:8000/wxwl/Wireless_Communications_&_Networking_Stallings_2nd.pdf
- https://ebookreading.net/view/book/EB9780071782586_10.html

Unit 08: Wireless LAN Technology

CONTENTS

Objectives

- Understanding the concepts of WLAN
- Analyzing the transmission technology behind the wireless local area network.
- Understanding the Infrared LAN and its configurations.
- Analyzing the spread spectrum LAN.

Introduction

These days, wireless local area networks (WLAN) are becoming increasingly widespread. It's possible that you've already utilized wireless programs on your laptop or mobile phone. Users of wireless LANs are able to communicate with one another without the usage of cables. In order for users to send and receive data, every WLAN network requires a wireless Access Point, also known as an AP. Because wireless networks do not function like conventional networks, which can both send and receive data at the same time, an Access Point (AP) is frequently referred to as a Wireless Hub (full duplex). The primary distinction between a wireless local area network (WLAN) and a wired local area network (LAN) is that a WLAN transmits data via energy waves, also known as radio waves, rather of transferring electrical signals through a cable. To access media, WLAN makes use of CSMA/CA, which stands for Carrier Sense Multiple Access with Collision Avoidance. This is in place of the more traditional CSMA/CD protocol. The CSMA/CD protocol is incompatible with WLAN because devices that transfer data cannot simultaneously send and receive data. There are now three organizations with a voice in the development of WLAN standards. They are the Wi-Fi Alliance, which makes it simpler for wireless products made by different companies to work together, the IEEE, which specifies how RF is modulated to send data, and the ITU-R, which is in charge of allocating RF bands. The Wi-Fi Alliance makes it easier for wireless products made by different companies to work together. However, the IEEE 802.11 standard, more often referred to as Wi-Fi, is the foundation of the wireless local area network (LAN) that is currently the most widely used. The ISM band at 5.7 GHz is where 802.11a may be found operating. The wireless signal can travel up to a distance of 25–75 feet indoors, and it can travel at a maximum speed of 54 Mbps. The ISM band at 2.4 GHz is where 802.11b may be found operating. The wireless signal may travel between 100 and 200 feet indoors, and the maximum

speed that 802/11g is capable of sending data at is 11 Mbps. This gadget operates on the ISM band that operates at 2.4 GHz. Wireless signals have a range of between 100 and 200 feet within buildings, and their maximum transfer speed is 54 megabits per second (Mbps). The Federal Communications Commission (FCC) is in charge of overseeing the Industrial, Scientific, and Medical (ISM) band in the United States. Permission is often required for the many usages of the spectrum. The Federal Communications Commission (FCC) has reserved bandwidth for unlicensed usage so that wireless local area networks can be implemented. This includes the 2.4 GHz band, which is utilized by a large number of WLAN devices. The acronym "Wi-Fi" refers to "Wireless Fidelity," which is the name given to any of the wireless technologies that comply with the IEEE 802.11 standard. The Wireless Ethernet Compatibility Alliance came up with the moniker "Wi-Fi" for its networking standard (WECA). Products that have received the Wi-Fi certification are able to communicate with one another, even when they were manufactured by different businesses. There are three IEEE WLAN standards that are most popular: 802.11a, 802.11b, and 802.11g. Some access points, if not all, support these protocols.

8.1 Types of Wireless Networks

There are three primary usage scenarios for wireless connectivity:

1. Wireless Personal Area Networking (WPAN)
2. Wireless Local Area Networking (WLAN)
3. Wireless Wide Area Networking (WWAN)

8.2 WPAN (Wireless Personal Area Network)

WPAN stands for "wireless personal area network" and is an application for wireless technology that is designed to be utilized mostly in private settings. Instant communication between devices that handle personal data or allow small groups of individuals to share data is the primary topic of this discussion. One illustration of this would be saving the same information on both a traditional computer and a personal digital assistant. One further illustration of this is the accidental sharing of a paper by two or more persons. In instances like these, data sharing is always done on an ad hoc basis, and it's not necessarily planned out in advance. Because wireless communication streamlines the process, it enables these sorts of applications to perform more effectively (i.e. eliminates the need for cables). A personal area network (PAN) that makes use of wireless connections is known as a wireless personal area network, or WPAN for short (WPAN). PANs, or personal area networks, are a type of network that connects devices and is concentrated on the workplace of a single individual. Wireless personal area networks (PANs) are constructed on top of the IEEE 802.15 standard. Bluetooth and Infrared Data Association are both forms of wireless technology, and WPAN makes use of both of these technologies. There are a wide variety of potential applications for a WPAN. For instance, it could be able to link all the widespread computers and mobile phones that many people have on their workstations or carry with them in the modern day. It might also be used for something more particular, such as allowing members of the surgical team and other team members to communicate with one another while an operation is being performed. The concept of "plugging in" is essential to the operation of WPAN technology. When two WPAN-enabled devices are in close proximity to one another (within a few meters), or when they are in close proximity to a central server, they should be able to communicate with one another as easily as if they were physically linked by a cable. This would be the ideal scenario. Another key aspect is that each device should have the capacity to selectively shut out other devices, so eliminating interference that isn't necessary and information access that isn't allowed. The WPAN technology is still in its infant phases, but its development and use are accelerating at a rapid pace. It is recommended that the operating frequency for digital modes be at around 2.4 gigahertz. The idea is to make it simpler for the many systems and appliances found in homes and businesses to get along with one another. Every device that is part of a WPAN has the ability to connect to every other device that is part of the same WPAN as long as those devices are in close proximity to one another. WPANs all over the world will be connected to one another as well.

An archeologist on site in Greece might use a PDA to directly access databases at the University of Minnesota in Minneapolis, and to transmit findings to that database.

Bluetooth: When using Bluetooth, short-range radio waves may travel up to a distance of 10 meters. Examples of devices that are able to connect wirelessly to Bluetooth peripherals include personal digital assistants (PDAs), mobile phones, and personal computers. Other Bluetooth peripherals include headphones, keyboards, and mouse.

A Bluetooth Personal Area Network, often known as a piconet (from the prefix "pico," which means "extremely small" or "one trillionth"), is a network that can consist of up to 8 active devices that operate in "master-slave mode" (a much larger number of devices may be linked in "parked" mode). In a piconet, the first Bluetooth device in the network acts as the master, while the other Bluetooth devices in the network function as slaves to it. A piconet has a maximum range of 100 meters (330 feet) when the circumstances are perfect; but, in most cases, it can only reach a distance of 10 meters (33 feet).

Infrared Data Association: The Infrared Data Association (IrDA) makes use of infrared light with a frequency that is lower than what the human eye can detect. For instance, infrared technology is utilized in the majority of TV remote controllers. IrDA is typically utilized by WPAN devices such as printers, keyboards, and several other serial data interfaces.

WiFi: WiFi usually works within a local area network (LAN), and it uses radio waves to connect devices up to 91 meters away. WiFi can connect local area networks so that multimedia content from a PC can be streamed to the TV (using a Wireless Multimedia Adapter). It can also connect video game consoles to their networks, connect cellphones to the Internet so that music and other media can be downloaded, and do other things. Smart phones can use WiFi to connect to the Internet and download music and other content (Nintendo WiFi Connection).

Body area network: The foundation of a body area network is the IEEE 802.15.6 standard for transmission across the capacitive near field of human skin. This standard is what enables devices worn by and in close proximity to the wearer to communicate with one another over a body area network. The application of Skin plex has the ability to locate and communicate with human bodies located up to 1 meter (3 feet 3 inches) away. Its purpose is to prevent the tops of convertible cars from being jammed and to regulate who is allowed to open doors.

8.3 WLAN (Wireless Local Area Network)

On the other hand, WLAN connections, like their cable counterparts, are more for organizational networking. With the use of wireless local area network (WLAN) technology, users may access corporate network resources like shared data, apps, or email without being constrained by the network's physical location. Maintaining a robust wireless connection inside a specific location, such as an office building or college campus, is crucial. This indicates that a certain region where the network operates is defined by wireless access points. WLANs, also known as wireless local area networks, are similar to traditional local area networks (LANs), except they employ wireless interfaces rather than cable ones. Wireless local area network (WLAN) technology is swiftly gaining popularity since there are so many tiny, portable devices like personal digital assistants (PDAs). Wireless local area networks (WLANs) enable rapid Internet access in locations such as offices and buildings. Users may move about freely in a constrained area while still being connected to the network thanks to this capability.

Transmission Technology

There are three main ways by which WLANs transmit information: microwave, spread spectrum and infrared.

1. Microwave Transmission: In order to broadcast and receive data, the Motorola WLAN device known as ALTAIR makes use of low-power microwave radio frequencies. It is capable of operating at frequencies up to 18 GHz.

2. Spread Spectrum Transmission: Products for wireless local area networks that utilize frequency hopping and direct sequence modulation are the ones that make use of this transmission method.

1) **Frequency hopping**: Within the confines of a certain frequency range, the signal hops from one frequency to the next The transmitter "listens" to a channel, and if it detects a period of silence during that "listening," it will send data utilizing the full bandwidth of the channel (i.e., when no signal is being sent). It "hops" to another channel and repeats whatever it was doing before if the

original one is already at capacity. When the transmitter and receiver "jump," they both experience the same phenomenon.

b) **Direct Sequence Modulation**: This approach makes use of Code Division Multiple Access and a comprehensive spectrum of frequencies (CDMA). A certain frequency range is used for the transmission of signals from a variety of different devices. These signals don't pack much of a punch, that's for sure (just above background noise). Every signal has a unique code that identifies the unit that transmitted it to the receiver and lets them know which signal was transmitted. "Industrial, Scientific, and Medical band" is the name given to the frequency at which these sorts of signals are transmitted; the acronym "ISM" stands for "industrial, scientific, and medical." Only devices that fall under the category of ISM are permitted to use this frequency band. The ISM band consists of three distinct frequency ranges: 902–928 MHz, 2400–2483.5 MHz, and 5725–5850 MHz. Each of these ranges is used for a specific purpose. The Motorola ALTAIR is an exception to this rule because it operates at 18GHz. Numerous manufacturers of wireless LANs, such as NCR for its wave LAN and Spectra Link for its 2000 PCS, make use of spread spectrum transmission in their products.

3. Infrared Transmission Information is transmitted by the use of infrared light in this approach, which is referred to as "infrared transmission." Transmission of infrared rays can either be dispersed or directed, or it can be directed from one location to another.

a) Diffused: Because the area is flooded with infrared light emanating from the sending unit (for example, an office), any equipment that is capable of detecting the signal in that region is able to do so.

b) Directed: Before the signal is transmitted, the infrared light is directed in a certain direction. The transmission goes much more quickly when you use this strategy.

c) Directed point-to-point transmission: This is the method that transfers infrared waves from one location to another in the shortest amount of time. At this point, the receiver and the transmitter unit are aligned with one another. After that, the infrared light is sent without any intervening steps to the receiver.

The environment has a significant role in determining the kind of light source that is employed for infrared transmission. LEDs are often utilized for applications that take place inside, whereas lasers are typically employed for applications that take place outside.

Caution: Infrared radiation (IR) has major biological effects. It greatly affects the eyes and skin. Microwave signals are also dangerous to health. But with proper design of systems, these effects are reduced considerably.

Technical Standards

People that make use of wireless LAN solutions should place a high level of importance on adhering to certain technical requirements. On the same wireless network, users want to be able to utilize wireless devices that were manufactured by a variety of different vendors. The IEEE Project 802.11 has ensured that there are international standards for wireless local area networks (LAN). In the following paragraphs, we'll discuss a few of these guidelines in more detail.

Requirements

In March of 1992, the IEEE Project 802.11 developed a standard protocol for wireless local area networks (LANs). You require at least 1 Mbps of bandwidth for activities like transmitting files and loading applications. Things like digital voice and process control, which need to send and receive data in real time, are examples of applications that necessitate the use of time-bound services.

Classification of wireless LANs

A distinction was drawn by the Project 802.11 group between wireless local area networks that are "ad-hoc" and those that are "infrastructure."

Ad-hoc Network: Networking on an as-needed basis (AN) By congregating in a concentrated space, many users of mobile devices can create their own network. It is not dependent on assistance from a wired or wireless backbone in any way. There are two distinct applications that are possible with this network.

Flooding and Broadcasting: Suppose a mobile user A wishes to share certain information with a user B who is in close proximity to them. User A immediately transmits the completed data packets to the rest of the network once they are prepared. The receiver verifies the sender's identity once it has the packet in its possession. If it determines that the person who received the packets wasn't the intended recipient, it transmits the packets again. This process is repeated as many times as necessary until user B receives the data.

Temporary structures: By utilizing this method, mobile users can construct a temporary infrastructure. However, this strategy is difficult to implement and results in additional expenses. It is only useful when there are a relatively small number of users utilizing mobile devices.

Infrastructure Networks: Users of this type of network are able to travel freely around an entire building while still maintaining their connection to the various computer resources. The components of a wireless LAN architecture were outlined in the IEEE Project 802.11 document. In the context of a network architecture, a cell may also be referred to as a Basic Service Area (BSA) (BSA). There are several wireless stations located inside the building. The power of the transmitter and receiver, in addition as the surrounding environment, are taken into account while determining the size of a BSA. Access Points are the nodes that connect a group of Base Station Adapters (BSAs) to a distribution system as well as to one another (APs). A Basic Service Set is the name given to the collection of stations that make up an Access Point (BSS).

8.4 Infrared LANs

For items like remote controls, optical wireless communication in the infrared region of the spectrum is routinely utilized in the majority of residential settings. Infrared technology has recently been under investigation for its application in the creation of wireless local area networks (LANs). In this part of the article, we will begin by contrasting the characteristics of radio LANs and infrared LANs, and then proceed to investigate the specifics of infrared LANs.

Strengths and Weaknesses

Infrared and microwave radio, both of which can utilize either spread spectrum or narrowband transmission, are the two modes of data transfer that are utilized by wireless local area networks. Radio communication using infrared is superior to that via microwave in a number of critically significant respects. To begin, the vastness of the infrared spectrum suggests that it would be able to transmit data at extremely rapid rates. The infrared spectrum, on the other hand, is devoid of any regulations, in contrast to some regions of the microwave range. In addition, infrared light shares some of the same characteristics as visible light, which makes it a viable option for certain topologies of local area networks (LANs). Because objects with light colors scatter infrared light, it is simple to illuminate an entire room by reflecting light off of the ceiling. This is because light-colored objects disperse infrared light. Things like walls that are very opaque prevent infrared light from passing through them. This has two distinct benefits: It is possible for each individual room in a building to have its own independent infrared installation that does not interfere with that of the other rooms. Because of this, it is possible to construct very large infrared LANs. To begin, it is far simpler to prevent anyone from eavesdropping on infrared transmissions as opposed to microwave ones. Another advantage of using infrared is that the necessary equipment is inexpensive and simple to use. Since most IR receivers need only to measure the amplitude of optical signals, in contrast to most microwave receivers, which also need to measure the frequency or phase, intensity modulation is frequently used when sending data over infrared. This is because most IR receivers can only measure the amplitude of optical signals. There are also some activities that are incompatible with infrared technology. Because of the illumination and the sunshine, the level of infrared background radiation that is present inside is rather high in a good number of the rooms. Because of this background radiation, infrared receivers are able to pick up noise. Because of this, infrared transmitters have to be stronger than they otherwise would have to be, which reduces the range. On the other hand, increasing transmitter power is prevented due to worries about the effects on the eyes and the use of an excessive amount of electricity.

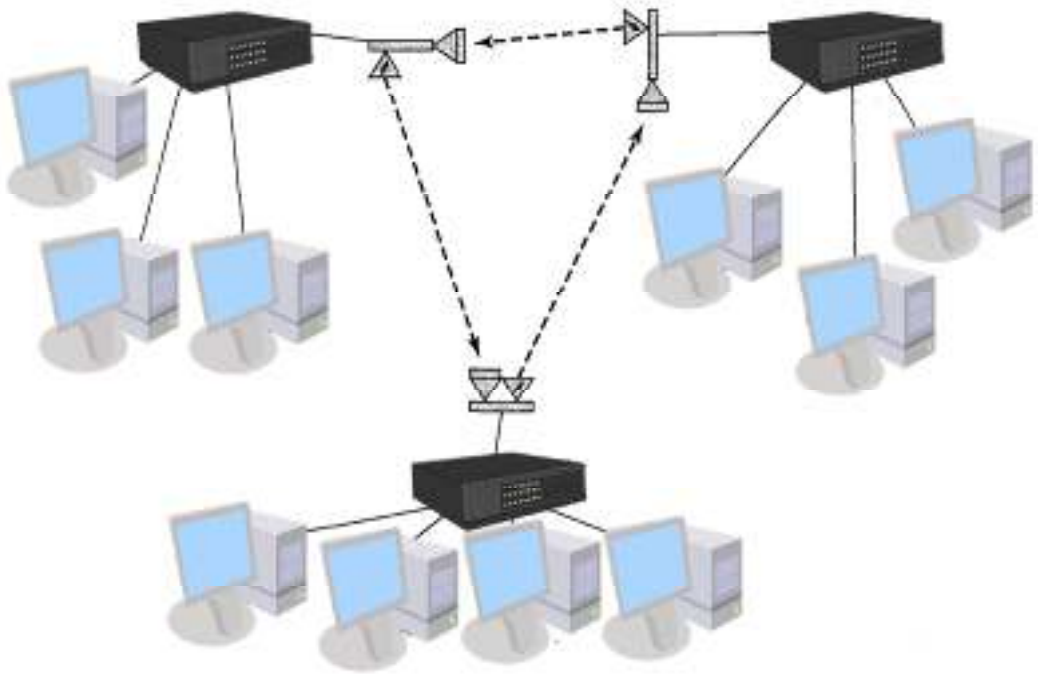
Transmission Techniques

For infrared (IR) data transfer, the signal can also be sent out in all directions, reflected off a light-colored ceiling, or controlled and concentrated like a remote control for a television set.Making wide-angle point-to-point connections using an infrared directed beam may be done with this

technology. In this mode, the range is determined by the amount of power that is sent out as well as the amount of focus that is applied.

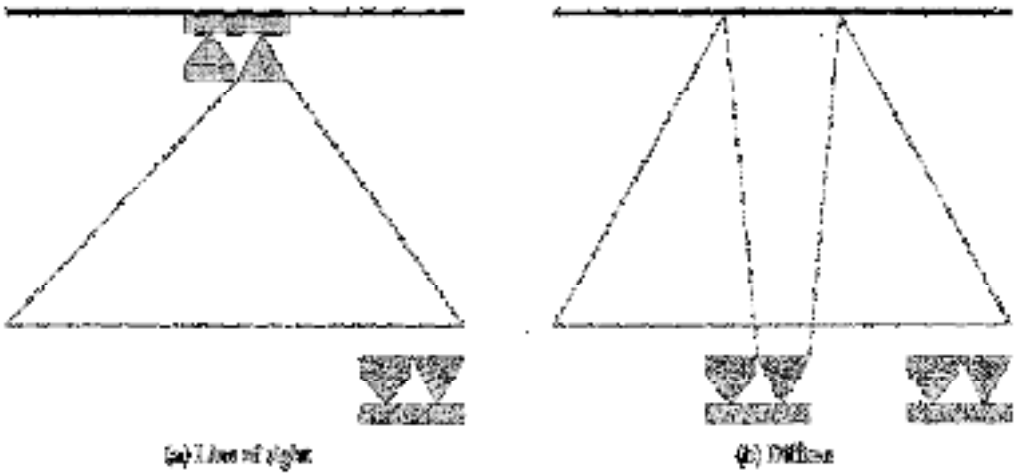
Directed Beam Infrared

A data link using focused infrared light can travel up to several kilometers. Building wireless local area networks (LANs) inside does not require ranges of this kind. However, a bridge or router in one building can be connected to another bridge or router in a separate building using an infrared link. Token ring local area networks (LANs) can be established inside with the use of point-to-point infrared (IR) communication. You are able to arrange a collection of infrared (IR) transceivers in such a way that data circulates in a ring around them. Each transceiver has the capability of supporting either a single workstation or a hub of several stations. The hub serves as a connection point for all of the stations.



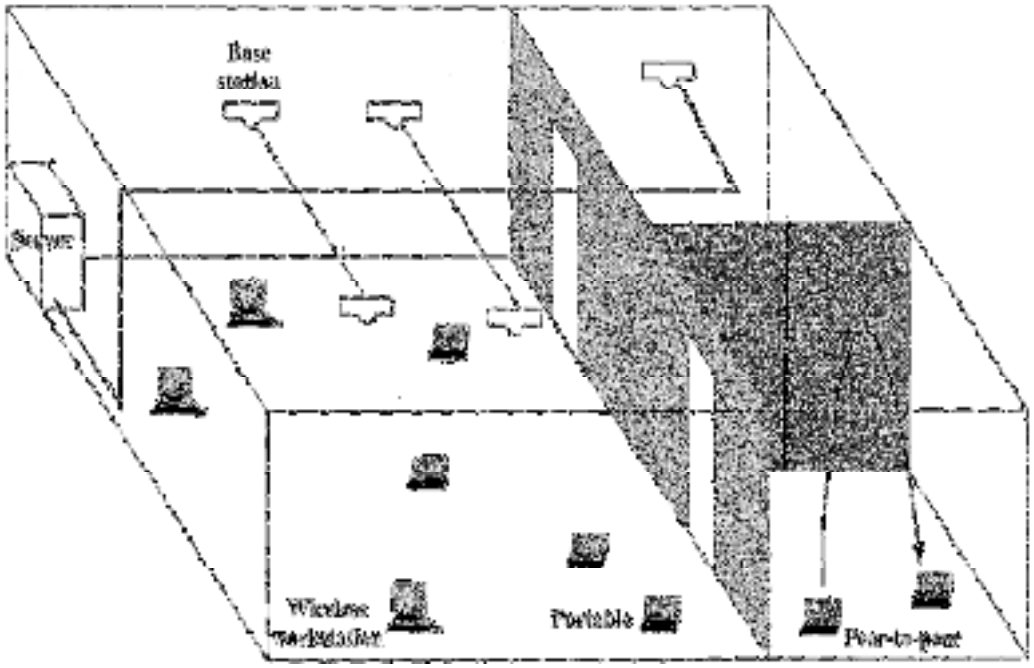
Omni directional

There is just one base station used in an omni directional configuration, and that station is able to view every other station on the local area network. This station is typically mounted on the ceiling in most settings. The base station consists of a multiport repeater, which describes the function of the station itself. The signal that is broadcast from the ceiling transmitter can be received by any of the other IR transceivers that are in the immediate vicinity. These additional transceivers each emit a beam that is directed at the base unit that is located in the ceiling of the room.



