PNS SCHOOL OF ENGINEERING AND TECHNOLOGY
NISHAMANI VIHAR, MARSHAGHAI, KENDRAPARA

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

LECTURE NOTE

Semester: 5th Semester

Subject: MOBILE COMPUTING

Prepared By:

Mr. BISWARANJAN SWAIN

HoD, DEPT. OF CSE

Chapter- 1
INTRODUCTION TO WIRELESS NETWORKS & MOBILE COMPUTING

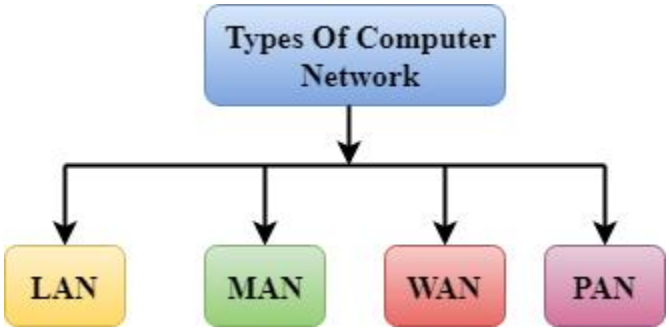
1.1Networks
1.2 Wireless Networks
1.3 Mobile Computing
1.4 Mobile Computing Characteristics
1.5 Application of Mobile Computing

1.1 Networks

A network is a collection of two or more computers (or other electronic devices) that are connected by any transmission medium. Some computer networks will have a server. A server is a powerful computer that often acts as a central hub for services in a network.
e.g. e-mails, internet access and file storage.

Types of Networks

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.
A computer network can be categorized by their size. A computer network is mainly of four types:



LAN (Local Area Network)
MAN (Metropolitan Area Network)
WAN (Wide Area Network)
PAN (Personal Area Network)

i) LAN (Local Area Network) :

The LAN is designed to connect multiple networking devices and systems within a limited geographical distance. The devices are connected using multiple protocols for proper and efficient exchange of data and services.

Advantage: Transmission of data and services is relatively higher than the other network types.
The network server acts as a central unit for the whole network.
Disadvantages: Need constant administration of experienced engineers for functioning.
Probability of leak of sensitive information by LAN administrator.

ii) MAN (Metropolitan Area Network):

The MAN is a type of network that covers the network connection, of an entire city or connection of a small area.

The area covered by the network is connected by using a wired network, like data cables.

Application
Network covers an entire town area or a portion of a city
Data transmission speed is relatively high due to the installation of optical cables and wired connections.
Advantages:
The new connection area covers an entire city on some parts using the optic cable

Disadvantages:
High probability of attack from hackers and cybercriminal due to large this.
The need for good quality flow & the Installation cost is very high.

iii) WAN (Wide Area Network):

The WAN is designed to connect devices over large distances like states or between countries. The comection is wireles in most cases and uses radio towers for communication.
The WAN network can be made up of multiple LAN and MAN networks.
Applications
The Speed of the WAN data transfer is lower than in comparison to LAN & MAN.
The WAN network uses a satellite medium to transmit data between multiple locations .

1.2 Wireless Networks:

Wireless network is a network of devices that are connected wireless medium. Wireless network uses electromagnetic waves, such as radio wave, infrared wave etc. It includes cellular telephones, Personal Digital Assistants (PDAs) and wireless networking, , wireless computer mouse and keyboards, satellite television, cordless telephones etc.

Use of wireless technology:
To span a distance beyond the capabilities of typical cabling
To avoid obstacles such as physical structures etc
To provide a backup communications link in case of normal network failure
To link portable or temporary workstations
To overcome situations where normal cabling is difficult or expensive.
To remotely connect mobile users.

Wireless communication involves:
- Radio frequency communication
- Microwave communication, for example long-range line-of-sight via highly directional antennas, or short-range communication, or
- Infrared (IR) short-range communication, for example from remote con-trols or via IRDA

In wireless communication, electromagnetic waves (rather than some form of wire) carry the data signals. Common examples of wireless equipment in use today include:
- *Cellular phones and pagers:* provide connectivity for portable and mobile applications both personal and business.
- *Global Positioning System (GPS):* allows drivers of cars and trucks, captains of boats and ships, and pilots of aircraft to ascertain their location anywhere on earth.
- *Cordless computer peripherals:* the cordless mouse is a common example; keyboards and printers can also be linked to a computer via wireless.
- *Cordless telephone sets:* these are limited-range devices, not to be con-fused with cell phones.
- *Satellite television:* allows viewers in almost any location to select from hundreds of channels.