Diffused

The architecture of this system directs all of the infrared (IR) transmitters toward a single point on the ceiling that diffusely reflects light. All of the neighboring receivers are able to pick up the IR energy as it reenters the room after it has been reflected by the ceiling. A possible configuration for a wireless IR LAN is shown in the figure. A base station is installed on the ceiling at the center of each individual room. Each station provides access to the network for a certain number of mobile and stationary workstations in the surrounding area. Through the cable in the ceiling, all of the base stations are connected to a server, which can function as an access point to a wired LAN or WAN. Ad hoc networks can also be set up in conference rooms even if there is no base stations present in the room.



8.5 Spread Spectrum LANs

A multiple-cell architecture is utilized by spread spectrum wireless LANs unless the working area is extremely compact. Cells that are next to one another utilize different center frequencies within the same band to prevent their signals from interfering with one another. Both a hub architecture and a peer-to-peer architecture are viable options for the network structure of a cell. A hub is used in a topology known as a hub topology to link stations that are connected to the wired LAN as well as stations that are connected to wireless LANs in different cells. Hubs are often mounted on the ceiling, and they are connected to a backbone wired local area network (LAN). Access control is another function that the hub may do; it serves as an IEEE 802.11 point coordinator as well. In addition, access may be controlled by the hub by using it in the role of a multiport repeater, which is the same function served by 10-Mbps and 100-Mbps Ethernet multiport repeaters. In this scenario, the hub is the only location within the cell where all of the stations may send and receive data at the same time. A design for a rational bus would look exactly the same as this. On the other hand, and irrespective of the technology used for access control, every station has the ability to broadcast using an antenna that is capable of picking up signals from any location inside the cell. It is also possible to employ a hub to provide an automated switching system between mobile stations. The proximity of particular stations to a central hub determines whether or not they are permanently and routinely connected to that hub. When the hub detects that the signal is becoming less strong, it is able to immediately hand control of the network over to the hub that is physically located closest to it. There is no "hub" or other centralized location in a peer-to-peer topology since there is no need for one. Access is restricted by the use of a MAC technique such as CSMA. This design works well for ad hoc local area networks (LANs).

Transmitter Issues

It is recommended that a wireless local area network (LAN) be used without the need to go through a licensing procedure; however, this is not a necessity. This objective is made more difficult to achieve because the licensing rules in each nation are different from one another. Spread spectrum systems, which can use up to 1 watt, and extremely low power systems, which can use up

to 0.5 watt, are two unlicensed uses of the ISM band that the Federal Communications Commission in the United States allows. Spread spectrum systems can use up to 1 watt. Extremely low power systems can use up to 0.5 watts (FCC). Wireless local area networks that utilize spread spectrum technology have gained popularity since the FCC made this band available for usage. In the United States, there are three microwave bands that can be utilized without the need for a license: the 902–928 MHz (915 MHz band), the 2.4–2.4835 GHz (2.4 GHz band), and the 5.725–5.7825 GHz band (5.8 GHz band). This particular use of the 2.4 GHz frequency band may be found in both Europe and Japan. The sequence in which the three bands are presented is noteworthy from the perspective of capacity because of the link that exists between frequency and the maximum bandwidth that may be supported by the band. It is also essential to take into consideration the possibility of interference. Numerous electronic gadgets, including cordless phones, wireless microphones, and amateur radios, make use of the radio frequencies that are located around 900 MHz. The microwave oven is an example of a well-known appliance that operates at 2.4 GHz. As units age, they have a greater propensity to release more radiation.

8.6 Narrowband Microwave LANs

The transmission of a signal using a radio frequency band that has a bandwidth that is relatively narrow is an example of narrowband microwave. The signal can be processed since the bandwidth is just large enough. Up until quite recently, all narrowband microwave local area network (LAN) equipment were required to use a microwave band that required a license. At least one manufacturer has recently developed a local area network (LAN) device that is compatible with the ISM frequency.

Licensed Narrowband RF

The microwave radio frequencies that are used to convey speech, data, and video are licensed and coordinated in particular regions to prevent systems from being confused. These frequencies may be used to send voice, data, and video. In the United States, licensing is overseen by the Federal Communications Commission (FCC). Each region has a radius of 28 kilometers and is permitted to have a maximum of five licenses, each of which covers a pair of frequencies. In the 18 GHz band, Motorola possesses 600 licenses (1,200 frequencies), which allow the company to cover all cities with 30,000 people or more. The typical configuration of the cells used in a narrowband technique is seen in Figure 13.2. The frequency bands that are used by cells that are next to one another do not overlap within the 18-GHz range as a whole. Because Motorola controls the frequency spectrum in the United States, the company is able to ensure that separate local area networks (LANs) that are in close proximity to one another do not communicate with one another. Each and every transmission is encoded with a secret key in order to maintain confidentiality and prevent eavesdropping. The licensed narrowband local area network has the benefit of ensuring that the connection does not become disrupted in any way. In contrast to ISM, which does not require a license, licensed spectrum bestows the legal right on the holder of the license to a data communication channel that is unaffected by interference. Users of local area networks operating in the ISM band could have problems interacting, and they might not be able to legally do anything about it.

Unlicensed Narrowband RF

In 1995, Radio LAN was the first business to market a narrowband wireless local area network (LAN) that operated on the unlicensed ISM frequency. Signals with low power and narrow bandwidths can be sent using this frequency (0.5 watts or less). The Radio LAN device operates at 10 megabits per second while utilizing the 5.8 GHz band. The device may be utilized up to 50 meters away in an office that has some partitions, and up to 100 meters away in an office that is completely open. In one respect, the peer-to-peer technology that is utilized by the Radio LAN is an unusual one. The Radio LAN device uses an algorithm to determine which node should serve as the Dynamic Master rather than having a permanent hub. The algorithm takes into account factors such as location, interference, and signal strength. It's possible that the master's name will evolve all on its own as time goes on. The local area network also possesses a function known as "dynamic relay," which enables each station to function as a repeater for other stations that are located too far apart to communicate with one another directly.

Summary

- In this unit the concepts of wireless local area network were discussed
- The discussion about the transmission technology behind the wireless local area network was discusses.
- The explanation of Infrared LAN and its configurations was done.
- In this chapter the spread spectrum LAN was discussed.

Keywords

WLAN - Wireless local area network

AP - Access point

CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance

CSMA/CD - Carrier Sense Multiple Access with Collision Detection

WECA - Wireless Ethernet Compatibility Alliance

WPAN - Wireless Personal Area Networking

WWAN - Wireless Wide Area Networking

IrDA - Infrared Data Association

BSA – Base service area

IR - Infrared

Self Assessment

1. What is the standard form of WI-FI?

A. Wired Fidelity
B. Wired Function
C. Wireless Fidelity
D. None of the above

2. The frequency range of WI-FI is about?

A. 4 GHz and 5 GHz
B. 9 GHz and 5 GHz
C. 4 GHz and 5 GHz
D. 4 GHz and 5 GHz

3. WI FI can support

A. Unlimited number of users
B. Limited number of users
C. Users less than Bluetooth devices can handle
D. None of the above

4. Range of a typical WI-FI is about

A. 50 meters
B. 60 meters
C. 70 meters

D. 80 meters

5. With the WI-FI it is possible to connect
A. Mobile Phones
B. Laptops
C. PCs
D. All of the above

6. Out of the following which is NOT a type of wireless Network
A. WPAN
B. WLAN
C. WWAN
D. None of the above

7. IRDA uses the frequency of infrared waves that has a frequency _____ human eye sensitivity.
A. Higher than
B. Lower than
C. Equal than
D. None of the above

8. The other name for the Bluetooth PAN is _____.
A. Bluenet
B. Piconet
C. Biconet
D. Viconet

9. Body area network is based on_____ Standard.
A. 802.15.1
B. 802.11
C. 802.15.6
D. 802.15

10. The frequency of ALTAIR transmission is
A. 11 GHz
B. 18 GHz
C. 10 GHz
D. 5 GHz

11. Out of the following which is not a type of Infrared transmission
A. Diffused
B. Directed
C. Directed point to point

D. Broadcast

12. In spread spectrum local area networks which algorithm is used for controlling the access.
A. CDMA/CD
B. CDMA
C. CSMA/CA
D. CSMA

13. FCC stand for
A. Finance commission center
B. Federal communications commission
C. Frequency control center
D. Frequency communication center

14. In the Omni directional infrared LANs the station is typically mounted on
A. Ground
B. Walls
C. Ceilings
D. Outdoors

15. The spectrum for infrared is virtually unlimited.
A. True
B. False

16. The standard 802.11a doesn't support data rate of _____
A. 6 Mbps
B. 9Mbps
C. 12Mbps
D. 1Mbps

Answers for Self Assessment

1.	C	2.	A	3.	B	4.	B	5.	D
6.	D	7.	B	8.	B	9.	C	10.	B
11.	D	12.	D	13.	B	14.	C	15.	A
16.	C								

Review Questions

1. Write and explain the WLAN technology in detail.
2. Explain how the Spread spectrum LANs systems in detail.

3. Compare and contrast the functionality WLAN and Spread spectrum LAN
4. Explain the Narrowband microwave LANs functionality in detail.
5. Elaborate the concept of infrared LANs in detail.
6. Explain how the WPAN operates.

Further Readings

- Wireless communications & networks by William Stallings, Pearson
- Principles of wireless networks by Kaveh Pahlavan, Pearson
- Fundamentals of wireless networking by Ron price, McGraw hill education
- Wireless networks first-step by Jim Geier, cisco press

Web Links

http://59.51.24.50:8000/wxwl/Wireless_Communications_&_Networking_Stallings_2nd.pdf

Unit 09: Wi-Fi and IEEE802.11

CONTENTS

Objectives

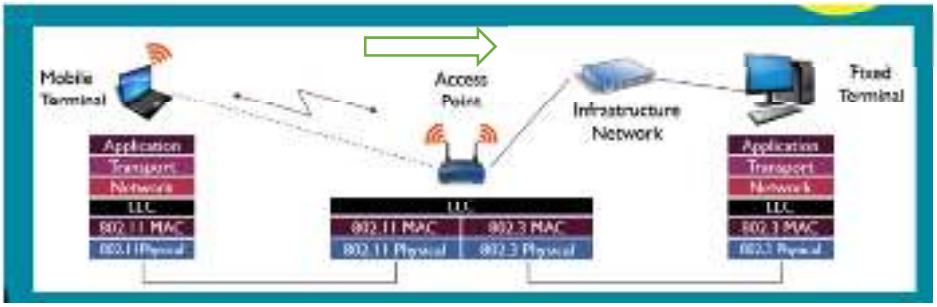
- Understanding the concepts of WLAN
- Analyzing the transmission technology behind the wireless local area network.
- Understanding the Infrared LAN and its configurations.
- Analyzing the spread spectrum LAN.

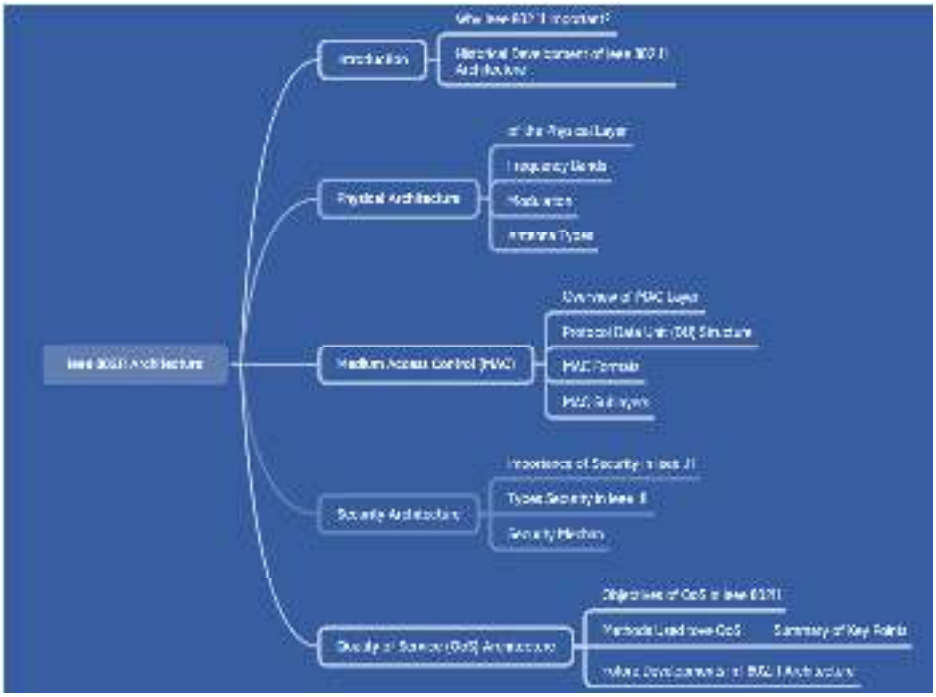
Introduction

The IEEE 802.11 architecture is a commonly used set of protocols for wireless local area network (WLANs). This defines the physical and data-link layer specifications to enable wireless communication devices. It provides support for multiple channels, data, and security mechanisms that allow for reliable and secure transmission. The architecture is based on radio frequencies and utilizes carrier signals to transmit data between devices. IEEE standard has evolved over the years to include newer versions that support higher data rates and improved security features. As a result, the architecture has become widely adopted standard for wireless communication in industries. The standard is a set of protocols that govern wireless local area networks (WLANs). Introduced in 1997, IEEE 802.11 was the first wireless networking standard, and it has several updates over the years to up with the evolving. The 802.11 architecture includes several layers, each with its own set of protocols and functions. The standard is a set of protocols that govern wireless local area networks (WLANs). Introduced in 1997, IEEE 802.11 was the first wireless networking standard, and it has several updates over the years to up with the evolving. The 802.11 architecture includes several layers, each with its own set of protocols and functions. These layers include the physical layer, data link layer, network layer transport layer, and application layer. Each layer is for different aspects wireless communication, from encoding and data to establishing connections between devices. As wireless technology advance, the IEEE 802.11 standard will continue to evolve to keep pace the needs of modern users and devices. IEEE 802.11 is important because it is the internationally recognized standard for wireless communication . This standard defines protocols that are necessary to enable wireless devices communicate with other seamlessly and safely. It allows users to stay connected to internet regardless of their location within the network coverage area eliminating the need for physical connections.

The IEEE 802.11 standard is continually evolving to meet the growing demand for faster and more reliable wireless connectivity. This evolution has led to the development of newer versions of the

standard that provide faster speeds, greater, and improved security features. With the increasing popularity of mobile devices the internet of things, IEEE 802.11 has become an essential part of the technology landscape. The historical development of the IEEE 802.11 architecture can traced back to the late1980s when the Federal Commission (FCC) opened up the 900 MHz and 2.4 GHz frequency bands. This led to the emergence of wireless technologies that enabled faster data rates and better connectivity. The first versions of the IEEE standard were developed and released in 1990s. Over the years, the standard underwent several advancements such as the of higher data transfer rates, improved security features, and the of new frequency bands. Today, the IEEE 802.11standard has become the de facto for WLANs and has revolutionized the way we connect and wirelessly.



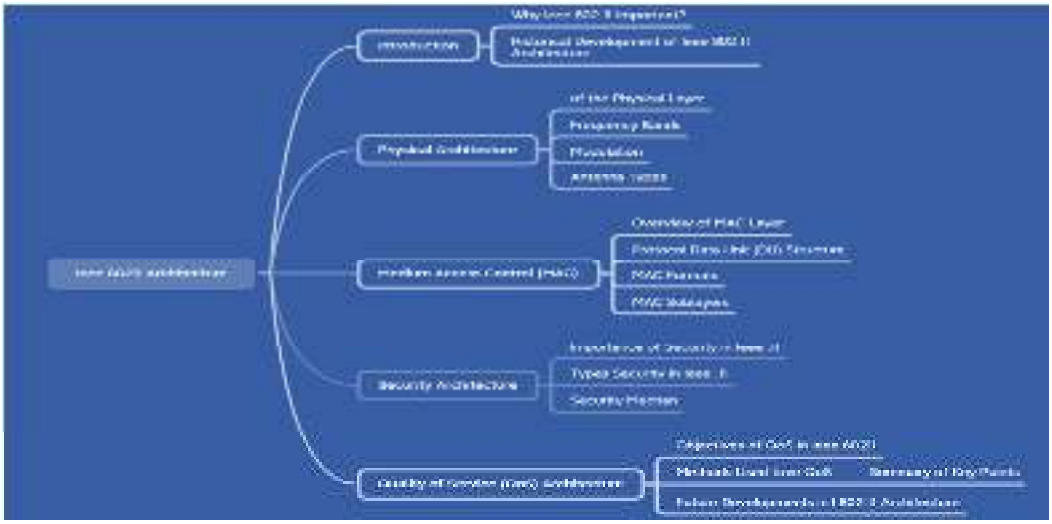


9.1 IEEE 802.11 Physical Layer

The Physical Architecture of IEEE802.11 is an important of its overall structure and it refers to the physical transmission between devices within the same network. In addition it supports multiple antennas on both the and receiver, which improves range and reliability. The IEEE 802.11 Physical Architecture also protocols for power management, avoidance, and signal quality monitoring to ensure efficient and reliable data transmission. Overall, the Physical Architecture helps to maintain a robust wireless connection within. The Physical Layer is the layer in the IEEE 80211 architecture, responsible for physical transmission of data across the network. It defines the encoding and modulation techniques used to transmit data over the wireless medium, including frequency band, channel bandwidth and transmission power. The Physical Layer also manages synchronization and timing of the wireless network, making sure that all are communicating on the same channel with the correct timing. The Physical Layer is crucial component in the overall IEEE 802.11 and its proper functioning is critical to the success of the wireless network. The IEEE802. architecture operates within certain frequency bands have been allocated for wireless. These frequency bands

include the 2.4 GHz and the 5 GHz band. 2.4 GHz band divided into 14 overlapping, which can be used for purposes depending on the country and region. The 5 GHz band is divided into several non-overlapping channels, providing a number of channels to avoid.

The use of these frequency bands allows IEEE 802.11 to provide wireless communication for a wide range of devices, including laptops, smartphones and other wireless-enabled devices. Understanding the frequency bands used by IEEE 802.11 is important in ensuring wireless networks are configured correctly provide optimal performance and avoid interference with other devices. Modulation is the process modifying a signal to carry information In the context of IEEE 802.11. The modulation scheme used by 802.11 can vary on the operating frequency, transmission power, and channel conditions. Common modulation techniques used 802.11 include phase-shift keying, quadrature phase-shift keying (QPS), and quadrature amplitude modulation (QAM). These modulation allow for and reliable transmission of data over networks. Antenna types play a crucial role in the IEEE 802.11 architecture as they are used to transmit and receive wireless signals There are multiple types of antennas that are used to serve purposes. Some antennas are designed to provide long-range communication, while are intended to provide high-speed data transfer over short distances. The most commonly used antennas IEEE .11 architecture are omnidirectional and directional antennas. Omnidirectional antennas radio signals in all directions, making them the option when communication needs to multiple directions. In contrast, directional antennas can transmit in only one direction, providing high gain, a limited transmission range. It is important to choose the right type of antenna based on the communication requirements to ensure optimum performance and signal.



9.2 Medium Access Control (MAC)

In the Open Systems Interconnection (OSI) paradigm, the Medium Access Control (MAC) sublayer is located inside the Data Link Layer. In a network where numerous devices compete for a single transmission opportunity, such as a wireless channel or a shared transmission medium like Ethernet, it is responsible for regulating access to the shared communication medium.

When it comes to preventing or fixing collisions (simultaneous transmissions that interfere with one another), the MAC sublayer's main purpose is to offer a fair, efficient, and reliable way for devices to access the medium. MAC protocols vary across network topologies since each network has its own unique set of features and needs.

Examples of typical MAC protocols include:

Typical Ethernet networks use CSMA/CD, or Carrier Sense Multiple Access with Collision Detection. In order to choose the best way to send data, devices must listen to the medium. They wait a random amount of time before retrying if the medium is crowded; this is done to decrease the possibility of collisions.

Wi-Fi (IEEE 802.11 networks) use CSMA/CA, which stands for Carrier Sense Multiple Access with Collision Avoidance. In order to ensure that the transmission channel is clear before data is sent,

devices utilize a method called Request to Send/Clear to Send (RTS/CTS). By letting devices announce their intention to broadcast, collisions may be avoided.

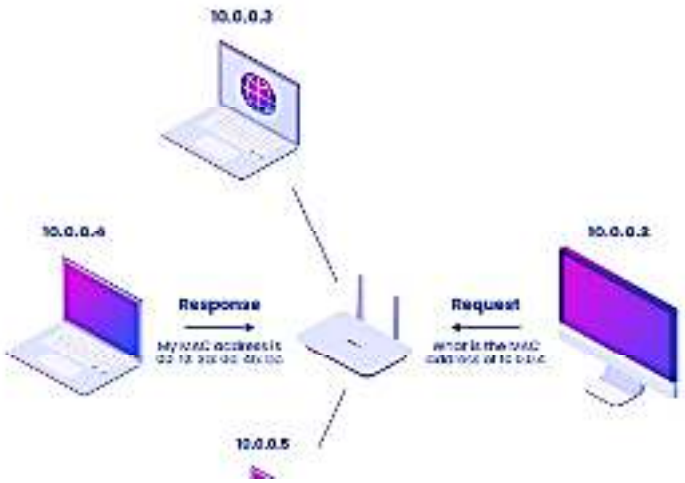
For example, Token Ring networks rely on token passing. In order to authorize a device to send data, it must first get a token from another device in the network. Token-based access controls ensure that only authorized devices may send and receive data.

Time Division Multiple Access (TDMA) is a media access control (MAC) technology used in cellular networks that relies on scheduling. Each device has its own time slot during which it may broadcast, preventing interference from other devices.

Cellular networks like CDMA2000 use CDMA (Code Division Multiple Access). To allow for simultaneous data transmission, each gadget is given a unique code. The intended message is deciphered using the same code used by the sender.

Example: Medium Access Control (MAC) is a sublayer of the Data Link Layer that manages access to shared communication channels, preventing collisions and enabling efficient data transmission in networked environments.

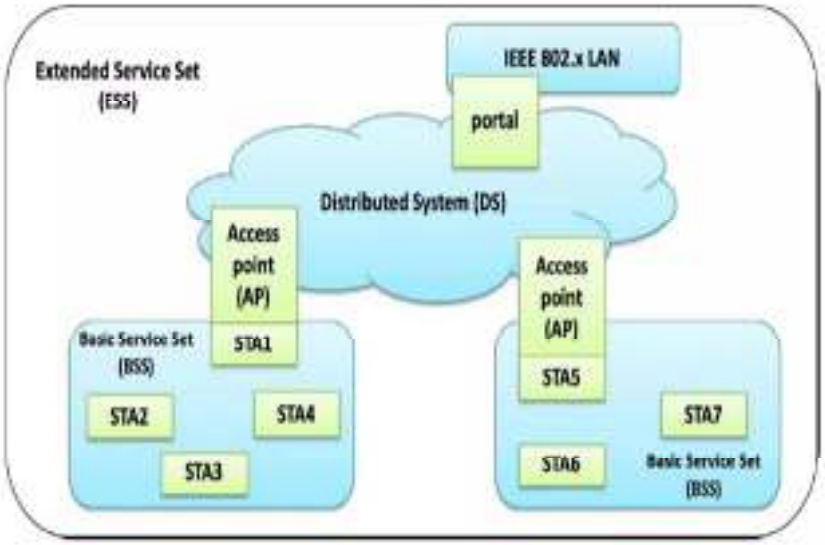
The Medium Access Control is one of the two components of the IEEE .11 architecture, the other the Physical Layer (PHY). MAC layer is responsible for managing access to wireless medium handling the transmission and reception of packets. The MAC layer also supports various types of data traffic, voice, video, and data, and provides mechanisms for QoS (Quality of Service) ensure that different types of traffic are given appropriate levels of on the. Overall, the MAC layer plays a critical role in enabling and efficient communication over wireless networks. The MAC provides such as frame fragmentation, reassembly, and error control, well as handling functions such as authentication and encryption. The layer is composed of a set protocols that define how frames are, received, and acknowledged, including Carrier Sense Multiple Access. The IEEE 802.11 architecture is a set of standards govern wireless LAN technologies and it contains PDU. Protocol Data Unit (PDU) plays a vital in transmitting data packets between devices.



When data is transmitted from one device to, it is encapsulated in a PDU which contains information such as the and destination, frame type, and version. The PDU structure highly standardized, ensuring that devices different can communicate with each other seamlessly. Understanding the PDU structure critical for network administrators and developers working wireless LAN. The IEEE standard defines the Medium Access Control formats for wireless. MAC is responsible for controlling coordinating access to the physical medium between wireless by setting rules for addressing authentication, encryption, and fragmentation data. The 802.11 standard supports different MAC formats which are: Distributed Coordination Function (DCF), Point Coordinator Function (PCF), Coordination Function (HCF), PCF, and Enhanced DCF (EDCF) of these MAC formats serves a purpose and offers different levels performance, efficiency, and priority mechanisms. The IEEE 802.11 architecture consists of two main sub-layers: the Media Access (MAC) sublayer and Physical (PHY) sublayer. MAC sublayer further includes two layers, the Distributed Function and Point Coordination Function (PCF), which are responsible for controlling the access wireless devices to the shared.

9.3 Security Architecture

The IEEE 802. Security Architecture provides a framework for securing wireless communications. It defines for protecting data confidentiality and integrity, as well as authenticating. The security architecture based on the principle of security, where multiple security mechanisms are implemented at different layers of the protocol stack. At the layer, the physical layer mechanisms such as encryption and are used to secure wireless transmissions At the higher layers, protocols such as WPA and WPA2 provide additional security features such as key management and pre-shared key authentication. Security is of utmost importance the IEEE 802.11, as it enables safe of data over wireless networks. absence of proper security mechanisms can render sensitive information to and unauthorized access, leading to data integrity and privacy. Thus, ensuring security in IEEE .11 architecture is crucial for protecting data from potential breaches and. With the rising use of networks, the need for robust measures IEEE 802.11 architecture become a paramount concern for and individuals using this technology. By implementing strong encryption authentication, and access controls, IEEE802.11 architecture can unauthorized access, safeguard data, ensure the integrity and of information exchanged over wireless networks.



IEEE 80211 has several types of security protocols to the safe transmission of data over wireless networks. The original security, Wired Equivalent Privacy (WEP), no longer considered secure. The Wireless Protected Access (WPA) was introduced to replace WEP offering a higher level of protection. Overall, IEEE 802.11 security protocols aim to provide wireless network access by implementing robust features and mechanisms. The IEEE standard provides various security mechanisms to protect wireless networks against unauthorized access The security mechanisms are classified into two categories: authentication and encryption. The IEEE 802.11 standard provides two main encryption mechanisms: Equivalent Privacy (WEP) Wi-Fi Protected Access (PA). The WEP encryption mechanism is now considered insecure and has been replaced by the WPA its later versions: WPA and WPA3. WPA and WPA2 mechanisms use Temporal Key Integrity Protocol (IP) and Advanced Encryption Standard (AES) algorithms. The WPA3 introduces additional security features, including forward secrecy and protection against brute-force attacks.

9.4 Quality of Service (QoS) Architecture

The Quality of Service (QoS) Architecture is an important in the IEEE 802.11 standard. It defines the for prioritizing different types of traffic, ensuring that data is, stable, and efficient. QoS Architecture includes service classes, each with own priority level and associated traffic characteristics. These service classes allow network to allocate bandwidth and manage traffic flow based on the specific needs different applications such as real-time multimedia or interactive gaming. The QoS also includes mechanisms for managing congestion and controlling access the medium. Together, these features help ensure that wireless networks can a wide range of high-quality applications, even in challenging environments with high levels of interference congestion. The objectives of Quality of (QoS) in IEEE 802.11 are to the overall performance of wireless networks prioritizing data and allocating network resources based on the specific needs of different types of traffic protocols in

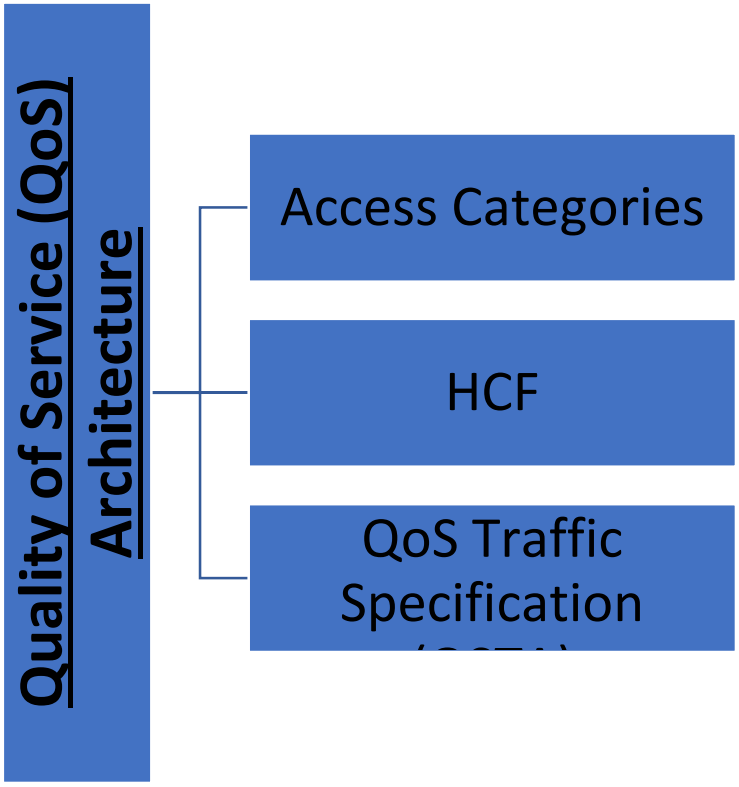
802.11 aim to certain levels of service for real-time traffic, like voice and video, while also maintaining fairness and equality for all users. The IEEE architecture includes different QoS protocols, such as Wi-Fi Multimedia which classifies and prioritizes based on its type and more efficient use of network resources. Different methods are used to ensure quality of service. These methods include-based and contention-free access modes, along mechanisms. Contention-based modes enable nodes to share wireless and compete for access to it.

The QoS architecture of IEEE 802.11e consists of three main components:

Access Categories (ACs): ACs are used to differentiate between different types of traffic, such as voice, video, and data. Each AC has a different priority, and traffic in a higher-priority AC will be given more bandwidth than traffic in a lower-priority AC.

HCF: HCF is a new coordination function that is used to manage the access to the medium for different ACs. HCF provides a number of features that are not available in the Distributed Coordination Function (DCF), such as bandwidth reservation and traffic prioritization.

QoS Traffic Specification (QSTA): QSTAs are used to inform the access point (AP) of the QoS requirements for a particular flow of traffic. The AP can use this information to make scheduling decisions and to ensure that traffic is delivered with the desired QoS.



On the other, contention-free access assign time slots for individual nodes transmit data, eliminating contention ensuring equal access. Prioritization mechanisms nodes to prioritize certain types traffic over others, ensuring that traffic is given higher priority. Overall, these methods work together to that QoS is maintained within IEEE 802.11 despite the challenges posed by wireless. The IEEE 802.11 Architecture is a accepted standard for wireless networking outlines the requirements for physical and link layers of wireless communication. The points of this architecture include of wireless access points and a variety of security protocols such as Wi-Fi Protected Access (WPA) and Wi-Fi Protected II (WPA2). Overall, IEEE 802.11 Architecture serves as a for creating reliable, scalable, interoperable wireless networks.

Summary

- In this unit the concepts of wireless local area network were discussed
- The discussion about the transmission technology behind the wireless local area network was discusses.
- The explanation of Infrared LAN and its configurations was done.

- In this chapter the spread spectrum LAN was discussed.

Keywords

WLAN - Wireless local area network

AP - Access point

CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance

CSMA/CD - Carrier Sense Multiple Access with Collision Detection

WECA - Wireless Ethernet Compatibility Alliance

WPAN - Wireless Personal Area Networking

WWAN - Wireless Wide Area Networking

IrDA - Infrared Data Association

BSA – Base service area

IR - Infrared

Self Assessment

1. What does the term "Wi-Fi" stand for?

A. Wireless File Transfer
B. Wireless Fidelity
C. Wireless Internet Connection
D. Wireless Network Protocol

2. Which organization is responsible for defining and managing the IEEE 802.11 standards?

A. IEEE (Institute of Electrical and Electronics Engineers)
B. Wi-Fi Alliance
C. FCC (Federal Communications Commission)
D. ITU (International Telecommunication Union)

3. Which of the following frequency bands is commonly used for Wi-Fi communication?

A. 2.4 GHz and 5 GHz
B. 900 MHz and 3.5 GHz
C. 1.8 GHz and 4.2 GHz
D. 6 GHz and 60 GHz

4. In the context of Wi-Fi, what is SSID?

A. Secure Signal Identifier
B. Service Set Identifier
C. Signal Strength Indicator
D. Security Service Identifier

5. Which IEEE 802.11 standard introduced the use of the 5 GHz frequency band for Wi-Fi?

A. 802.11a

B. 802.11b

C. 802.11g

D. 802.11n

6. Which of the following encryption protocols is commonly used to secure Wi-Fi networks?

A. WEP (Wired Equivalent Privacy)

B. WPA (Wi-Fi Protected Access)

C. SSL (Secure Sockets Layer)

D. IPsec (Internet Protocol Security)

7. Which IEEE 802.11 standard supports the highest data rates and multiple input, multiple output (MIMO) technology?

A. 802.11a

B. 802.11g

C. 802.11n

D. 802.11ac

8. What is the maximum theoretical data rate of an 802.11ac Wi-Fi network using multiple spatial streams?

A. 54 Mbps

B. 150 Mbps

C. 300 Mbps

D. 1.3 Gbps

9. Which channel bonding technique allows 802.11n and 802.11ac devices to use adjacent channels to increase bandwidth?

A. WPS (Wi-Fi Protected Setup)

B. WEP (Wired Equivalent Privacy)

C. DFS (Dynamic Frequency Selection)

D. HT (High Throughput) mode

10. Which IEEE 802.11 standard was specifically designed for IoT (Internet of Things) devices with low power and data rate requirements?

A. 802.11a

B. 802.11ah

C. 802.11ac

D. 802.11n

11. Which IEEE 802.11 standard operates primarily in the 60 GHz frequency band and is known for its high data transfer rates over short distances?

A. 802.11a

B. 802.11ac

C. 802.11ad

D. 802.11n

12. What is the purpose of the Wi-Fi Alliance in the context of Wi-Fi technology?

A. To define and manage IEEE 802.11 standards
B. To regulate Wi-Fi usage in public spaces
C. To certify interoperability of Wi-Fi devices
D. To allocate IP addresses for Wi-Fi networks

13. Which of the following is a common security method used in Wi-Fi networks to protect against unauthorized access by verifying a user's identity?

A. MAC filtering
B. WPS (Wi-Fi Protected Setup)
C. WEP (Wired Equivalent Privacy)
D. WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key)

14. In a Wi-Fi network, what does the term "Roaming" refer to?

A. Connecting to a Wi-Fi network for the first time
B. Moving between different Wi-Fi channels
C. Moving between access points without losing network connectivity
D. Turning off Wi-Fi on a device

15. Which IEEE 802.11 standard introduced the concept of beamforming, which allows Wi-Fi devices to focus signals toward specific clients for improved performance?

A. 802.11a
B. 802.11n
C. 802.11ac
D. 802.11ax

Answers for Self Assessment

1.	B	2.	A	3.	A	4.	B	5.	A
6.	B	7.	D	8.	D	9.	D	10.	B
11.	C	12.	C	13.	D	14.	C	15.	C

Review Questions

1. Explain the key differences between the 2.4 GHz and 5 GHz frequency bands used in Wi-Fi networks. What advantages and disadvantages does each band offer in terms of wireless communication?
2. Describe the role and significance of the Wi-Fi Alliance in the context of Wi-Fi technology. How does the Wi-Fi Alliance contribute to the development and standardization of Wi-Fi devices and technologies?
3. Discuss the evolution of Wi-Fi security protocols from WEP to WPA3. What were the security shortcomings of earlier protocols, and how have newer protocols improved security in Wi-Fi networks?

4. Explain the concept of "roaming" in Wi-Fi networks. What challenges does seamless roaming address, and what mechanisms or protocols are commonly used to facilitate roaming between different access points?
5. Describe the technology behind beamforming in IEEE 802.11ac Wi-Fi networks. How does beamforming work, and what benefits does it provide in terms of wireless signal quality and coverage?
6. Compare and contrast the IEEE 802.11ac and IEEE 802.11ax standards. What are the key features and improvements introduced by each standard, and how do they address the growing demands of modern wireless communication?

Further Readings

- Wireless communications & networks by William Stallings, Pearson
- Principles of wireless networks by Kaveh Pahlavan, Pearson
- Fundamentals of wireless networking by Ron price, McGraw hill education
- Wireless networks first-step by Jim Geier, cisco press

Web Links

http://59.51.24.50:8000/wxwl/Wireless_Communications_&_Networking_Stallings_2nd.pdf

Unit 10 : Wireless LAN Standards

CONTENTS

Objectives

- Understanding the 802.11 physical layer uses.
- Analyze the various devices used in the 802.11 Architecture.
- Understanding the difference among routers and access points.
- Analyzing the revolution of WPA security standard.

Introduction

The original 802.11 standard for the physical layer describes two types of spread spectrum modulation: direct sequence and frequency-hopping spread spectrum, also called 802.11 FHSS . For these two needs, the data transfer speed needs to be either 1 or 2 Mbps, and the operating frequency needs to be 2.4GHz. Another first physical layer uses passive infrared reflection to send data at 1 or 2 Mbps, even though this standard hasn't been used in any devices yet. Late in 1999, the IEEE said that the 802.11a and 802.11b improvements to this 802.11 standard were ready to be used. The 802.11a standard sets a maximum data transfer rate of 54 megabits per second. This is done by using orthogonal frequency division multiplexing modulation in the 5.8GHz frequency range. IEEE 802.11b is the version of the standard that lets you use the 2.4GHz band and has faster data transfer speeds of between 5.5 and 11Mbps. This new standard has increased the amount of data that can be sent over the original 802.11 DSSS. Most businesses today use 802.11b-based systems to build wireless local area networks. Radios that use the 802.11 DSSS standard can connect to 802.11b access points. Radios that use the 802.11 FHSS standard, on the other hand, can only connect to 802.11a access points.

10.1 IEEE 802.11 Architecture

The physical layer architecture of IEEE 802.11 has the following components –

Stations (STA)-

In the language of IEEE 802.11 (Wi-Fi), a station, which is also referred to as a STA, is a piece of hardware that is capable of utilizing the 802.11 protocol. Stations can take many forms, such as a laptop computer, desktop computer, personal digital assistant (PDA), access point, or Wi-Fi phone. A STA can either remain in one location, move to a new location, or be taken with you. Because there is no obvious distinction between the three, the terms "station," "wireless client," and "node" are frequently used interchangeably when discussing wireless networking. A station may be referred to as either a transmitter or a receiver, depending on the manner in which it transmits information. Any device that is compliant with IEEE 802.11 and has an interface to the wireless medium that is both media access control and physical layer is considered to be a station according to IEEE 802.11-2007. A station can be classified into two different types.

Wireless Access Points

Access points, commonly known as APs, are a wireless local area network solution that is safe, affordable, and simple to use. They satisfy the requirements of networking experts by combining portability and adaptability with enterprise-level functionality. Access points are Wi-Fi certified and, depending on the model, are compatible with the 802.11a, 802.11b, 802.11g, 802.11n, and 802.11c standards. An access point is the hub of a wireless network that operates independently, as well as the location where wireless and wired networks are able to communicate with one another. Users using wireless technology in large-scale deployments are able to walk freely across a building while remaining connected to the network as long as they are within radio range of an access point. This is possible because access points are equipped with radio antennas. There is either one, two, or three radios located on each platform that makes up an access point. In order to extend the range of your infrastructure or get around a barrier that prevents radio transmission, you can configure an access point to function as a standalone repeater. The repeater is responsible for moving traffic between the wired LAN and wireless users. This is accomplished by sending packets to either a different repeater or an access point that is connected to the wired LAN.

Differences of Access points from Routers

People today have access to a diverse assortment of tools, gadgets, and home appliances as a result of the rapid advancements that have been made in computer technology. Because there are so many different kinds and categories of computer hardware, it is possible for regular people to become perplexed by the complexity of each individual tool or gadget. In fact, there are so many different kinds and categories of computer hardware. These two devices, in addition to the primary distinctions that separate them from one another, have a few additional subtle distinctions that are nonetheless significant.

Router

A router is a type of network equipment that creates a regulated local area network by connecting many computers, cellphones, tablets, and other devices to one another. It also provides Internet access to all of the connected devices that are suited for doing so. Establishing a router and then connecting one or more devices to it is the first step in establishing a local area network, abbreviated as LAN. Today's users have the option of connecting their devices to routers either wirelessly or by utilizing Ethernet cables (using Wi-Fi).In order to send and receive data to and from the devices in the local area network, the router has to be linked to the customer premises equipment of an Internet service provider over an Ethernet connection. Only then will the router be able to do so.

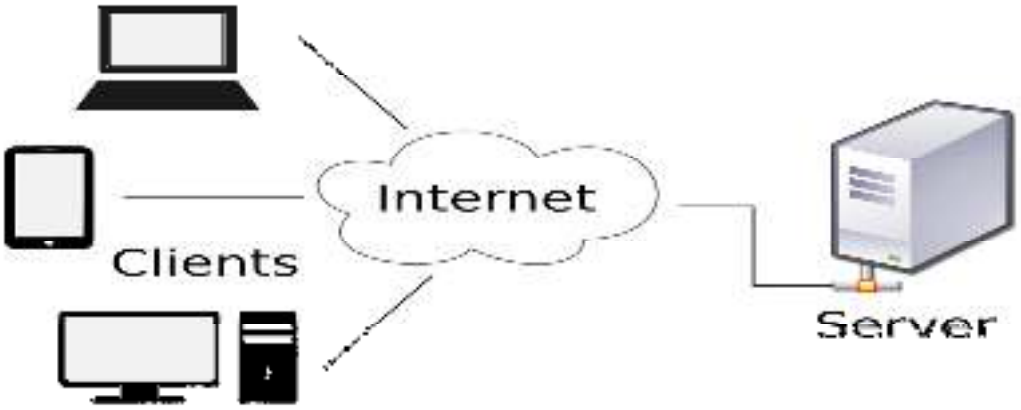
Access Point

An access point is a piece of hardware for a wireless network that allows devices to join to a local area network. Access points are also known as wireless access points. Access points are used to expand the amount of territory that may be covered by a wireless network as well as the number of users that can join to the network at once. A wired signal may be converted into a wireless one by connecting a router to an access point with a high-speed Ethernet connection. This transforms the wired signal. The vast majority of access points only offer wireless connections, and they make use of Wi-Fi in order to establish connections with end devices.

The router not only creates a local area network, but it also manages all of the connected devices and the manner in which they communicate with one another. On the other hand, an access point is a component of a local area network that not only enables additional devices to connect to the network but also provides those devices with an additional location from which they can connect to the network. There is no such thing as an access point that cannot function as a router; nevertheless, not every access point is also a wireless router. In most cases, you will only be able to join to the network that the router has already established if you use an access point. On the other hand, routers are responsible for managing local area networks, connecting to other network systems, collecting, distributing, and sending data in many different ways, establishing a point of contact, and maintaining security.

Client

Clients are a piece of computer hardware or software that establishes a connection to a service that is made available by a server is referred to as a client. The client-server paradigm of computer networks includes this aspect of the model. When the client needs to access the service across a network since the server is often located on a different computer system (although this is not always the case). A computer or program is considered to be a client when it accesses a service offered by a server through the utilization of a different program, item of computer hardware, or item of software. Web browsers, for instance, are examples of clients since they connect to web servers in order to retrieve web pages that may be displayed. Email clients get emails from mail servers. Different clients are utilized for online chat, and the particular clients that are utilized is determined by the chat protocol that is utilized. A customer may be participating in a multiplayer or online video game on each computer in the establishment. The term "client" can refer to both the individuals who utilize client software as well as the computers and other pieces of gear that are used to execute client software. Clients are an essential part of the client-server model, which is still widely employed today. Inter-process communication is a method that allows computer programs that are running on the same system as clients and servers to communicate with one another. Clients and servers both use the same system. Through the use of the Internet protocol suite and Internet sockets, programs are able to connect to a service that is operating on a system that may be located in another location. The servers are waiting for potential clients to open connections before they can accept them as new customers. The word was initially used to refer to hardware that could connect to a network and communicate with other computers, but the devices themselves were unable to execute their own programmers independently. People who shared time on the mainframe computer would use these terminals to access the machine.



Thick clients, thin clients, and diskless nodes are the three distinct categories of client computers and devices.

Thick Clients

A client that does the majority of the data processing on its own and does not always require assistance from the server is referred to as a thick client. This type of client is also referred to as a rich client or a fat client. A personal computer is an excellent example of a fat client since it has a lot of features and capabilities and doesn't require much assistance from a server. This makes the personal computer a good example of a fat client. A machine that runs an art application such as Krita or Sketchup and then shares the results of its work across a network is referred to as a thick client. A computer known as a workstation is one that is capable of performing practically any task on its own, with the exception of transmitting and receiving data across a network.

Thin Clients

The most fundamental type of client is known as a thin client. Thin clients are clients that make use of the resources provided by the host machine. The vast majority of the time, a thin client does little more than display data that has already been handled and transmitted by an application server, which is responsible for the majority of the necessary data processing. "Thin client" refers to a piece of hardware that runs web-based programs, such as Microsoft's Office Web Apps.

Diskless systems

The two different kinds of clients described above are integrated into one within a diskless node. It operates locally, just like a fat client would, but keeps all of its data on the server instead. This approach incorporates aspects of both the thin client and the fat client, namely support for multimedia applications and a focus on high performance, respectively (high manageability, flexibility). One example of a system that is considered to be diskless is one that can play the online version of the video game Diablo III. Another classification of the clients done with respect to the movement of the clients. The two classifications are fixed clients and mobile clients. Fixed clients are like desktop computers ,servers ,Networked Printers etc. they do not change their location frequently. On the other hand, mobile devices are like Laptops, Smartphones, PDA's, Tablets, IOT devices etc.

10.2 Infrastructure of 802.11

The architecture of the IEEE 802.11 WLAN was designed to function properly inside a network in which mobile stations were responsible for the majority of the decision-making. There are several positive aspects to this type of structure. It eliminates the bottlenecks that can be caused by a centralized design and continues to function normally even if a WLAN device fails. The adaptable architecture is able to readily accommodate a wide variety of network configurations, including

fleeting, temporary, semi-permanent, and even permanent ones. Even if it does not influence the mobile devices' capacity to connect to networks, the design and protocols have a significant role in determining how much power mobile devices consume and how long their batteries continue to function.

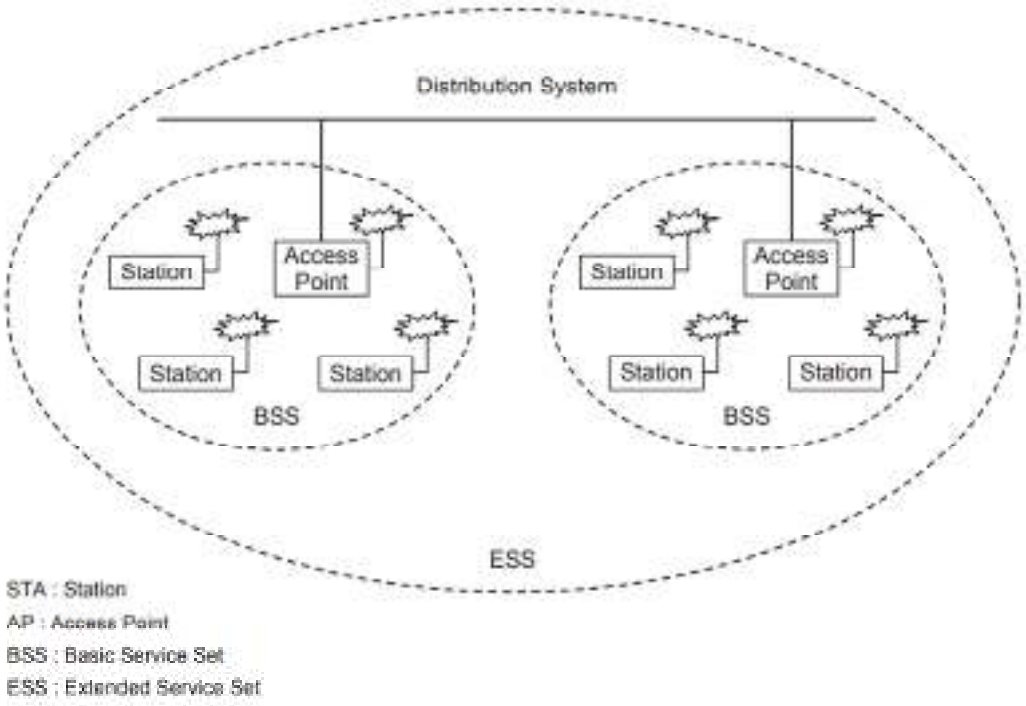
The IEEE 802.11 standard discusses two distinct types of network designs, which are as follows:

Infrastructure network: An infrastructure network is a sort of network that enables wired and wireless clients to communicate with one another. Infrastructure networks also allow for the sharing of network resources. When moving data from a wireless connection to a wired connection, an access point is required. The coverage area is determined by an access point (AP) in conjunction with the wireless clients that it is linked to.

Point-to-point networks: These are often known as ad-hoc networks, are a form of network architecture that enable wireless clients to communicate directly with one another. The vast majority of the time, an ad-hoc network is thrown together on the fly, and it is unable to connect to wired networks. An access point is not required for use with an ad-hoc network.

The independent basic service set (IBSS), the basic service set, and the extended service set are the three fundamental topologies that are supported by the IEEE 802.11 standard for WLANs (ESS). Implementations of the integrated basic service set, enhanced service set, and enhanced service set configurations can be supported at the MAC layer.

IBSS: These are the configurations that are also called ad-hoc networks or independent configurations. An IBSS can be set up like a peer-to-peer office network, where it's not necessary for any one node to act as a server. IBSS wireless local area networks (WLANs) are made up of a number of nodes or wireless stations that can talk to each other peer-to-peer and ad hoc. IBSS systems usually only work in a small area and aren't linked to any large networks. An IBSS is usually a network that is made for a specific purpose, has a small number of stations, and only lasts for a short time.



Basic service set: An access point (AP) serves as the logical server for a single WLAN cell or channel when the basic service set is configured. The only channels for legitimate communication between stations 1 and 4 are those leading from station 1 to AP1, from AP1 to AP2, from AP2 to AP4, and finally from AP4 to station 4. An access point creates a connection between a wired LAN in a corporation and a WLAN cell. Additionally, it may link numerous WLAN cells or channels by performing the function of a bridge.

Extended service set: A wired or wireless distributed system is used to connect the numerous basic service set cells that come together to form the ESS configuration. ESS configurations are available for IEEE 802.11, and they allow several cells to share the same channel. This results in an increase in the network's overall throughput. The ESS seems to be a single MAC layer network in which all stations are physically still to equipment that is external to the ESS, as well as to the ESS itself and all of its mobile stations. Therefore, the ESS is able to conceal the mobility of the mobile stations from anything and everything that is not part of the ESS.

The following categories of stations can be found in the ESS:

IEEE 802.11 classifies wireless stations into one of three categories according to their degree of mobility within a wireless local area network:

1) Lack of mobility in transition: A station is said to lack mobility in transition if it is unable to move at all or if it can only move inside a BSS.

2) BSS Transition Mobility: A station that possesses BSS Transition Mobility is able to transfer between BSSs while remaining in the same ESS; this is a unique ability.

3) ESS transition mobility: A station that possesses ESS transition mobility has the ability to switch between different ESSs. Nevertheless, IEEE 802.11 does not guarantee that the station will remain connected even if it moves.

10.3 WPA (Wi-Fi Protected Access)

Over the course of the past year, the Wi-Fi Alliance has been at the forefront of efforts to develop a standards-based interoperable security protocol. This would provide a significant improvement to the data security as well as the management of access for wireless local area networks that use Wi-Fi. That the protocol that is used for Wi-Fi Protected Access (WPA).

The first native security solution for WLANs, known as Wired Equivalent Privacy, has been in use since the IEEE 802.11 standard was published in 1997. WPA addresses the weaknesses that WEP possesses. By 2001, the cryptographic weaknesses in WEP were well knowledge among everyone. Multiple independent research conducted by academic and corporate organizations have come to the conclusion that an adversary armed with the appropriate tools and a fundamental grasp of technology is capable of breaking into a WLAN that has WEP enabled. In spite of the fact that WEP has a few flaws, using it rather than having no security at all is still preferable. Even in settings where there isn't a lot of network activity, such as the house or a small office/home office , it can assist prevent individuals from listening in on conversations that are taking place. However, the standard for commercial success was not met. Combining WEP with other third-party security tools such as virtual private networks (VPNs), 802.1X authentication servers, and other proprietary technologies enabled many large companies to increase its level of protection and make it more widely used. The Wi-Fi Alliance and the IEEE have begun collaborating on a project with the goal of developing an improved, standards-based, and interoperable Wi-Fi security solution. They did this because they were concerned that consumers would have a more difficult time purchasing Wi-Fi devices if there was not a robust native wireless security option available.

The solution is the WPA. WPA is able to secure all 802.11 devices, including those that are multi-band and multi-mode, such as 802.11b, 802.11a, and 802.11g devices. One of the many subsets that make up WPA is the soon-to-be-approved IEEE standard 802.11i, which is also known as WPA2 and is scheduled for approval in the first quarter of 2004. Therefore, it is compatible with WPA2 in both the present and the future. WPA should operate perfectly with WPA2 devices when they become available, and it will continue to be an excellent option for commercial use for many years to come. WPA ensures the safety of wireless networks by using a robust new encryption mechanism and user authentication, two features that WEP was largely lacking. When it is properly configured, it provides users with a great deal of assurance that the data they save on their devices will be secure and that only authorized users will be able to access the network. Enterprises are able to provide their workers with the freedom and convenience of working wirelessly while keeping them safe when WPA is turned on. This eliminates the need for businesses to implement additional security measures such as VPNs.Strong network security is accessible to all users, including both small office and home office (SOHO) users and business users. Wireless Internet Service Providers

(WISPs) may find that these schemes are also appealing in public "hot spots" because WPA's improved encryption and authentication methods offer a high level of security for service providers and mobile customers who aren't using VPN connections. This is because WPA's improved encryption and authentication methods offer a high level of security for service providers and mobile customers who aren't using VPN connections.

10.4 Need of WPA

WPA addresses all of the known flaws in WEP, making it far more secure for use with wireless data. LANs and safeguard users from hacking attempts of even the highest level of expertise. It is designed to have as minimal of an impact as possible on the performance of the network, and it is intended to act as an upgrade to the more recent version. Wi-Fi Certification has been achieved by more than 650 different devices at this point. Cryptologists have examined Wi-Fi Protected Access and discovered that it is both effective at what it claims it would do and a formidable barrier to entry for potential hackers. It addresses every known vulnerability in the WEP protocol known infractions. WPA encrypts data via the Temporal Key Integrity Protocol (TKIP), and it leverages one of the most widespread kinds of 802.1X authentication that are available right now. Both of these protocols were developed by the National Institute of Standards and Technology .

WPA may be added to the software of virtually all new devices as an upgrade to the existing software. Wi-Fi devices. Software is essential to the operation of access points (APs) upgrade. It is necessary to update the software that is found on client workstations' network interface cards , and it is possible that the software for the operating system will also need to be updated. Authentication servers are going to be necessary for businesses (usually a Remote Authentication Dial-In server or User Service). Users in private homes and small offices or home offices (SOHOs), who do not have access to these servers, are given a special means to activate WPA by making use of a shared password using WPA. WPA products are currently being certified by the Wi-Fi Alliance. It is anticipated that shipments will begin in the middle of the year, and a number of other goods will follow shortly after. Wi-Fi CERTIFIED will provide the WPA security protocol as an option. When things were first being put into use but had not yet reached their full potential. Your device's Wi-Fi certification badge will provide information about the type of WPA encryption that it employs. WPA will replace WEP as the default security protocol in all newly developed WiFi hardware and software. There are certain PC devices that will require certification for Wi-Fi till the conclusion of the year 2003.

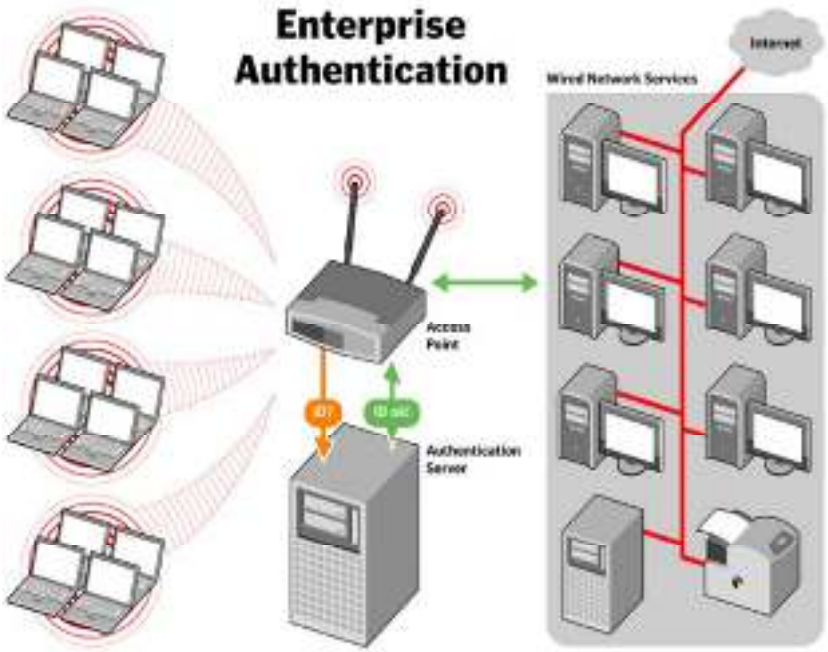
One of the most significant shortcomings of WEP was that it began the encryption process with a relatively simple static key. This 40-bit key has to be manually entered on the access point as well as on every client that communicates with the access point. It won't change unless it's put in again by hand on every device, which is difficult to do in a large company where there are many devices. Studies in cryptography have shown that there are three different ways in which hackers can cause damage to a WEP network: by intercepting and decrypting data that is being sent over the air, by changing the data that is being sent, or by figuring out the WEP key and making a fake one in order to gain unauthorized access to the network and Internet services. This could be accomplished in a matter of hours using a busy business WLAN. WEP does not have a method for checking the credentials of a user, which means that it cannot guarantee that only those who are authorized to access the network will be able to do so. WPA is a security protocol that not only addresses these issues but also adds additional safeguards to Wi-Fi. WPA, which uses a protocol called Temporal Key Integrity Protocol, is a significantly superior method for encrypting data. TKIP employs a key structure that results in significantly increased levels of security when used in conjunction with 802.1X/EAP authentication. Additionally, it possesses a MIC to prevent packets from being altered in any way.

10.5 Authentication Process in WPA

One of the currently available EAP types is used for authentication in WPA networks that employ 802.1X. Based on the ports, 802.1X is a method that may be used to manage access to wired as well as wireless networks. That particular year, in August, the IEEE adopted it as a standard. EAP is responsible for managing the presentation of user credentials, regardless of whether those credentials are secure IDs, smart cards, secure usernames and passwords, or any other sort of identification credential that is acceptable to the IT administrator. It is also possible to make use of digital certificates, which are utilized extensively already to maintain security on the internet. You

have options available to you under WPA regarding the sort of EAP to use as well as the credentials to utilize. Protected Extensible Authentication Protocol (PEAP), EAP-Tunneled Transport Layer Security (EAP-TTLS), and EAP-Transport Layer Security are some examples of standards-based EAP implementations that may be utilized (EAP-TLS).

The foundation for mutual authentication between client workstations and the authentication server is laid by 802.1X and EAP. Through the use of a process known as mutual authentication, network administrators may be certain that only authorized users are accessing the system. Additionally, it prevents users from connecting to "rogue" or illegal access points (APs) on the Wi-Fi network by mistake. When a user wishes to log into the network, the client will transmit the user's credentials to the authentication server by way of the AP. If the server validates the user's credentials, then the master TKIP key is communicated to the client as well as the access point. A four-way handshake is performed to conclude the procedure. During this step, the client and the AP acknowledge each other and install the keys.



Summary

- In this Unit we have covered the architecture of 802.11 standard.
- The concepts behind the physical layer of 802.11 standard was discussed.
- The topics of discussion included the various devices used in the infrastructure of 802.11.
- The usage and need of WPA security was discussed.
- The basic differences between the routers and access points were discussed in the unit.

Keywords

FHSS- Frequency hopping spread spectrum

FDMA- frequency division multiple access

STA- Station

MAC- Media access control

PHY -Physical Layer

LAN – Local area network

CPE- Customer premises equipment

WLAN – Wireless local area network

AP- Access Point

IBSS – Independent basic service set

ESS- Enhanced service set

WEP – Wired equivalent privacy

WAP- Wi-fi protected access

VPN – Virtual private network

WISP- Wireless internet service provider

TKIP- temporary key integrity Protocol

NIST – National institute of standards and technology

NIC – Network interface cards

MIC- Message Integrity Check

EAP - Extensible Authentication Protocol

PEAP - Protected Extensible Authentication Protocol

Self Assessment

Q1) Which type of connection WPA security used?

A. Ethernet
B. Bluetooth
C. Wi-Fi
D. Infrared

Q2) What is the highest signaling rate if the frequency range if 5GHz in a 802.11a standard?

A. 11 Mbps
B. 1 Gbps
C. 22 Mbps
D. 54 Mbps

Q3) Out of the following which is the best standard for the vehicular communication ?

A. IEEE 802.11a
B. IEEE 802.11p
C. IEEE 802.11g
D. IEEE 802.11h

Q4) The integrity and security of the signal is preserved by using technique called.

A. Spread Spectrum
B. FHSS
C. DSSS
D. All of the above

Q5) Which of the following specifies WLAN security standard?

A. IEEE 802.11a

B. IEEE 802.11i
C. IEEE 802.11g
D. IEEE 802.11h

Q6) What are the two main types of Access control lists.

A. Standard and Extended
B. IEEE and Specialized
C. Standard and Specialized
D. None of the above

Q7) Which multiple access technique is used in the 802.11 standard?

A. CDMA
B. CSMA/CA
C. ALOHA
D. TDMA

Q8) In IEEE 802.11 the access method used in PCF sublayer is called?

A. Contention
B. Controlled
C. Polling
D. None of the above

Q9) What is the main use of the access point ?

A. Allow the wireless devices to connect the wired network
B. It is a wireless device
C. It is a intermediate device between router and host
D. None of the above

Q10) In ad-hoc networks

A. Access points are not needed
B. Access points are a necessity
C. Nodes are not required
D. Every node acts as a access point

Q11) In the wireless infrastructure

A. Multiple number of access points are connected with each other
B. No access points are needed
C. Only one access point is required
D. Host is an access point

Q12) The controller in the wireless network works in a _____ mode.

A. Infrastructure mode

B. Ad-hoc mode
C. Both infrastructure mode and ad hoc mode
D. WDS mode

Q13) In wireless network an extended service set is a set of _____

A. connected basic service sets
B. all stations
C. all access points
D. connected access points

Q14) Mostly _____ is used in wireless LAN.

A. time division multiplexing
B. orthogonal frequency division multiplexing
C. space division multiplexing
D. channel division multiplexing

Q15) What is Wired Equivalent Privacy (WEP)?

A. security algorithm for ethernet
B. security algorithm for wireless networks
C. security algorithm for usb communication
D. security algorithm for emails

Answers for Self Assessment

1.	C	2.	D	3.	B	4.	D	5.	B
6.	A	7.	B	8.	C	9.	A	10.	A
11.	A	12.	C	13.	A	14.	B	15.	B

Review Questions

1. Write and explain the difference between router and the access point.
2. Explain how the WEP and WPA are different for one another.
3. Compare and contrast the functionality of BSS and ESS in detail.
4. Explain the functionality of WPA authentication process in detail.
5. Elaborate the various components in Wireless infrastructure.
6. Explain the need of WPA security in detail .

Further Readings

- Wireless communications & networks by William Stallings, Pearson
- Principles of wireless networks by Kaveh Pahlavan, Pearson

- Fundamentals of wireless networking by Ron price, Mcgraw hill education
- Wireless networks first-step by Jim Geier, cisco press

Web Links

- https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-next-generation-of-wi-fi-security
- https://www.cs.kau.se/cs/education/courses/dvad02/p1/Papers%20Wireless/Wi-Fi%20Protected%20Access%20-%20Whitepaper.pdf
- https://www.rroij.com/open-access/securing-the-control-frames-in-wirelessnetwork.pdf

Unit 11: Introduction to Mobile Middleware

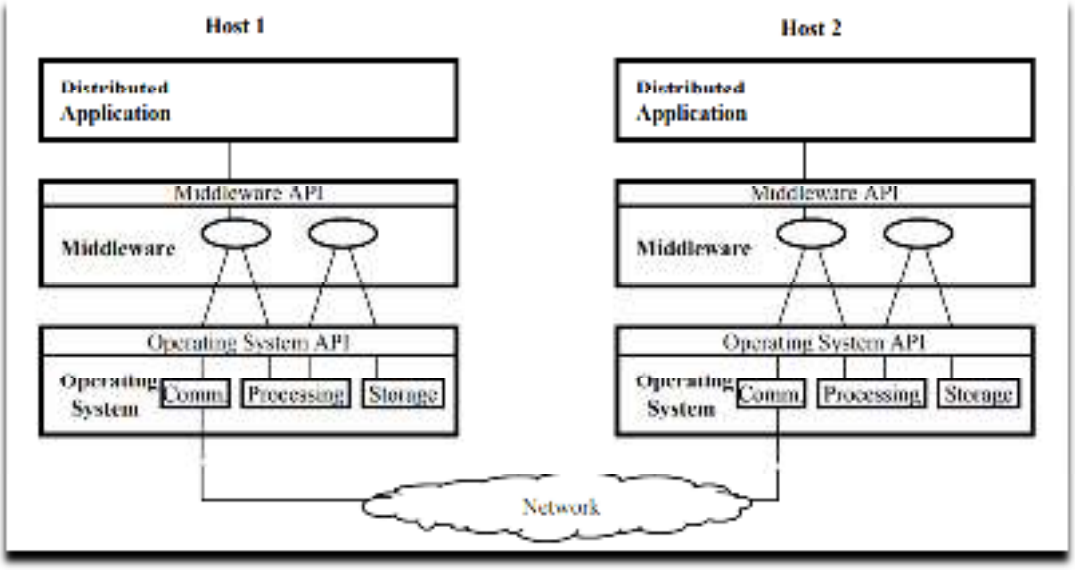
CONTENTS

Objectives

- Understanding the types of mobile middleware.
- Analyzing the differences between the types of the middleware.
- Understanding the middleware and various convergence concepts.
- Analyzing the adaptability of the middleware.
- Evaluate the service discovery middleware. .

Introduction

The term "middleware" refers to a collection of software technologies that can assist in the management of the complexity and various types of software that are inherent to distributed system architectures. As can be seen in Figure below , the common programming abstraction of a distributed system is provided by a layer of software that is placed above the operating system but beneath the application program. This layer of software is known as the middleware. One example of a programming building block that is more difficult to understand is the socket, which stands in contrast to the Application Programming Interfaces provided by operating systems. Application programmers won't have to deal with the tedious and error-prone programming anymore, which means they'll have significantly less work to do. Middleware is sometimes referred to informally as "plumbing" because of its role in connecting various components of a distributed application via data pipes and then transferring data between those components.



Middleware frameworks are designed to conceal a number of the complexities that are necessary for programmers working on distributed systems to manage. They consistently obscure the reality that hardware and networks are distinct from one another. The majority of software frameworks for middleware also conceal the fact that either programming languages or operating systems are distinct, or both. Some of them, like CORBA, also obscure the reality that various middleware suppliers might implement the same standard in different ways. In conclusion, the programming abstractions provided by middleware have the potential to clarify distribution in at least one of the following ways: location, concurrency, replication, failures, mobility, and mobility.

An operating system is "the software that makes the hardware operate," which is the meaning of the term. The ability to write programs for a distributed system is provided by middleware, which functions similarly to software in this regard. Programming a distributed system is typically significantly more difficult when middleware is not there, particularly in situations in which the system must function in a variety of ways. This is analogous to the difficulty that one could experience while trying to program a computer that does not have an operating system. Even though it is possible to write code for an application in an assembly language or even in machine code, the majority of programmers believe that writing code in a higher-level language is much faster and makes the code more portable. Even though it is possible to write code for an application in either of these languages.

11.1 Types of the Middleware

The production of middleware has, up until this point, only taken a few distinct forms. These are distinct from one another, in terms of the programming abstractions and heterogeneity they provide, both of which are independent of the network and the hardware.

Distributed Tuples

The most frequent type of middleware that is used in modern times is a distributed relational database It gives a representation that is abstract of distributed tuples. Its SQL which is based on set theory and predicate calculus, provides programmers with the ability to manage sets of these tuples (a database) in a language that is akin to English but still makes sense. In the context of relational databases that are distributed, a transaction may also be seen as an abstraction. The majority of distributed relational database systems often do not provide much, if any, distinction in how they are implemented by different vendors; nevertheless, they frequently do offer variances in how they are implemented by different programming languages. Transaction Processing Monitors, or TPMs, are commonly utilized to supervise client queries, transactions that take place across various databases, and server-side operations.

Tuple Space is an abstraction of distributed tuples that is made available via a framework that goes by the name Linda (TS). Accessing TS in an associative manner is possible using Linda's Application Programming Interface (API), but there is no relational meaning. By ensuring that the processes of depositing and withdrawing money are conducted in complete secrecy from one another, Linda ensures that geographical decoupling is achieved. Temporal decoupling occurs when their lives no longer intersect with each other in any significant way.

Jini is a Java framework for intelligent devices, particularly those that are employed in the domestic setting. Jini is built on Linda's TS, which is quite comparable to JavaSpaces. Jini was developed by Linda.

Remote Procedure Call

The interface for making procedure calls—known as remote procedure call, or RPC; see Remote Procedure Calls—is expanded with the help of middleware known as remote procedure call. Because of this, it is now feasible to initiate a method the body of which is located on the opposite side of a network. Because RPC systems are typically synchronous and only offer a limited number of ways to handle exceptions, it is impossible to implement parallel processing with them unless additional threads are added.

Message-Oriented Middleware

An abstraction of a message queue that is accessible across the network is made available by message-oriented middleware (MOM). The word "mailbox" from operating systems has been repurposed here to refer to a more generic storage location. Because of the construction of the programs that add and delete messages from a queue, there are many different methods in which these programs may be put together. Several different MOM solutions include queues that can operate in real time, may be duplicated, or remain active for an extended period of time. In the same way that Linda does, MOM also makes a distinction between space and time.

Distributed Object Middleware

Distributed object middleware makes it possible to create an abstraction of a remote object with methods that can be called in the same manner as methods on an object that is located in the same address space as the caller. This makes it possible for the caller to interact with the remote object in the same way that they would interact with an object that is located locally. A developer of a distributed program is now able to employ all of the benefits of object-oriented software engineering in their work. These benefits include encapsulation, inheritance, and polymorphism. These benefits are made possible thanks to distributed objects.

When it comes to networked object computing, the Common Object Request Broker Architecture (CORB) is the benchmark that everyone uses. It is currently the most comprehensive piece of distributed object middleware available on the market, and it is a component of the Object Management Architecture developed by the Object Management Group. It incorporates not only the distributed object abstraction that CORBA provides, but also additional OMA components that might be of assistance to software developers working on distributed systems for either general-purpose or vertical markets. CORBA allows you to select the vendor and programming language that best suits your needs. The vast majority of industry professionals are in agreement that CORBA (and the OMA) is the sort of middleware that is the most cutting-edge currently available on the market and is the type that is the most faithful to classic object-oriented programming ideals. Anyone can understand and comply with its requirements since they are straightforward.

The Object Linking and Embedding (OLE) and Component Object Model (COM) technologies developed by Microsoft led to the development of the Distributed Component Object Model, or DCOM for short (COM). Other Microsoft products, such as Active Directory and Microsoft Transaction Server, provide support for DCOM. You are able to use a variety of languages with DCOM, but you are unable to utilize a variety of operating systems or tool suppliers. Programming in DCOM will become much simpler with the upcoming edition of DCOM, which is going to be dubbed COM+. Microsoft developed the distributed object technology known as SOAP. It utilizes HyperText Transfer Protocols (HTTP) in addition to XML. It is possible for anybody to view its specifications, and it may be implemented in a variety of languages and by a number of different vendors. The.NET distributed object framework from Microsoft is designed with the intention of facilitating collaboration amongst a variety of programming languages and suppliers.

Marketplace Convergence of the Concepts

There are many different ways in which the market muddles the distinctions between the aforementioned kinds of middleware. In the late 1990s, a growing number of businesses began to provide application programming interfaces (APIs) for a variety of abstractions, including distributed objects and message queues, which were in part managed by a TPM. On the other side, TPMs often include management and control functions, and they either employ RPC or MOM as a transport. By introducing a variety of extensions, such as stored procedures that appear like RPCs, manufacturers of relational databases have broken the rigorous separation of data and code as well as the relational paradigm. This is because the relational paradigm was designed to separate data from code. The fact that these stored processes are programmed in Java adds still another layer of complexity to the situation. There are also MOM systems that provide transactions on message queues, which can cover a variety of different processes. In conclusion, but certainly not least, distributed object systems frequently contain event services or channels that, in terms of design, have the same topology and data flow as MOM.

Middleware and Legacy Systems

Because it is so frequently employed in the process of connecting historical components, middleware is frequently referred to as "glue" technology. Moving mainframe applications that were never intended to interact together or be networked is crucial so that they can react to queries from a great distance. To provide network integrators and maintainers with a control API that is compatible with the majority of devices, middleware is also beneficial for encasing network devices such as routers and mobile base stations. Distributed object middleware is advantageous for the integration of older systems due to the wide range of tasks that it can do . In a nutshell, it has an extremely high lowest common denominator, which is necessary for interoperability. CORBA is frequently put to use for this purpose because to the fact that it provides the widest range of potential types of heterogeneity and enables older components to be utilized in the broadest possible context.

Programming with Middleware

In order to create middleware, a programmer does not need to become proficient in a new language. Instead, they make use of a programming language that is already in existence and is simple for them to work with, such as C++ or Java. There are three primary approaches to programming middleware that may be taken when using today's languages. In the first scenario, distributed database systems and Linda each provide their users with a library of functions that may be called upon in order to access the middleware. The second approach is to make use of a language in order to build an interface with the outside world IDL . In this manner, the interface to the remote component is described by the IDL file, and the programmer produces code by employing a mapping from IDL to the programming language that is being used. The third possibility is to enable native distribution by utilizing the language and runtime infrastructure already in place. This is demonstrated by Java's Remote Method Invocation, for instance (RMI).

Middleware and Layering

Within a certain configuration of the system, there might be more than one layer of middleware. Application programmers are able to leverage lower-level middleware, such as a virtually synchronous atomic broadcast service, in a direct and immediate manner (see Virtual Synchrony). It may be used as a building component by higher-level middleware such as CORBA or message-oriented middleware in order to provide fault tolerance, load balancing, or all of these features.

The "Application" Layer 7 of the OSI network reference architecture is where a middleware system is assembled the majority of the time. However, certain components are also located at the "Presentation" Layer 6 of the design. Therefore, the operating system's network protocols are considered to be a "application" of the middleware. The "application" is considered to be on top of the middleware when seen from its point of view.

Middleware and Resource Management

It is feasible to manage resources in a distributed system at a higher level than is typically achievable by utilizing the abstractions that come with a variety of middleware frameworks. This is not the case with traditional systems. This is due to the fact that these abstractions are able to be made comprehensive enough to incorporate all three categories of low-level physical resources that are managed by an operating system. These categories include storage, compute, and communications (memory and disks). The use of middleware abstractions, which take into account a system for managing resources from beginning to finish rather than only from the perspective of a single host, makes it feasible to see the entire system at once.

All programming abstractions for middleware, by definition, contain communication resources. Some programming abstractions, however, go beyond and also include processing and storage resources. The client only receives a minimal benefit from the processing performed by distributed tuples. The MOM protocol does not entail any processing, whereas the RPC protocol does not involve the storage of anything. Distributed objects, on the other hand, encapsulate all three categories of resources in a manner that enables them to function effectively in conjunction with one another. This completeness makes it simpler to provide other types of distributed transparency, such as mobility transparency, and it also helps with managing resources in a distributed manner. Moreover, it is a key factor in achieving completeness.

Middleware and Quality of Service Management

Programming distributed systems can be difficult due to the inherent high level of dynamic complexity that they possess. Even though controlling resources can be of great assistance, this alone is typically not sufficient for distributed systems. Quality of service (QoS) is an organizational term that refers to the behavioral characteristics of an item or system. Distributed systems research has started to focus on providing comprehensive QoS in order to better manage the dynamic nature of distributed systems. QoS is an acronym that stands for "quality of service." This study's primary objective is to provide low-level resource managers with high-level quality of service (QoS) requirements for the application. The study of conventional distributed systems often focuses on runtime adaptability as a topic. Quality of Service (QoS) can be used to help with this. On the other hand, it could also make it easier for apps to evolve over time so that they can adapt to new circumstances and fulfill new requirements. Although this is more of a concern with the software engineering side of things, it is of the highest relevance to users and those who maintain distributed systems .

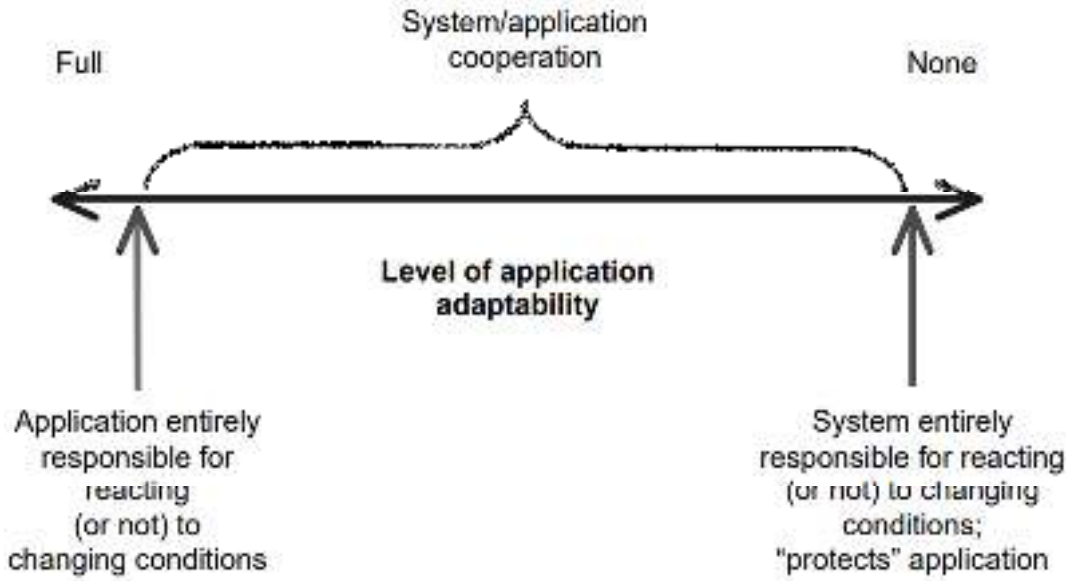
At the level of abstraction that is represented by an application software, quality of service may be optimally provided by middleware. Additionally, the abstractions that middleware systems provide may frequently be developed to incorporate a concept of quality of service while still maintaining their status as an abstraction that a programmer can comprehend and find helpful. Because it can encapsulate and mix such a broad variety of resources, distributed object middleware is an extremely useful tool for this purpose.

When provided with quality of service, applications are able to function well even when usage patterns or resource availability undergo significant and unpredictable shifts. When it is difficult to make the environment more predictable, this can assist the distributed application layer in seeing the environment in a more predictable light and assist the applications in adjusting to the new circumstances. Because their presumptions about the environment are not hard-coded into their application logic, quality of service (QoS) can also enable applications to be changed in a reasonable amount of time, making the apps easier to maintain and reducing the costs associated with doing so.

These things can be made feasible by middleware that has QoS abstractions because it can make obvious an application's QoS assumptions, such as how it will be utilized and what resources it will need, while still providing programmers with a high-level building block. Middleware with QoS capabilities is another high-level component that protects distributed applications from the low-level protocols and application programming interfaces (APIs) that will ultimately provide QoS. Shielding could be a good idea because of the difficulty and frequency with which these APIs and protocols are updated in comparison to the average lifespan of distributed systems. This separation of the application from lower-level functionality is a positive thing since it works in the same manner that TCP/IP has always enabled programs and devices develop on their own. On the other side, middleware that supports QoS makes it feasible to separate them while also providing a message stream, QoS, and a high-level abstraction. This is called a three-way split.

11.2 Adaptation

On mobile devices, both user-level and system-level programs run in a different manner than they do on desktop computers. This is due to mobile devices having a lower overall resource capacity than desktop computers. Electricity, volatile and nonvolatile memory, and network bandwidth are the most important factors, but screen resolution and other physical limitations are also very important. To provide users with a realistic computing environment that is as close as possible to what the resources they currently have will allow, applications and/or system software must be able to adapt to limited or changing levels of resources. This is necessary in order to give users a realistic computing environment. For instance, if the bandwidth suddenly became very limited, a mobile music application could stop sending an audio stream with a high bit rate and switch to a stream with a lower quality. There would be a lot of interruptions and stuttering if the program tried to give the high-quality stream, but the user is less likely to mind if they get the lower-quality stream. In the same vein, a video program can switch between high-quality, high-frame-rate color video, black-and-white video, color still photos, and black-and-white still photos depending on how much bandwidth is available. In addition, the program can also switch between color still photos and black-and-white still photos. Another illustration of this would be a mobile game app that, in order to conserve power, reduces the display resolution or disables any three-dimensional (3D) features when the battery level drops below a certain threshold. In order to put adaptation policies into effect, each and every adaptation strategy needs to take into consideration the resources that are currently accessible. The monitoring of certain resources, such as monetary assets, is not overly complicated. Simply create the appropriate accounts and set the appropriate limitations for each user. There are circumstances that call for more involved strategies. The ACPI provides software developers with a standardized method for obtaining information on the power level of "smart" batteries used in current gadgets. In networks with several hops, it is more difficult to obtain an accurate measurement of the network's bandwidth. Lai and Baker provide people who are interested with instructions on how to carry out various tasks. Since precise measurements of resource levels are required in order to make the appropriate judgments for adaptation, the methods that are used to monitor resource levels have a direct influence on how effectively adaptation functions as a whole.



11.3 Mobile Agents

Now, let's discuss mobile agent systems, which are a distinct sort of middleware for mobile devices. Mobile agent systems allow users to interact with mobile apps. Whether they are aware of it or not, the vast majority of computer users have at some point worked with mobile code. 11 Adaptation and the Role of Agents . Whether you like it or not, modern browsers enable runnable content like Java script, Java applets, and other items that can be executed. This indicates that even the act of merely browsing websites causes the relevant mobile code to be executed. Because code is sent

from one or more servers to a client and then executed on the client, applets and other applications that function in a similar manner tend to be rather static. The mobile code is frequently restricted from accessing resources located outside of the immediate vicinity. This is done for reasons related to security. The degree of complexity of mobile agents has significantly increased, which has made it much simpler for code and state to be relocated. Mobile agents are able to travel freely around a network and make their own decisions on where they should go next. This is in contrast to applets, the code for which typically only takes one "hop" to get from the server to the client (at least in principle). Mobile agents go around the network in search of information and engage in conversation with other agents so that they can achieve their objective.

Mobile agent systems function in a manner very similar to that of adaption middleware in that they make it possible for mobile applications to run in environments where there are restricted resources. Nevertheless, they accomplish a great deal more than simply allowing local applications to adapt to shifting resource availability. A client-server architecture (CS) is what's known as a mobile agent system. This design makes it simple for mobile applications (agents) to travel to and from remote servers. It is possible that an agent will decide to relocate because it has completed its task or because it feels the need to go to a different location in order to get additional information. It is possible for an agent to make the decision to construct one or more new agents on the fly and let them move instead of the agent itself moving. The objective is to move mobile code as near to the action as is practically practicable; hence, mobile agents will travel to remote computers to do computations and will then bring the results back to their home base. Sending remote procedure calls to the database servers is an example of a tried-and-true method that may be utilized on mobile devices for the purpose of conducting a search across several databases. A mobile agents method, on the other hand, would include sending one or more applications, which are referred to as "agents," to computers that are geographically close to the database servers, or even to the servers themselves. Following the execution of queries to the database servers, the agents sift the results in an effort to locate a remedy that is applicable to the issue faced by the mobile user. When the mobile agents are finally able to return to their homes, they report the results to the headquarters.

The advantages of adhering to this approach are not hard to discern. First, if a mobile user has a low bandwidth and their database queries are sophisticated, it may be prohibitively expensive for them to send a series of remote queries to the servers. This is because the remote queries must be sent. To obtain the information they want, the agents can do a number of queries that are significantly closer to the database servers. This might save a significant amount of traffic (though transmission of the agent code must still be considered). The second requirement is that the device does not need to be constantly linked to the network. The mobile user may first connect to the network, then send the agent on their way, and finally sever all links. The agent will be able to go home and deliver its report after the mobile user has successfully reconnected to the network. Last but not least, the agents' proximity to the event, along with the fact that they may be executed on considerably more powerful computers, may enable them to accelerate the process of mining the required information.

11.4 Service Discovery Middleware

It can be challenging to find out how to provide services to clients using mobile devices since, in comparison to their wired equivalents, mobile devices often have less processing power and less knowledge of their immediate surroundings. Mobile clients are often not tethered to any particular infrastructure, in contrast to desktop computers, which typically have prompt access to a broad variety of peripheral devices such as printers, scanners, and tape backup. They are less dependent on them as a result, which results in more freedom for them. On the other side, mobile clients place a greater emphasis on engaging in fluid exchanges with their immediate environment and discovering new services.

Building robust mobile computing environments may be accomplished with the help of service discovery frameworks, which also make it much simpler to install and configure networked services For instance, making use of and locating a printer is possible as soon as it has been linked to a network that supports service discovery. Because of this, there are fewer issues that arise when setting up the printer, and system administrators save a significant amount of time as a result of the printer's ability to automatically adjust to its surroundings. Additionally, users like how simple the procedure is: Service discovery-capable clients, such as a word processor, are able to locate and utilize the printer without the user having to seek for it, determine what sort it is, and then

download and install device drivers. This is because these clients can find the printer on their own. If the old printer is removed, for example to make room for a model that has more storage, the new printer won't be any more difficult to connect to the network than the previous one was. And a mobile client that travels away from the printer (for example, leaving the workplace to work in the afternoon at a coffee shop) will break relations with that printer and hunt for another one that is functional. When it comes to be required. When put to use in this manner, service discovery makes it possible for the local "plug and play" technology that (typically) functions on Windows computers to be utilized over the network and on a wide variety of platforms.

Because the same service discovery framework is available everywhere, a device does not need to have its settings changed when it is moved from one location to another, such as when it is taken from your home to your workplace to the home of a friend. Service discovery methods can also be utilized to provide more interesting services, such as printing, scanning, and other similar activities. A key chain that is capable of service discovery can be carried by a user and used to switch on lights, alter desktop settings, or change sound systems while the user is on the road. When the user walks into a meeting, the same device can automatically make a copy of a diagram that was written on a whiteboard or take a picture of an electronic business card. This is made possible by the service discovery feature. The usage of remote file storage services allows users of small mobile computers with limited storage capacity, such as personal digital assistants, to store a greater quantity of files (PDAs).

Since the late Marc Weiser published extensively on the subject many years ago, it's clear that these concepts aren't brand new. However, thanks to service discovery technologies, the software environment in which these sorts of settings are built has been standardized, making it much simpler to put these settings into place and ensuring that they are compatible with one another.

The term "service discovery framework" refers to, in its broadest sense, a collection of protocols enabling the construction of highly dynamic client-server (CS) systems. These protocols define several common methods in which clients and services can communicate with one another. What other kinds of services are available to customers? is an important consideration for the development of CS systems.

- Where exactly may the services be found?
- How can those who utilize the service get in touch with you?
- What types of guidelines does the customer have to follow when working with the service?
- How can we design computer systems that can troubleshoot and repair themselves?
- How can we set up redundant parts so that the system is more resistant to problems and can better handle the load that is being placed on it?
- How secure is it for a customer to make use of a service, or for a service to communicate with a particular customer?

Frameworks for service discovery provide a means through which responses to inquiries of this nature may be made to be consistent with one another. There are a number of similarities between several service discovery frameworks such as Jini, Service Location Protocol, and the Salutation Architecture (Salutation, 1999). the most significant components and actions needed to answer the questions above are already common knowledge. The conventional senses of the terms "client" and "service" are supported by each and every service discovery framework, namely: The services are able to fulfill the requirements of the customers. During a paper presentation, for instance, a client using a laptop computer can access wireless projection services from an LCD projector if the latter supports service discovery. A user may, in a similar fashion, be able to receive a high-resolution image of Saturn using a telescope that has service discovery switched on when the telescope is used when it is pointed in the right direction. Surprisingly, service discovery frameworks share a lot of similarities on a fundamental level, despite the fact that their individual design aspects are distinct from one another. Customers may engage with businesses on the most fundamental level by advertising and learning more about the services that are available. People can be informed through service marketing when a service is joining or leaving a network. This can be done both positively and negatively. In most cases, the advertisement contains the required contact information in addition to either material that defines the characteristics or information that assists in finding them.

11.5 Finding Needed Services

Service discovery, when seen from the perspective of the client, makes it feasible for them to locate services that exist either in their local network environment or on a broader scale (e.g., in the global Internet). Some individuals hunt for services directly, while others discover one or more catalogs of services and browse through them to find what they want. Some people look for services directly, while others look for services indirectly. Quite frequently, the discovery process will involve the gathering of information on the kinds of services that are required. This could include the standardized name(s) of the service categories as well as the service qualities. In the case of hardware services, these features may reveal the precise (geographic) location of the service, the capabilities of the device in question (such as whether or not a printer is able to print on both sides of a page), as well as accounting information such as the usage fee associated with the service.

Whether services are requested directly or through a catalog, a client does not need to know very much about its environment because it can find services (or service catalogs) on the fly with very little to no static setup. This is true whether the services are requested directly or through the catalog. In the same vein, choices may be made on the fly regarding service features such as the protocols that are required for communication. Service discovery frameworks ensure that service catalogs, garbage collection, security, and the development of protocols for client-service communication all operate in the same manner.

Consistency is the primary advantage that comes with the usage of service discovery protocol suites for both developers and end users. There is nothing especially magical about any of the CS interactions, such as discovery and advertising; in fact, an experienced programmer could easily make them up on the fly. Standardization, on the other hand, makes it feasible for a large number of clients and services to function together "straight out of the box." An implementation of a service discovery framework will, of course, give practical means by which discovery, advertising, and even ting may be accomplished. When compared to the process of constructing large computer systems from the ground up, this might save developers a significant amount of time and effort.

Summary

- Middleware technologies were discussed along with their need.
- Examining different types of the middleware were discussed.
- We have discussed how the marketplace has converged with middleware.
- How the adaption of the middleware and mobile agents is done in the development of middleware.

Keywords

API- Application programming interface

DA- Distributed applications

CORBA- Common Object Request Broker Architecture

SQL- Structured Query Language

RPC- Remote procedure Call

MOM- Message oriented Middleware

OMA- Object Management Architecture

OLE- Object Linking and Embedding

COM- Component Object Model

HTTP- Hypertext transfer Protocols

SOAP- Simple object access protocol

XML- Extensible markup language

TPM - Trusted platform module

IDL -Interface Definition Language

RMI – Remote Method Invocation

OSI – Open systems Interconnection

QoS- Quality of the service

ACPI- Advanced configuration and Power Interface

CS- Client server architecture

Self Assessment

Q1) A "glue" between client and server parts of application.

A. Middleware
B. Firmware
C. Package
D. System Software

Q2) MOM stands for?

A. Message oriented middleware
B. Mails oriented middleware
C. Middleware of messages
D. Main object middleware

Q3) The software that works between the operating system and the applications is called.

A. Firmware
B. Middleware
C. Utility Software
D. Application Software

Q4) Middleware between the built-in applications and the real-time OS?

A. Firmware
B. Database middleware
C. Portals
D. Embedded Middleware

Q5) What is the other name for object middleware?

A. Object request interface
B. Object enabled interface
C. Object Request broker
D. Object enabled broker

Q6) The _____ calls certain procedures on remote systems and is used to perform synchronous or asynchronous interactions between systems.

A. Procedure

B. RPC

C. Message Oriented

D. DB

Q7) _____ is an organizational term that refers to the behavioral characteristics of an item .

A. MOM

B. QoS

C. CS

D. None of the above

Q8) _____makes it feasible for clients to locate services.

A. SOS

B. QoS

C. Service discovery

D. Service catalogues

Q9) The_____ provides software developers with a standardized method for obtaining information on the power level of "smart" batteries used in current gadgets.

A. API

B. SOS

C. ACPI

D. None of the above

Q10) _____ is the most widely used middleware in modern times.

A. Centralized database

B. Distributes relational database

C. Abstract database

D. Client database

Q11) A_____ architecture is also known as mobile agent system.

A. Serverless

B. Client server

C. Distributed server

D. Centralized

Q12) Programming distributes systems has a_____ level of dynamic complexity .

A. Low

B. High

C. Medium

D. None

Q13) Distributed object middleware is extremely useful because it can perform _____.

A. Abstraction

B. Identification

C. Encapsulation

D. Comprehension

Q14) Another informal name of the middleware is _____.

A. Worker

B. Plumbing

C. Builder

D. None of the above

Q15) Is it possible for the middleware to have more than one layer?

A. True

B. False

Q16) Mobile agent systems allow users to interact with mobile apps

A. True

B. False

Answers for Self Assessment

1.	A	2.	A	3.	B	4.	D	5.	C
6.	B	7.	B	8.	B	9.	C	10.	B
11.	B	12.	B	13.	C	14.	B	15.	A
16.	A								

Review Questions

1. Write and explain about the middleware in detail.
2. Explain the distributed tuples in detail.
3. Compare and contrast the functionality RPC and distributed object middleware.
4. Explain the relation between Middleware and Resource Management in detail.
5. Elaborate the concept of service discovery middleware.
6. Explain how mobile agents play an important role in middleware .

Further Readings

- Wireless communications & networks by William Stallings, Pearson
- Principles of wireless networks by Kaveh Pahlavan, Pearson
- Fundamentals of wireless networking by Ron price, Mcgraw hill education
- Fundamentals of Mobile and Pervasive Computing by Golden G. Richard III Frank Adelstein Sandeep K. S. Gupta Loren Schweibert
- Wireless networks first-step by Jim Geier, cisco press

Web Links

https://eecs.wsu.edu/~bakken/middleware.htm

Unit 12: Wireless Application Protocol and Mobile IP

CONTENTS

Objectives

- Understanding the concepts of WLAN
- Analyzing the transmission technology behind the wireless local area network.
- Understanding the Infrared LAN and its configurations.
- Analyzing the spread spectrum LAN.

Introduction

In IP networks, when a device is within its home network, the routing is based on the static IP addresses. The device within a network is connected through normal IP routing by the IP address assigned on the network. It is the same as how a postal letter is delivered to the fixed address on the envelope. The problem occurs when a device goes away from its home network and is no longer reachable using normal IP routing. In this condition, the active sessions of the device are terminated. The idea of Mobile IP was introduced to resolve this issue. It facilitates users to keep the same IP address while going to a different network or a different wireless operator without being communication disrupted or without sessions or connections being dropped.

12.1 Mobile IP395

This is an IETF (Internet Engineering Task Force) standard communications protocol designed to allow mobile devices' (such as laptop, PDA, mobile phone, etc.) users to move from one network to another while maintaining their permanent IP (Internet Protocol) address.

Defined in RFC (Request for Comments) 2002, mobile IP is an enhancement of the internet protocol (IP) that adds mechanisms for forwarding internet traffic to mobile devices (known as mobile nodes) when they are connecting through other than their home network.

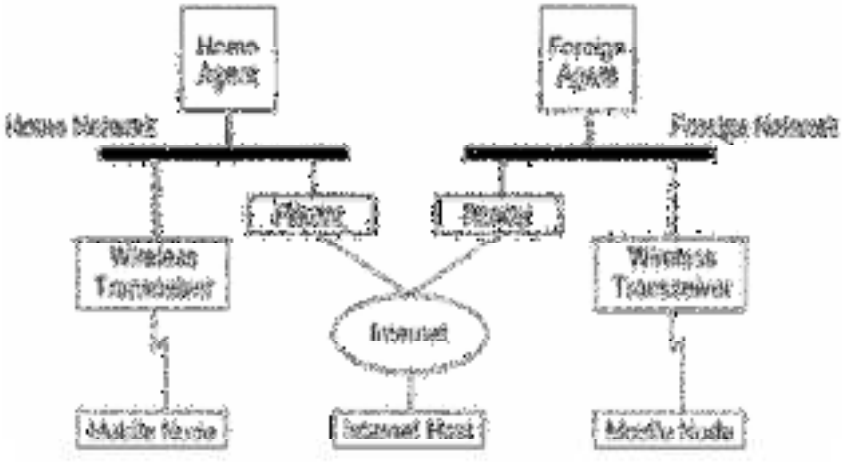


Fig: Mobile IP topology

Mobile IP Framework

First of all, the internet host sends a datagram to the mobile node using the mobile node's home address (normal IP routing process). If the mobile node (MN) is on its home network, the datagram is delivered through the normal IP (Internet Protocol) process to the mobile node. Otherwise the home agent picks up the datagram. If the mobile node (MN) is on foreign network, the home agent (HA) forwards the datagram to the foreign agent. The foreign agent (FA) delivers the datagram to the mobile node. Datagrams from the MN to the Internet host are sent using normal IP routing procedures. If the mobile node is on a foreign network, the packets are delivered to the foreign agent. The FA forwards the datagram to the Internet host.

Components of Mobile IP

1. Mobile Node (MN): The mobile node is an end system or device such as a cell phone, PDA (Personal Digital assistant), or laptop whose software enables network roaming capabilities.
2. Home Agent (HA): The home agent provides several services for the mobile node and is located in the home network. The tunnel for packets towards the mobile node starts at home agent. The home agent maintains a location registry, i.e. it is informed of the mobile node's location by the current COA (care of address). Following alternatives for the implementation of an HA exist. Home agent can be implemented on a router that is responsible for the home network. This is obviously the best position, because without optimization to mobile IP, all packets for the MN have to go through the router anyway. If changing the router's software is not possible, the home agent could also be implemented on an arbitrary node in the subset. One biggest disadvantage of this solution is the double crossing of the router by the packet if the MN is in a foreign network. A packet for the mobile node comes in via the router; the HA sends it through the tunnel which again crosses the router.

12.2 Foreign Agents (FA)

The foreign agent can provide several services to the mobile node during its visit to the foreign network. The FA can have the COA (care or address) acting as a tunnel endpoint and forwarding packets to the MN. The foreign agent can be the default router for the MN. Foreign agent can also provide security services because they belong to the foreign network as opposed to the MN which is only visiting.

In short, FA is a router that may function as the point of attachment for the mobile node when it roams to a foreign network delivers packets from the home agent to the mobile node.

Example: An archeologist on site in Greece might use a PDA to directly access databases at the University of Minnesota in Minneapolis, and to transmit findings to that database.

Care of Address (COA): The Care- of- address defines the current location of the mobile node from an IP point of view. All IP packets sent to the MN are delivered to the COA, not directly to the IP address of the MN. Packet delivery toward the mobile node is done using a tunnel. To be more precise, the COA marks the endpoint of the tunnel, i.e. the address where packets exit the tunnel.

Two different possibilities:

Foreign Agent COA: The COA could be located at the foreign agent, i.e. the COA is an IP address of the foreign agent. The foreign agent is the tunnel endpoint and forwards packets to the MN. Many MN using the FA can share this COA as common COA.

Co-located COA: The COA is co-located if the MN temporarily acquired an additional IP address which acts as a COA. This address is now topologically correct, and the tunnel endpoint is at the mobile node. Co-located address can be acquired using services such as DHCP. One problem associated with this approach is need for additional addresses if MNs request a COA. This is not always a good idea conside.

Correspondent Node (CN): At least one partner is needed for communication. The correspondent node represents this partner for the MN. The correspondent node can be a fixed or mobile node. ring the scarcity of IPv4 addresses

Home Network: The home network is the subset the MN belongs to with respect to its IP address. No mobile IP support is needed within this network.

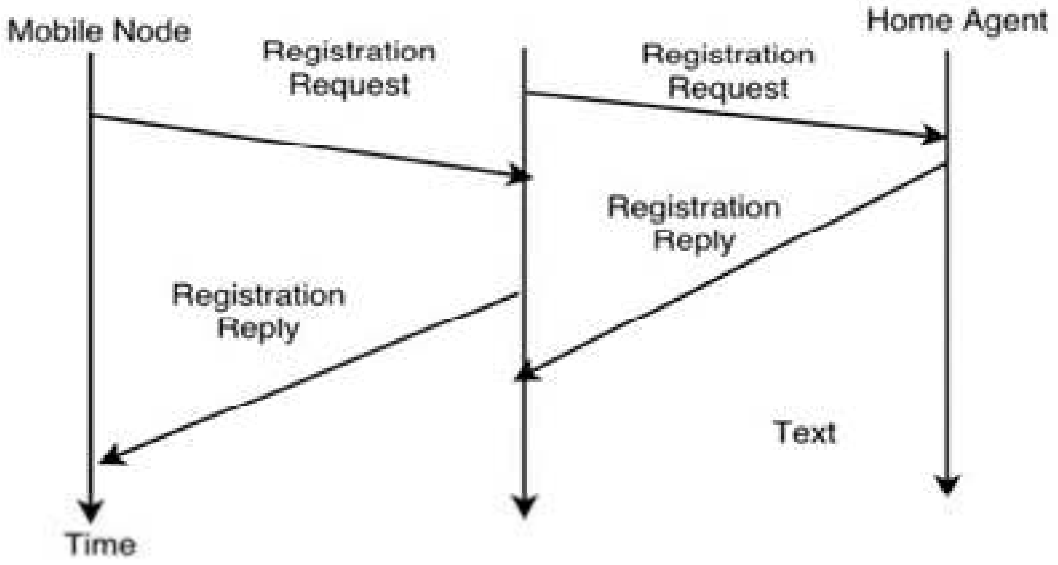
12.3 Process of Mobile IP

The mobile IP process has following three main phases, which are:

1. Agent Discovery: During the agent discovery phase the HA and FA advertise their services on the network by using the ICMP router discovery protocol (IROP).Mobile IP defines two methods: agent advertisement and agent solicitation which are in fact router discovery methods plus extensions.
2. Agent advertisement: For the first method, FA and HA advertise their presence periodically using special agent advertisement messages. These messages advertisement can be seen as a beacon broadcast into the subnet. For this advertisement internet control message protocol (ICMP) messages according to RFC 1256, are used with some mobility extensions.
3. Agent advertisement: For the first method, FA and HA advertise their presence periodically using special agent advertisement messages. These messages advertisement can be seen as a beacon broadcast into the subnet. For this advertisement internet control message protocol (ICMP) messages according to RFC 1256, are used with some mobility extensions.

Registration

The main purpose of the registration is to inform the home agent of the current location for correct forwarding of packets.



Registration can be done in two ways depending on the location of the COA. If the COA is at the FA, the MN sends its registration request containing the COA to the FA which is forwarding the request to the HA. The HA now set up a mobility binding containing the mobile node's home IP address and the current COA. Additionally, the mobility biding contains the lifetime of the registration which is negotiated during the registration process. Registration expires automatically after the lifetime and is deleted; so a mobile node should register before expiration. After setting up the mobility binding, the HA send a reply message back to the FA which forwards it to the MN.

If the COA is co-located, registration can be very simpler. The mobile node may send the request directly to the HA and vice versa. This by the way is also the registration procedure for MNs returning to their home network.

Caution: Infrared radiation (IR) has major biological effects. It greatly affects the eyes and skin. Microwave signals are also dangerous to health. But with proper design of systems, these effects are reduced considerably.

12.4 Tunneling

A tunnel is used to establish a virtual pipe for data packets between a tunnel entry and a tunnel endpoint. Packets which are entering in a tunnel are forwarded inside the tunnel and leave the tunnel unchanged. Tunneling, i.e., sending a packet through a tunnel is achieved with the help of encapsulation. Tunneling is also known as "port forwarding" is the transmission and data intended for use only within a private, usually corporate network through a public network. Tunneling is a method that involves encapsulating one network protocol's data packets within the payload of another protocol to facilitate secure or efficient data transmission across networks. This technique is commonly used in scenarios where data must traverse networks with different characteristics or security requirements. By encapsulating the original data in a tunneling protocol, such as the Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), or IPsec, data can be securely transmitted through untrusted or incompatible network segments, often providing encryption and authentication to safeguard the communication. VPNs, for instance, employ tunneling to create private, encrypted communication channels over the public internet, ensuring data confidentiality and integrity.

Tunneling is particularly useful for achieving specific network objectives, such as:

Virtual Private Networks (VPNs): Tunneling is a fundamental component of VPN technology. It enables the creation of secure, encrypted communication channels over public networks, like the internet. Protocols like IPsec, PPTP, L2TP, and SSL/TLS are used for tunneling in VPNs, ensuring the privacy and security of data transmitted between remote locations or users.

IPv6 Transition: Tunneling can be used to facilitate the transition from IPv4 to IPv6. When two networks use different IP versions, tunneling allows IPv6 packets to be encapsulated within IPv4

packets (or vice versa), ensuring compatibility and enabling communication between the two network types during the transition period.

Remote Access: Tunneling is employed for remote access solutions, allowing users to securely access resources on a private network from a remote location. For example, employees can access corporate resources from home using a tunneling protocol like SSL/TLS or IPsec.

Connecting Branch Offices: Tunneling is used to interconnect branch offices in a secure and efficient manner. This ensures that data can flow seamlessly between geographically distributed locations within an organization's network.

Overcoming Network Restrictions: In some cases, tunneling can help bypass network restrictions imposed by firewalls, content filters, or other security measures. However, this use of tunneling is often associated with attempts to circumvent network policies and can raise security and ethical concerns.

The correspondent node sends the data to the mobile node. Data packets contain the correspondent node's address (Source) and home address (Destination). Packets reach the home agent. But now mobile node is not in the home network, it has moved into the foreign network. The foreign agent sends the care-of-address to the home agent to which all the packets should be sent. Now, a tunnel will be established between the home agent and the foreign agent by the process of tunneling. Tunneling establishes a virtual pipe for the packets available between a tunnel entry and an endpoint. It is the process of sending a packet via a tunnel and it is achieved by a mechanism called encapsulation. Now, the home agent encapsulates the data packets into new packets in which the source address is the home address and destination is the care-of-address and sends it through the tunnel to the foreign agent. Foreign agent, on another side of the tunnel, receives the data packets, decapsulates them, and sends them to the mobile node. The mobile node in response to the data packets received sends a reply in response to the foreign agent. The foreign agent directly sends the reply to the correspondent node.

Agent Registration: Mobile node after discovering the foreign agent sends a registration request (RREQ) to the foreign agent. The foreign agent, in turn, sends the registration request to the home agent with the care-of-address. The home agent sends a registration reply (RREP) to the foreign agent. Then it forwards the registration reply to the mobile node and completes the process of registration.

12.5 Why do we need Mobile IP?

Mobile Internetworking Protocol (Mobile IP) is an advanced version of Internetworking Protocol (IP). IP addresses were designed for the stationary host that always remains attached to one specific network. The prefix of the IP address identifies the network to which the host belongs. The suffix of the IP address identifies the particular host in the corresponding network.

Entities of Mobile IP

Home Network is a network to which the mobile host actually belongs. It is a permanent network of the mobile host. Foreign Network is a new network into which the mobile host has moved. Remote Network is a network which is neither the home network nor the foreign network. Mobile Host is a host of the home network which has moved to the foreign network. Remote Host is a host in a remote network. Home Agent is a router attached to the home network that allows the mobile host to send and receive data from the remote host over the internet. Foreign Agent is a router attached to the foreign network that allows a mobile host to send and receive data from a remote host over the internet. Care-of address is a temporary IP address provided by the foreign agent to the mobile host till it is in the foreign network. Home Address is the address of the mobile host in its home network.

Advantages and Disadvantages of Mobile IP

- A user with its network devices can move to any other network without losing its connection with its home address.
- Mobile IP provides transparency while the data transfer process. It hides the fact that the mobile host is not in its home network and is communicating from a foreign network.

Disadvantages

- When the 'remote host' and 'mobile host' both are in a foreign network and still the data transfer is occurring through the 'home agent' then the data packet has to travel more distance though both the host are in the same network.
- As we have seen above, if the mobile host in the foreign network wants to send the data packet to the remote host it sends it directly from the foreign network with its home address as the source and the remote host address in the destination.
- But, if a remote host wants to send a packet to a mobile host in a foreign network, the data packet has to travel to the mobile host via its home agent. So, here it has to travel the extra distance.
- The most important advantage of mobile IP is that it allows the communication of a mobile host with a remote host even if the mobile host is in a foreign network.
- The disadvantage of mobile IP is, it seems to be inefficient due to the extra distance that a message has to travel. Like, in the case of double-crossing and triangle routing

12.1 Home Agent Considerations

Home agents play an active role in the registration process. The home agent receives registration requests from the mobile node. The registration request might be relayed by the foreign agent. The home agent updates its record of the mobility bindings for this mobile node. The home agent issues a suitable registration reply in response to each registration request. The home agent also forwards packets to the mobile node when the mobile node is away from the home network. A home agent might not have to have a physical subnet configured for mobile nodes. However, the home agent must recognize the home address of the mobile node through the mipagent.conf file or some other mechanism when the home agent grants registration.

12.2 Dynamic Home Agent Discovery

In some situations, the mobile node might not know the home agent address when the mobile node attempts to register. If the mobile node does not know the home agent address, the mobile node can use dynamic home agent address resolution to learn the address. In this situation, the mobile node sets the home agent field of the registration request to the subnet-directed broadcast address of its home network. Each home agent that receives a registration request with a broadcast destination address rejects the mobile node's registration by returning a rejection registration reply. By doing so, the mobile node can use the home agent's unicast IP address that is indicated in the rejection reply when the mobile node next attempts registration. If the mobile node is registered and uses a foreign agent care-of address, the process is straight forward. The mobile node chooses its default router from among the router addresses that are advertised in the ICMP router advertisement portion of that agent advertisement. The mobile node can also consider the IP source address of the agent advertisement as another possible choice for the IP address of a default router.

Summary

- Mobile IP allows mobile devices to keep a consistent IP address while moving across networks.
- It involves home and foreign agents for seamless connectivity.
- Benefits include uninterrupted sessions during network changes.
- It exists in both Mobile IPv4 and Mobile IPv6 forms.
- Adoption is limited due to alternatives and network overhead concerns.

Keywords

WLAN - Wireless local area network

AP - Access point

CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance

CSMA/CD - Carrier Sense Multiple Access with Collision Detection

WECA - Wireless Ethernet Compatibility Alliance

Care-of Address

Registration

Seamless mobility

IP address continuity

Mobility management

Mobile IPv4

Mobile IPv6

Self Assessment

1. What does WAP stand for?
A. Wireless Application Platform
B. Wireless Access Protocol
C. Wireless Application Protocol
D. Wireless Application Provider

2. Which layer of the OSI model does WAP primarily operate in?
A. Physical Layer
B. Data Link Layer
C. Network Layer
D. Application Layer

3. Which of the following is NOT a core component of WAP architecture?
A. WAP Gateway
B. WAP Browser
C. WAP Server
D. WAP Modem

4. In WAP, what is the purpose of a WML (Wireless Markup Language) document?
A. To encode binary data
B. To define wireless network parameters
C. To display content on mobile devices
D. To manage network security

5. Mobile IP is a protocol that allows:
A. Mobile phones to communicate with satellites
B. Mobile devices to maintain the same IP address while moving across networks
C. Mobile devices to connect to Wi-Fi networks only
D. Mobile devices to encrypt their data transmissions

6. Which of the following is a primary advantage of Mobile IP?
A. Improved battery life
B. Enhanced data transfer speed
C. Seamless mobility across networks
D. Reduced call drop rates

7. In Mobile IP, what is the role of a Home Agent (HA)?
A. Assigning IP addresses to mobile devices
B. Routing packets to the current location of a mobile device
C. Authenticating users on the network
D. Providing internet access to mobile devices

8. What is the purpose of the Mobile IP Care-of Address (CoA)?
A. It is the permanent IP address of a mobile device.
B. It is a temporary address used when the device is away from its home network.
C. It is the address of the Home Agent (HA).
D. It is the address of the mobile device's user.

9. Which protocol is commonly used for secure communication between a Mobile Node (MN) and its Home Agent (HA) in Mobile IP?
A. HTTP
B. HTTPS
C. SSL/TLS
D. FTP

10. What does a WAP gateway do in the context of WAP technology?
A. It converts WML to HTML.
B. It connects mobile devices to Wi-Fi networks.
C. It provides a secure tunnel for mobile data.
D. It manages mobile device batteries.

11. Which layer of the OSI model is responsible for session management in WAP?
A. Presentation Layer
B. Transport Layer
C. Session Layer
D. Data Link Layer

12. Which protocol is commonly used for transporting WAP content over the internet?
A. HTTP
B. SMTP
C. FTP
D. UDP

13. In Mobile IP, what is the purpose of the Registration Request message?

A. To request a new IP address
B. To notify the Home Agent of the mobile device's current location
C. To authenticate the mobile device
D. To establish a secure connection

14. Which of the following is NOT a security concern in the context of Mobile IP?
A. Unauthorized access to data
B. Location tracking of mobile devices
C. Battery drain on mobile devices
D. Spoofing of Home Agents

15. Which organization developed the initial specifications for WAP?
A. IEEE
B. W3C
C. IETF
D. WAP Forum

Answers for Self Assessment

1.	C	2.	D	3.	D	4.	C	5.	B
6.	C	7.	B	8.	B	9.	C	10.	A
11.	C	12.	A	13.	B	14.	C	15.	D

Review Questions

1. What is the primary purpose of Wireless Application Protocol (WAP)?
2. Which layer of the OSI model does WAP primarily interact with, and why?
3. What is the role of a WAP gateway in the context of WAP architecture?
4. How does Wireless Markup Language (WML) differ from HTML, and why is it used in WAP?
5. What is Mobile IP, and why is it important in mobile communication networks?
6. What are the key components involved in Mobile IP, and how do they work together to provide mobility to mobile devices?
7. What is the Home Agent (HA) in Mobile IP, and what functions does it perform?
8. Explain the concept of the Care-of Address (CoA) in Mobile IP and

Further Readings

- Wireless communications & networks by William Stallings, Pearson
- Principles of wireless networks by Kaveh Pahlavan, Pearson
- Fundamentals of wireless networking by Ron price, McGraw hill education
- Wireless networks first-step by Jim Geier, cisco press

Web Links

http://59.51.24.50:8000/wxwl/Wireless_Communications_&_Networking_Stallings_2n

d.pdf

Unit 13: Wireless Security

CONTENTS

Objectives

- Ensure the confidentiality of wireless data transmissions by preventing unauthorized access.
- Protect against cyber threats, such as malware and phishing, targeting wireless networks.
- Establish robust user authentication mechanisms to verify the identity of devices and users.
- Maintain the integrity of data transmitted over wireless networks, safeguarding it from tampering.
- Continuously monitor and respond to security threats and vulnerabilities in wireless infrastructure.

Introduction

Wireless protection is an important part of the digital world we live in today. With the rise of wireless technologies and our growing dependence on them, it is more important than ever to protect the privacy, security, and access of data sent over wireless networks. Wireless security is a set of means and rules that protect wireless communication from unauthorized access, data breaches, and hacking, among other things. It means putting in place strong login methods, encryption, access control mechanisms, and regular updates, as well as making sure users know about security policies and follow them. As wireless communication keeps getting better and spreads to more and more part of our lives, it's important to understand and prioritize wireless security to protect our digital assets and keep our trust in these technologies.

13.1 Wireless Security

Wireless security is a set of rules and means that are meant to keep wireless networks and devices safe from different security risks. Some of these dangers are unauthorized access, listening in on conversations, changing data, and denial of service attempts. As wireless technology keeps getting better, so do the methods and tools that bad people use to take advantage of security holes. So, it is very important to know how important Wi-Fi security is and how to improve it.

Wireless networks give people a lot of comfort, but the way they work is actually very complicated. There are a lot of systems and tools that work together to give people a stable link. Users feel safe when data bits travel through wire because data travelling through wire is probably not heard by snoops.

To keep the wifi link safe, we should pay attention to the following:

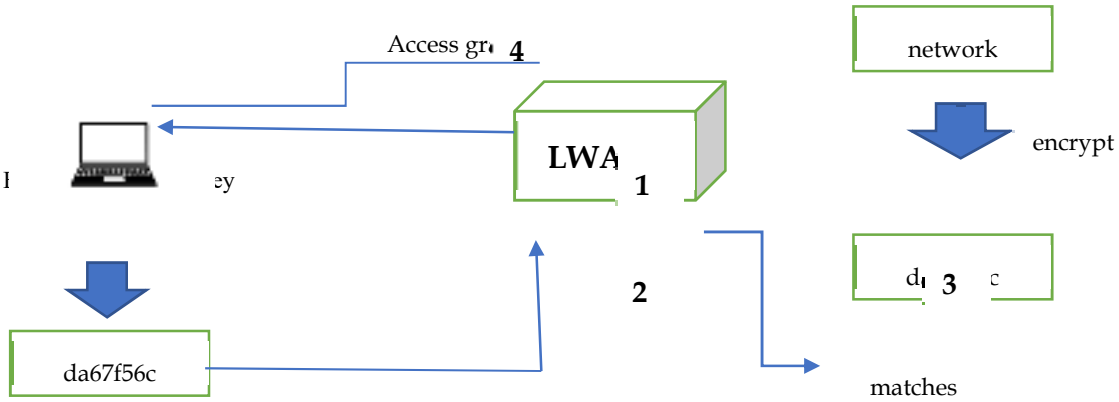
Authentication is the process of finding the endpoint of a wireless network and the end users.

Keeping middlemen from getting in the way of wireless data bits, i.e., Privacy.

Maintaining the integrity of the wireless data bits, i.e., Integrity.

We know that wireless clients connect to Access Points (AP) and send and receive data wirelessly. All wifi gadgets can work together as long as they follow 802.11 guidelines. But not all wireless devices are nice and trustworthy. Some illegal devices may be a threat to wireless security. Rogue devices can steal our important information or make the network unavailable.

Wired Equivalent Privacy (WEP): Open identification does not protect data that is sent wirelessly over the air.Every frame that WEP sends is encrypted with the RC4 cypher method. The RC4 cypher also uses a string of bits called a WEP key as a key to secure data at the sending site and recover it at the receiving site.WEP key can be used to prove who you are or to hide information. Only if a computer has the right WEP key can it connect to an AP. AP uses a challenge word to see if you know the WEP key. The client uses his own key to encrypt the phrase and sends it back to the AP. AP checks to see if the encrypted frame he got matches the encrypted phrase he sent. If both match, the connection is open to the user.



Extensible Authentication Protocol (802.1x/EAP) :

In WEP security, the wireless clients are verified locally at the access point (AP). But 802.1x changes the scenario. The system gets a computer that is only for identification. There are three things working together:

Supplicant: The device that wants to get in.

Authenticator: A device that gives entry to a network, usually a WLAN controller (WLC).

Authentication Server: A device that checks the details of a client and decides whether to let them in or not.

The Significance of Wireless Security

Wireless networks, like any other technology, are susceptible to security threats. These threats can range from unauthorized access and data breaches to denial-of-service attacks and eavesdropping. Understanding the significance of wireless security is crucial for safeguarding sensitive information, ensuring privacy, and maintaining the integrity of data. Let's take a closer look at why wireless security matters:

1. **Privacy Concerns:** Wireless devices often transmit personal and sensitive data. Without proper security measures, this data can be intercepted and misused. Consider, for example, the personal and financial information shared when making online purchases or conducting mobile banking. Protecting this data from prying eyes is paramount.

2. **Business and Organizational Data:** In the corporate world, wireless networks are the backbone of operations. Businesses rely on these networks for communication, data sharing, and remote access. A breach in wireless security can lead to significant financial losses, damage to reputation, and legal consequences.

3. **Critical Infrastructure:** Wireless systems are used in critical infrastructure sectors such as energy, transportation, and healthcare. Any disruption or unauthorized access to these networks can have catastrophic consequences, affecting public safety and national security.

13.2 Authentication

Authentication plays a crucial role in wireless security by verifying the identity of users or devices before granting access to a network or specific resources within it. Robust authentication mechanisms are essential for preventing unauthorized access and ensuring that only trusted entities can connect to a wireless network. Let's explore authentication in greater detail:

Passwords and Passphrases

Passwords and passphrases are the most common and widely used authentication methods in wireless networks. Users are required to enter a secret combination of characters, which must match the stored credentials on the network server or device for access to be granted. Here are key considerations for password-based authentication:

1. **Strength and Complexity:** Strong passwords should be complex, consisting of a mix of upper and lower-case letters, numbers, and special characters. Passphrases, longer phrases made up of words or sentences, are increasingly popular due to their ease of remembrance and increased complexity.
2. **Password Policies:** Organizations often implement password policies that specify requirements such as minimum length, complexity, and expiration periods. Users may be required to change passwords regularly.
3. **Password Hashing:** Storing passwords in plain text is a security risk. Instead, passwords are typically hashed, which involves applying a one-way mathematical function to create a unique hash value. Hashed passwords are stored on the server, making it more difficult for attackers to obtain the actual passwords even if they breach the system.
4. **Multi-Factor Authentication (MFA)**: MFA enhances security by requiring users to provide multiple forms of identification before granting access. Common factors include something the user knows (password), something the user has (a mobile device for receiving one-time codes), and something the user is (biometrics like fingerprint or retina scans).

Certificate-Based Authentication

Certificate-based authentication is a more advanced method that relies on digital certificates issued by a trusted authority, typically a Certificate Authority (CA).

Digital Certificates: Each user or device is issued a unique digital certificate that includes a public key. The corresponding private key is securely stored on the user's device.

Certificate Verification: When connecting to a wireless network or resource, the user or device presents its digital certificate. The network server or device verifies the certificate's authenticity by checking the CA's digital signature and ensuring it hasn't been revoked.

Strong Security: Certificate-based authentication offers strong security since it requires possession of a valid certificate and the associated private key.

Common Use Cases: Enterprise networks often use certificate-based authentication for secure access to corporate resources. Government and military networks also rely heavily on digital certificates for authentication.

Biometric Authentication

Biometric authentication uses unique physical or behavioral characteristics to verify a user's identity. Common biometric factors include:

Fingerprint Recognition: Scanning and matching fingerprints against stored templates for authentication. Found in many mobile devices for unlocking and authorization.

Retina or Iris Scanning: Analyzing the unique patterns in the retina or iris of the eye. Used in high-security environments.

Face Recognition: Analyzing facial features for identity verification. Widely used in smartphones for unlocking and user authentication. Biometric authentication provides a high level of security but may have privacy and usability considerations, such as potential data breaches or false positives/negatives.

13.3 Access Control in Wireless Security

Access control is a fundamental component of wireless security that regulates who can access specific resources within a network and what actions they can perform once they gain access. It involves defining policies, permissions, and mechanisms to restrict unauthorized users or devices from accessing sensitive data or functionalities. Here, we'll delve into access control in greater detail:

Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) is a widely used access control model that assigns permissions and access rights to users or devices based on their roles within an organization. Here's how RBAC works:

Role Assignment:

Users and devices are categorized into roles based on their responsibilities, job functions, or attributes. Common roles may include "Administrator," "Employee," or "Guest."

Role Permissions:

Each role is associated with specific permissions or access rights. For example, an "Administrator" role might have full access to all network resources, while an "Employee" role may have limited access.

Access Control Policies:

Access control policies define which roles can access particular resources and what actions they can perform. Policies are typically managed centrally and enforced at the network or application level.

RBAC simplifies access control by streamlining the management of permissions and ensuring that users or devices only have access to the resources necessary for their roles. It enhances security by minimizing the risk of unauthorized access to critical systems or data.

MAC (Media Access Control) Address Filtering

MAC address filtering is a basic access control method that restricts access to a wireless network based on the unique hardware MAC addresses of devices. Here's how it works:

Allowed and Denied Devices:

Network administrators maintain lists of allowed (whitelisted) and denied (blacklisted) MAC addresses. Whitelisted devices are granted access, while blacklisted devices are blocked.

Limitations:

While MAC filtering provides a simple way to control access, it is not foolproof. Skilled attackers can spoof MAC addresses or intercept legitimate MAC addresses, rendering this method less effective against determined intruders.

Access Control Lists (ACLs)

Access Control Lists (ACLs) are rule-based mechanisms used to define access control policies for specific network resources, such as routers or firewalls. ACLs can be applied at various network layers, including the network, transport, and application layers. Key aspects of ACLs include:

Rule Definition: ACLs consist of rules that specify which devices or users are allowed or denied access to specific resources. Rules can be based on IP addresses, port numbers, protocols, and other criteria.

Rule Priority: ACLs are typically evaluated in order, with the first matching rule being applied. Administrators must carefully arrange rules to ensure desired access control.

Granularity: ACLs offer fine-grained control, allowing administrators to define precise access policies. They can be used to permit or deny access to individual services or applications.

Dynamic Access Control

Dynamic Access Control (DAC) adapts access control policies based on changing circumstances, user attributes, or contextual information. This approach allows for more flexible and adaptive security. Key features of DAC include:

Contextual Information:

DAC takes into account factors like user location, time of day, device type, and network conditions to determine access permissions. For example, an employee may have different access privileges when working remotely compared to being on-site.

Attribute-Based Access Control (ABAC):

ABAC extends DAC by considering a broader set of attributes (e.g., user role, department, clearance level) to make access decisions. It allows for highly customized access policies based on complex criteria.

Log and Audit Access Events

Logging and auditing access events is an integral part of access control. By maintaining detailed records of who accessed what resources and when, organizations can:

Detect Anomalies: Monitoring access logs helps identify suspicious or unauthorized activities. Security teams can respond quickly to potential threats.

Accountability: Access logs provide a record of who is responsible for specific actions or data access. This accountability can deter malicious behavior and assist in investigations.

Example: An archeologist on site in Greece might use a PDA to directly access databases at the University of Minnesota in Minneapolis, and to transmit findings to that database.

13.4 Regular Updates and Patch Management

Software and firmware updates are critical for maintaining the security of wireless devices and systems. Vendors release updates to fix known vulnerabilities, and failing to apply these updates can leave systems exposed.

13.5 Security Awareness and Training

Human error remains a significant threat to wireless security. Organizations should invest in educating their users and employees about best practices, phishing attacks, and the importance of strong passwords.

Summary

- Wireless security is essential for protecting data transmitted over wireless networks.
- Encryption is a key component of wireless security, preventing unauthorized access to data.
- Wi-Fi Protected Access (WPA) and WPA2 are common encryption protocols used in wireless networks.
- Strong and unique passwords are crucial for securing Wi-Fi networks.
- MAC address filtering can restrict access to authorized devices on a network.
- Regularly updating router firmware helps patch security vulnerabilities.
- Public Wi-Fi networks are often insecure and should be used cautiously.

Keywords

Wi-Fi

Encryption

WPA (Wi-Fi Protected Access)

WPA2

WEP (Wired Equivalent Privacy)

SSID (Service Set Identifier)

Password/Passphrase

MAC Address Filtering

Router Firmware

Public Wi-Fi

VPN (Virtual Private Network)

WIDS (Wireless Intrusion Detection System)

Remote Administration

Network Security

Self Assessment

1. What is the primary purpose of wireless security?

A. To increase network speed

B. To prevent unauthorized access and protect data

C. To reduce the range of Wi-Fi signals

D. To improve device battery life

2. Which encryption protocol is considered the most secure for Wi-Fi networks as of 2021?
A. WEP
B. WPA
C. WPA2
D. WPA3

3. What is the name of the wireless network identifier?
A. IP Address
B. SSID
C. MAC Address
D. URL

4. Which of the following is a common method for securing a home Wi-Fi network?
A. Enabling WEP encryption
B. Disabling SSID broadcasting
C. Using default admin credentials
D. Sharing the Wi-Fi password with neighbours

5. Which type of attack involves an attacker intercepting and eavesdropping on wireless network traffic?
A. DDoS attack
B. Phishing attack
C. Man-in-the-Middle (MitM) attack
D. Buffer overflow attack

6. What does MAC address filtering do in wireless security?
A. Filters out spam emails
B. Filters harmful websites
C. Restricts access to specific devices
D. Filters wireless interference

7. Which security measure involves periodically changing the Wi-Fi password?
A. MAC address filtering
B. WPA3 encryption
C. Password rotation
D. Two-factor authentication

8. What is the purpose of a VPN in wireless security?
A. To increase Wi-Fi signal strength
B. To hide the SSID
C. To encrypt data traffic over public Wi-Fi
D. To disable remote administration

9. Which security protocol should be avoided due to its vulnerabilities?

A. WPA3
B. WPA2
C. WEP
D. WPA

10. What is a common risk of using public Wi-Fi networks?
A. Strong encryption
B. Slow internet speed
C. Network isolation
D. Data interception

11. Which wireless security mechanism helps detect and respond to unauthorized access attempts?
A. Firewall
B. Intrusion Detection System (IDS)
C. MAC address filtering
D. Password rotation

12. What should you do to secure your router's management interface?
A. Enable remote administration
B. Use the default admin credentials
C. Change the default username and password
D. Share the admin credentials with friends

13. Which protocol allows for secure and encrypted remote access to a network?
A. SSH (Secure Shell)
B. FTP (File Transfer Protocol)
C. Telnet
D. HTTP (Hypertext Transfer Protocol)

14. What is the purpose of a firewall in wireless security?
A. To boost Wi-Fi signal strength
B. To filter out spam emails
C. To block unauthorized network traffic
D. To encrypt data traffic

15. Which of the following is NOT a wireless security best practice?
A. Enabling strong encryption
B. Keeping the default SSID
C. Regularly updating router firmware
D. Changing default passwords

Answers for Self Assessment

1. B 2. D 3. B 4. B 5. C

6.	C	7.	C	8.	C	9.	C	10.	D
11.	B	12.	C	13.	A	14.	C	15.	B

Review Questions

1. What is the primary advantage of wireless technology compared to wired connections?
2. Name three common wireless communication standards or protocols.
3. What is the difference between Wi-Fi and cellular networks?
4. Explain the concept of "spectrum" in the context of wireless communication.
5. What are the main components of a typical Wi-Fi network setup?
6. How does Bluetooth technology differ from Wi-Fi?
7. What is the purpose of an SSID in a wireless network, and how does it relate to network security?
8. Describe the term "bandwidth" in the context of wireless communication.
9. What is the role of a router in a wireless network, and how does it differ from a modem?
10. What is the significance of encryption in wireless security, and what are some common encryption methods used in Wi-Fi networks?

Further Readings

- Wireless communications & networks by William Stallings, Pearson
- Principles of wireless networks by Kaveh Pahlavan, Pearson
- Fundamentals of wireless networking by Ron price, McGraw hill education
- Wireless networks first-step by Jim Geier, cisco press

Web Links

http://59.51.24.50:8000/wxwl/Wireless_Communications_&_Networking_Stallings_2nd.pdf

Unit 14: Security in Wireless Network

CONTENTS

Objectives

- Understanding the concepts of Security in Wireless Network
- Analyzing the use encryption protocols to protect data confidentiality in wireless communications. Understanding the Infrared LAN and its configurations.
- Identify and address common security vulnerabilities and weaknesses in wireless infrastructure.

Introduction

Wireless networks have become a crucial element of our everyday lives in our increasingly connected environment. The ease of wireless access has changed how we engage with the digital world in everything from homes and companies to public areas and cities. However, maintaining the security and integrity of wireless networks is a significant difficulty that comes along with this convenience. The challenges of wireless network security, potential threats, and recommended practices for safeguarding your wireless environment will all be covered in this chapter.

However, this convenience comes with a critical challenge—ensuring the security and integrity of wireless networks. As we rely on wireless technology for everything from sensitive business transactions to personal communications, the stakes have never been higher. The protection of our data, privacy, and digital assets hinges on our ability to safeguard wireless networks from an ever-evolving array of threats.

In this chapter, we embark on a journey into the intricate world of wireless network security. We'll explore the complexities, threats, and vulnerabilities that exist in the wireless landscape. From the casual user at a coffee shop connecting to public Wi-Fi to large organizations managing intricate wireless infrastructures, understanding wireless security is essential.

Our exploration begins with a deep dive into the significance of wireless security in today's interconnected world. We'll unravel the critical role wireless networks play and why their security is paramount. Then, we'll dissect the key components that make up wireless networks, shedding light on the inner workings of access points, routers, client devices, and encryption protocols.

14.1 Understanding Wireless Security

In the current digital era, where wireless networks are prevalent and essential to our everyday lives, understanding wireless security is essential. Wireless security refers to the practises and policies used to guard against threats and unauthorised access to wireless networks, their data, and the devices linked to them.

Some aspects related to Wireless Secuirty:

1. **Importance of Wireless Security-**Wireless networks, such as Wi-Fi and cellular, have become essential for connecting devices, accessing the internet, and enabling communication. However, their wireless nature makes them susceptible to security risks, including data interception, unauthorized access, and malicious attacks.
2. **Threat Landscape-** Wireless networks face a range of threats, including eavesdropping, man-in-the-middle attacks, rogue access points, denial-of-service attacks, and more. Understanding these threats is fundamental to implementing effective security measures.
3. **Encryption-** Encryption is a fundamental component of wireless security. It involves encoding data transmitted over wireless networks in such a way that only authorized parties can decipher it. Modern encryption protocols, like WPA3 for Wi-Fi, provide robust protection against data interception.
4. **Authentication Mechanisms-** Authentication ensures that devices and users connecting to a wireless network are legitimate and authorized. Various authentication methods, such as passwords, certificates, and two-factor authentication, play a critical role in network security.
5. **Access Control-** Access control mechanisms determine who can connect to the network and what resources they can access. Techniques like MAC address filtering, network segmentation, and role-based access control help restrict access to authorized users and devices.
6. **Regular Updates and Patching-** Keeping wireless devices, including routers and access points, up-to-date with firmware updates and security patches is essential. Outdated software can contain vulnerabilities that attackers can exploit.
7. **Network Monitoring-** Ongoing monitoring of network traffic and activities helps detect suspicious behavior and security breaches promptly. Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are used to monitor and respond to threats.
8. **Public Wi-Fi Risks-** Public Wi-Fi networks, such as those in coffee shops or airports, are often insecure. Connecting to them without taking precautions can expose your data to potential risks. Using a VPN and being cautious with sensitive transactions on public Wi-Fi is advisable.
9. **IoT Device Security-** The proliferation of Internet of Things (IoT) devices introduces new security challenges. These devices can be vulnerable to attacks if not properly secured. It's essential to secure IoT devices on your wireless network.
10. **User Education-** Educating users about best practices in wireless security, including using strong passwords, recognizing phishing attempts, and being cautious with Wi-Fi networks, is a crucial aspect of overall security.

14.2 Authentication

The threat landscape in wireless networks is diverse and continuously evolving, presenting various risks and challenges to the security and integrity of wireless communications. Understanding these threats is essential for implementing effective security measures. Wireless networks have become integral to our daily lives, but their wireless nature exposes them to vulnerabilities and threats that differ from traditional wired networks. The need for robust security in wireless networks cannot be overstated. In this chapter, we will delve into the intricacies of the threat landscape in wireless networks, shedding light on the risks that can compromise the confidentiality, integrity, and availability of wireless communications. Wireless networks face a multitude of threats, each with its own unique characteristics and potential consequences. Among the most prevalent threats is

eavesdropping, where unauthorized entities intercept and monitor data transmitted over wireless connections. Whether it's sensitive business communications, personal messages, or financial transactions, eavesdropping can expose confidential information to prying eyes.

Man-in-the-Middle Attacks

Man-in-the-Middle (MitM) attacks are a category of cyberattacks where an unauthorized entity secretly intercepts or relays communication between two parties, all while the victims believe they are communicating directly with each other. MitM attacks can occur in various communication mediums, including wired and wireless networks, and can compromise the confidentiality, integrity, and authenticity of the communication. Some details of MitM attacks:

How MitM Attacks Work

1. **Interception**: In a MitM attack, the attacker positions themselves between the two legitimate parties who are trying to communicate. This can be done physically or through various technical means, such as exploiting vulnerabilities in network infrastructure.
2. **Data Capture**: Once in the middle, the attacker can intercept and capture data being transmitted between the legitimate parties. This data may include sensitive information, such as login credentials, personal messages, or financial transactions.
3. **Modification**: In some MitM attacks, the attacker may modify the data before passing it along to the intended recipient. This alteration can lead to the compromise of data integrity, potentially resulting in unauthorized changes to the communication.
4. **Relaying**: Instead of modifying data, the attacker may simply relay messages between the parties, acting as a middleman. This allows the attacker to eavesdrop on the conversation without directly altering the data.

Common Scenarios for MitM Attacks

MitM attacks can occur in various contexts and across different communication channels:

1. **Wi-Fi Networks**: Attackers can set up rogue access points or exploit weaknesses in Wi-Fi security protocols to intercept and manipulate data transmitted over wireless networks.
2. **Email**: Attackers can intercept emails by compromising email servers or using email spoofing techniques, making it appear as if they are part of the email conversation.
3. **Web Browsing**: Attackers can exploit vulnerabilities in web browsers, web servers, or use malicious browser extensions to intercept and manipulate data exchanged during online sessions, including login credentials and personal information.
4. **Instant Messaging and VoIP**: Communication platforms like instant messaging and Voice over Internet Protocol (VoIP) can be vulnerable to MitM attacks, where attackers eavesdrop on or alter conversations.
5. **Secure Sockets Layer (SSL) Stripping**: Attackers may downgrade secure HTTPS connections to unencrypted HTTP, allowing them to intercept sensitive information in transit.

Motivations for MitM Attacks

MitM attacks can serve various malicious purposes, including:

- **Data Theft**: Stealing sensitive information such as login credentials, financial details, and personal messages for financial gain or identity theft.
- **Data Tampering**: Modifying data during transmission to carry out fraudulent activities, alter messages, or manipulate financial transactions.
- **Eavesdropping**: Gaining access to confidential information, trade secrets, or classified data for espionage or competitive advantage.

- **Session Hijacking**: Taking control of an ongoing session (e.g., online banking) to carry out unauthorized actions on behalf of the victim.
- **Espionage and Surveillance**: Monitoring the communications of individuals or organizations for intelligence gathering or surveillance purposes.

Mitigation and Prevention

MitM attacks are insidious, but they can be mitigated through various security measures, including:

- **Encryption**: Implementing end-to-end encryption using protocols like HTTPS, VPNs, or secure email can protect data from interception.
- **Authentication**: Employ strong authentication mechanisms, such as two-factor authentication (2FA), to ensure that parties are who they claim to be.
- **Secure Network Configurations**: Regularly update and secure network infrastructure to prevent unauthorized access and rogue access points.
- **Public Key Infrastructure (PKI)**: Implementing PKI can help verify the authenticity of communication parties.
- **Security Awareness**: Educating users about the risks of MitM attacks and how to recognize suspicious activities or websites.
- **Regular Software Updates**: Keep software, operating systems, and applications up to date to patch known vulnerabilities.

MitM attacks underscore the importance of maintaining robust security practices and staying vigilant in an increasingly interconnected digital world. Understanding the tactics employed by attackers is the first step toward effective prevention and mitigation.

Certificate-based authentication is a more advanced method that relies on digital certificates issued by a trusted authority, typically a Certificate Authority (CA).

Digital Certificates: Each user or device is issued a unique digital certificate that includes a public key. The corresponding private key is securely stored on the user's device.

Certificate Verification: When connecting to a wireless network or resource, the user or device presents its digital certificate. The network server or device verifies the certificate's authenticity by checking the CA's digital signature and ensuring it hasn't been revoked.

Strong Security: Certificate-based authentication offers strong security since it requires possession of a valid certificate and the associated private key.

Common Use Cases: Enterprise networks often use certificate-based authentication for secure access to corporate resources. Government and military networks also rely heavily on digital certificates for authentication.

14.3 Security in Wireless local Area Network

Wireless local area networks (WLANs) have become ubiquitous in today's world, providing users with convenient and reliable access to the internet and other resources. However, the open nature of wireless communications makes WLANs more vulnerable to security attacks than traditional wired networks. This chapter provides an overview of WLAN security, including the key threats and challenges, as well as the most common security measures. It is intended for a general audience, with no prior knowledge of WLAN security required. Security in a Wireless Local Area Network (WLAN) is critical to protect the confidentiality, integrity, and availability of data transmitted over the network. Without proper security measures, WLANs are vulnerable to various threats, including eavesdropping, unauthorized access, data manipulation, and denial of service attacks.

Example: An archeologist on site in Greece might use a PDA to directly access databases at the University of Minnesota in Minneapolis, and to transmit findings to that database.

WPA3/WPA2: Use the latest Wi-Fi Protected Access (WPA3) or its predecessor, WPA2, to encrypt data transmission. Avoid using WEP (Wired Equivalent Privacy), which is highly insecure.

AES Encryption: Prefer the use of Advanced Encryption Standard (AES) encryption, which is more secure than TKIP (Temporal Key Integrity Protocol).

Network Authentication

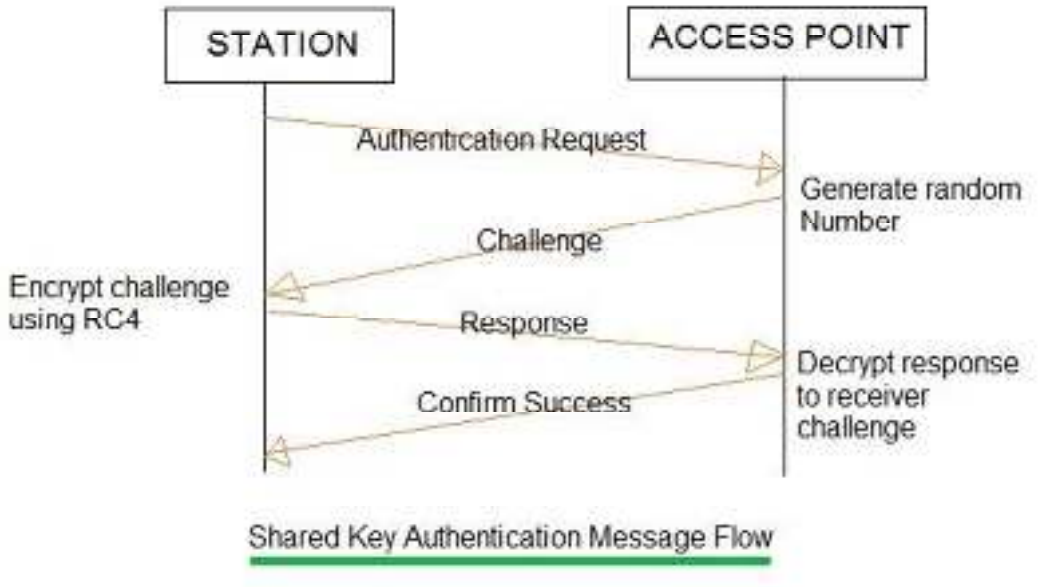
Strong Passwords/Passphrases: Enforce the use of complex and unique passwords or passphrases for WLAN access.

802.1X Authentication: Implement 802.1X authentication, which requires users or devices to authenticate before gaining network access, typically using a username and password or digital certificates.

User mobility, quick installation, adaptability, and scalability are just a few advantages of WLAN. The Wired Equivalent Privacy protocol (WEP) offers WLAN security services. During wireless transfers between stations (i.e., STAs/clients) and APs (Access Points), this protocol safeguards link-level data. Only the wireless portion of the WEP protocol handles security; the wired portion is not covered. For WLAN networks, the IEEE has established three security services: secrecy, integrity, and authentication.

Denying access to stations that fail to authenticate with the APs is handled via authentication.

Secure access to the WLAN network is ensured through confidentiality. Integrity ensures that messages are not changed while they are being transported. The WLAN system (IEEE 802.11) has two defined authentication methods. Open system authentication and shared key authentication are what they are. Without any identity verification, stations using open system authentication are permitted to connect to WLAN networks. It doesn't employ any encryption techniques or cryptography. The RC4 cryptographic technique is used for the second form of shared key authentication, as will be discussed below.

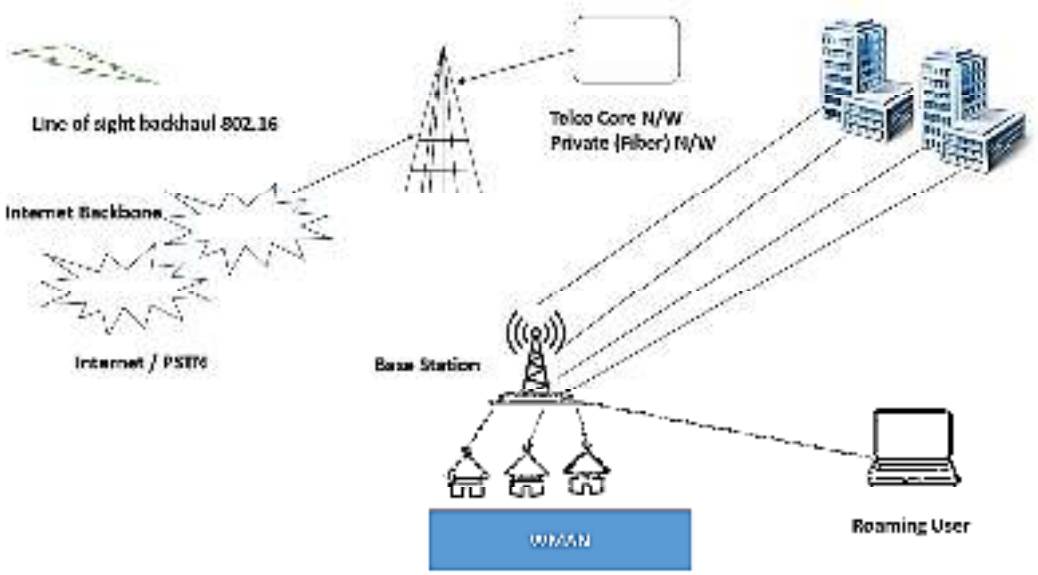


Shared Key Authentication Message Flow

14.4 Security in Wireless Metropolitan Area Network (802.16)

Security in Wireless Metropolitan Area Networks (WMANs), commonly referred to as IEEE 802.16 or WiMAX (Worldwide Interoperability for Microwave Access), is a critical aspect of ensuring the confidentiality, integrity, and availability of data transmitted over large-scale wireless networks that cover metropolitan areas. WMANs provide broadband wireless connectivity over extended geographical areas, making them valuable for urban and suburban environments. However, due to their expansive coverage, WMANs also present unique security challenges. The sole distinction between a Metropolitan Area Network (MAN) and a Wireless Metropolitan Area Network

(WMAN) is the mode of connection. It serves a range larger than 100 metres and stretches over many places within a given geographic region. It is a particular kind of wireless networking, and its coverage area is around the size of a city. In most cases, it extends across or covers a region that is bigger than a wireless local area network (WLAN) but smaller than a wireless wide area network (WWAN). Point to point and point to multipoint networks are also possible with WMAN connections. It is a more recent kind of networking technology that supports several wired ones, like Gigabit Ethernet, Resilient Packet Ring (RPR), SONET over IP, etc. The majority of a WMAN is controlled by a single organisation, such as an Internet Service Provider (ISP), a body of government, or another sizable business. To utilise WMAN, the user must have authorised access from the providers since access is only permitted for authorised users and subscribers.



Types of WMAN :

There are two fundamental types of wireless MAN

1. Back haul – It is an enterprise type of network, cellular-tower connection. It can also use WiFi hotspot. In this type of network fixed wireless is used which saves large amount of money per year. Digital Subscriber Line (DSL) can also be used in Back haul, but Wireless connection is faster and less cost than normal fiber optics connection.

2. Last mile – It is used for temporary networks means where network requirement is for a temporary period. Like some large construction buildings/sites where conventional network service (like DSL broadband and cable modem) is disrupted.

Characteristics of WMAN :

1. Connection can be Point to Point or Point to Multipoint networks.
2. Service to multiple nodes from one access point.
3. Covers a larger area within a radius up to 50 km.
4. Stable connections to the terminals.

Wireless Interoperable Metropolitan Area Exchange (WiMAX) –WiMAX is mostly used Wireless Metropolitan Area Network (WMAN) technology based on the IEEE 802.16 set of standards. It provides Multiple Physical Layer(PHY) and Media Access Control (MAC) options. It acts as an alternate wireless version of Ethernet and deployed in a variety of spectrum bands: 2.3GHz, 2.5GHz, 3.5GHz, and 5.8GHz.

Local Multipoint Distributed Service (LMDS) –It is a broadband microwave wireless transmission technology which provides reliable digital two-way voice, data and Internet services. It is a wireless point to multipoint communication system that's why called as Local Multipoint Distribution

System where Local refers to signal range limit, Multipoint refers to broadcast access, Distributed refers to transmission of wide range of data, Service refers to relationship between operators and users. It generally uses low powered, high frequency i.e. 25 to 31 GHz over a short distance.

Multi-Channel Multipoint Distributed Service (MMDS) – MMDS was previously known as Wireless Cable or Broadband Radio Service (BRS). It is a wireless telecommunication technology which operates in the ultra-high-frequency (UHF) portion of the radio spectrum between 2.5GHz and 2.7GHz and is used for telecommunications technology and general-purpose broadband networking.

Benefits of WMAN :

Covers multiple locations within a metropolitan area. Does not require high cost for infrastructure in placing fiber or copper cabling and leasing lines. Works as backups for wired networks. Easy to use, extend, exchange.

Examples of WMAN :

WiMAX

WiBro

Networking between buildings that are under construction.

14.5 Security in Wireless Wide Area Network

The sole difference between a WAN (Wide Area Network) and a WWAN (Wireless Wide Area Network) is that the link is wireless. It offers local, national, and international wireless coverage. The Wireless Wide Area Network connections are entirely wireless, unlike Wide Area Network, which may be either wired or wireless. In our daily lives, we use wireless wide area networks of various sizes, and we rely on them to transmit telephonic conversations, Web sites, and streaming video.WLAN (Wireless Local Area Network) and WWAN (Wireless Wide Area Network) are technologically distinct from one another. For instance, whereas WLAN connects to and transfers data using WiFi, WWAN does so using cellular network technologies including 2G, 3G, 4G LTE, and 5G. WWAN does not necessarily relate to a vast area; rather, it may also refer to a confined region with extensive geographic coverage. Consider a MANET (Mobile Ad Hoc Networks) with nodes on towers, skyscrapers, or aircraft. WWAN is often referred to as a Low Power and Low Bit Rate Wireless Wide Area Network (LPWAN). For instance, in the case of IoT (Internet of Things) applications, the transfer of tiny packets of data between objects.

In the above figure, several wireless devices are configured with the WLAN (Wireless Local Area Network) served by the Router-A and Router-B is a wireless router which connects to Router-A through ethernet and connected to the WAN (Wide Area Network) wirelessly flashed with DD-WRT.

Families of WWAN :

The main three families of WWAN technologies include

- GSM/UMTS
- WiMAX
- CDMA One/CDMA2000

Characteristics of WWAN :

Reduced transmission speed as compared to physical connection. It is based on IEEE 802.16 standards. On increase of distance, decrease of throughput occurs and vice versa.Getting faster due to Gigabit-Class LTE.

Advantages of WWAN :

- Global wireless coverage

- Flexible with cloud management, deploying and relocating
- Better security than WLAN
- Diverse, cost effective backup for data applications.
- Quick deployment for new applications.

Disadvantages of WWAN :

- Replacement of lost WWAN may be costly.
- To maintain the reliable network connectivity.
- To build a cost effective solution is a challenge.
- Decreased throughput during large coverage area.

Application of Wireless Wide Area Network (WWAN)

1. **Mobile correspondence**: WWAN is normally utilized for portable correspondence, for example, voice calls, text informing, and web access. This can be especially helpful for individuals who need to remain associated while progressing, like business voyagers or telecommuters.
2. **Fleet administration:** WWAN can be utilized for armada the board, like following the area of vehicles, checking their presentation, and advancing their courses. This can assist organizations with decreasing fuel costs, increment productivity, and further develop client support.
3. **Public security:** WWAN can be utilized for public wellbeing, like empowering people on call for speak with one another during crises, and giving constant reports on the area of episodes. This can assist with further developing reaction times, diminish setbacks, and improve generally security.
4. **Smart framework:** WWAN can be utilized for shrewd network applications, for example, observing the exhibition of force stations, anticipating power interest, and overseeing energy dispersion. This can assist with working on the unwavering quality and productivity of energy conveyance, lessen expenses, and increment environmentally friendly power mix.
5. **Environmental checking:** WWAN can be utilized for natural observing, like estimating air quality, water quality, and atmospheric conditions. This information can be utilized to illuminate strategy choices, work on natural administration, and safeguard general wellbeing.

Generally, WWAN has various applications that can help different ventures and work on our regular routines. By giving remote network over a huge topographical region, WWAN can empower portable correspondence, armada the executives, public wellbeing, savvy lattice, ecological observing, and different applications that can improve proficiency, security, and supportability.

Summary

- Wireless network security defends against unauthorized access, ensuring data protection.
- Encryption secures data during wireless transmission.
- Strong authentication methods verify user and device identities.
- Regular audits and updates maintain wireless network security.
- Intrusion detection systems monitor for suspicious activities.
- Access control policies restrict unauthorized network access.
- Physical security safeguards infrastructure from tampering.

- Privacy measures protect user information in wireless networks.

Keywords

Wireless security

Encryption

Authentication

Access control

Intrusion detection

WPA3

Cybersecurity

Network security

Man-in-the-Middle (MitM) attacks

Denial-of-Service (DoS)

Password protection

Self Assessment

1. What is the primary purpose of encryption in wireless network security?

A. To enhance network speed

B. To protect data confidentiality

C. To boost signal strength

D. To reduce latency

2. Which of the following is NOT a common threat in wireless networks?

A. Eavesdropping

B. MAC address filtering

C. Man-in-the-Middle (MitM) attacks

D. Rogue access points

3. What is the role of authentication in wireless network security?

A. Encrypting data

B. Managing access points

C. Verifying user and device identities

D. Enhancing signal strength

4. Which encryption protocol is commonly used for securing Wi-Fi networks?

A. HTTPS

B. AES

C. FTP

D ICMP

5. What does SSID stand for in the context of wireless networks?

A Secure Signal Identifier

B Service Set Identifier

C System Security Identifier

D Signal Strength Identifier

6. Which of the following is NOT a wireless network security best practice?

A Regular security audits

B Open guest networks

C Strong password policies

D Intrusion detection systems

7. What is the purpose of a Man-in-the-Middle (MitM) attack in wireless network security?

A To strengthen encryption

B To enhance signal strength

C To intercept and manipulate communications

D To protect against DoS attacks

8. Which security measure restricts access to specific resources within a wireless network?

A Encryption

B Access control

C Intrusion detection

D Two-factor authentication

9. What type of security attack aims to disrupt wireless network operations by overwhelming network resources with excessive traffic?

A Eavesdropping

B MAC address filtering

C Denial-of-Service (DoS)

D Encryption

10. What is the primary function of a Wireless Intrusion Detection System (WIDS)?

A To authenticate users

B To encrypt data

C To detect and respond to suspicious activities

D To boost signal strength

11. Which security measure involves marking physical locations with symbols to indicate open or vulnerable wireless networks?

A Eavesdropping

B MAC address filtering

C War driving and war chalking

D Intrusion detection

12. Which security practice aims to secure physical infrastructure, such as access points, from unauthorized access or tampering?

A Encryption

B Access control

C Physical security

D Intrusion detection

13. What security measure involves the continuous assessment of network security to identify and address vulnerabilities?

A Encryption

B Regular security audits

C MAC address filtering

D Eavesdropping

14. What is the primary purpose of access point (AP) MAC address filtering in wireless network security?

A To enhance network speed

B To verify user identities

C To restrict access to authorized devices

D To boost signal strength

15. What do IoT devices pose as a potential security challenge in wireless networks?

A Strong encryption

B Robust authentication

C Limited security measures

D Improved signal strength

Answers for Self Assessment

1.	B	2.	B	3.	C	4.	B	5.	B
6.	B	7.	C	8.	B	9.	C	10.	C
11.	C	12.	C	13.	B	14.	C	15.	C

Review Questions

1. What is the primary purpose of encryption in wireless network security, and how does it work to protect data?
2. Explain the significance of authentication mechanisms in wireless network security. What are some common authentication methods?
3. What are some common threats that wireless networks face, and how can they be mitigated or prevented?

4. Describe the role of access control in wireless network security. How does it restrict unauthorized access to network resources?
5. What is a Man-in-the-Middle (MitM) attack, and how can organizations defend against it in wireless networks?
6. How do regular security audits and vulnerability assessments contribute to the maintenance of wireless network security?
7. What are the best practices for securing a wireless network, including considerations for SSID management, guest network security, and intrusion detection?
8. Explain the concept of network segmentation and its importance in enhancing wireless network security.
9. What measures can be taken to ensure physical security for wireless network infrastructure components, such as access points and routers?
10. Why is privacy protection important in wireless networks, and what methods can be used to safeguard user information?

Further Readings

- Wireless communications & networks by William Stallings, Pearson
- Principles of wireless networks by Kaveh Pahlavan, Pearson
- Fundamentals of wireless networking by Ron price, McGraw hill education
- Wireless networks first-step by Jim Geier, cisco press

Web Links

http://59.51.24.50:8000/wxwl/Wireless_Communications_&_Networking_Stallings_2nd.pdf

LOVELY PROFESSIONAL UNIVERSITY
Jalandhar-Delhi G.T. Road (NH-1)
Phagwara, Punjab (India)-144411
For Enquiry: +91-1824-521360
Fax.: +91-1824-506111
Email: odl@lpu.co.in