Fig. 1.2 Wireless Network

A wireless network is a computer network that uses wireless data connections between network nodes.

Examples of wireless networks include cell phone networks, wireless local area networks (WLANs), wireless sensor networks, satellite communication networks, and terrestrial microwave networks.

IEEE Standard	Frequency/ Medium	Speed	Topology	Transmission Range	Access Method	Spread Spectrum
802.11	2.4GHz RF	1 to 2Mbps	Adhoc infrastructure	20 feet indoors.	CSMA/CA	DSSS/FHSS
802.11a	5GHz	Up to 54Mbps	Adhoc infrastructure	25 to 75 feet indoors; range can be affected by building materials.	CSMA/CA	OFDM
802.11b	2.4GHz	Up to 11Mbps	Adhoc infrastructure	Up to 150 feet indoors; range can be affected by building materials.	CSMA/CA	DSSS
802.11g	2.4GHz	Up to 54Mbps	Adhoc infrastructure	Up to 150 feet indoors; range can be affected by building materials.	CSMA/CA	DSSS
802.11n	2.4GHz/5GHz	Up to 600Mbps	Adhoc infrastructure	175+ feet indoors; range can be affected by building materials.	CSMA/CA	OFDM

Table 1.1. 802.11 Wireless Standards

1.3 MOBILE COMPUTING

Mobile Computing is a computing environment over physical mobility. The user of a mobile computing environment is able to access the data, information or other logical objects from any device in the network while on move. Mobile Computing system allows the user to perform a task from anywhere using a computing device in public (the web), corporate (business information) and personal information areas (medical record, address book etc). To make the mobile computing environment effective, it is necessary that the communication bearer is spread over both wired and wireless media.

Dimensions of Mobile Computing

It is obvious that any mobile computing system can also be stationery. It is stationery if we stop moving. Therefore we can say that stationery systems are the subset of mobile computing systems. Here we will take a look at the dimensions which make a system mobile. These dimensions are as follows:

- Location Awareness
- QoS
- Limited Device Capability
- Limited Power Supply
- Support for a wide variety of user interfaces

i)Location Awareness:

A mobile device is not always at the same place; its place is not fixed. Maintaining the location of the user is a big challenge for the application developers. There are varieties of methods for collecting data of location of user and device.

ii)Quality of Service (QoS):

Using any type of network whether wired or wireless, the quality of service must be maintained. The movement increases physical barriers and disconnection from network. So the mobile application should be developed such that the quality of service must be maintained in the wireless network .

iii)Limited Device Storage Capability:

All mobile devices are having limited storage capacity. If the device has large capacity for storing then its size would increase hence increase in the size of hand held device which is not preferable. The physical size limitations impose boundaries on mobile devices.

iv)Limited Power Supply:

Due to limited size and mobility there is a need to use smaller battery. The power supply constraint must be balanced with the processing power, storage and size constraints.

v) Support for a wide variety of user interfaces:

Mobile applications can also be handled from the stationary devices like PC's. The interfaces include touch pad, smaller displays, other pointing devices, keyboards etc.

1.4 MOBILE COMPUTING CHARACTERISTICS

Mobile Computing environment supports the following characteristics:

i) User Mobility:

User should be able to move from one physical location to another and use the same service without any interruption. For eg. User moves from Singapore to Germany and uses the internet to access his application the same way he uses in his office.

ii) Network Mobility:

User should be able to move from one network to another and use the same service. For eg. User moves from London to New Delhi and uses the same GSM phone to access his application through WAP.

iii)Bearer Mobility:

User should be able to move from one bearer to another and use the same service. For eg. User was using a service through WAP bearer in his home network in Bangalore. He moves to Chennal where WAP is not supported, he switched over to voice or SMS bearer to access the same application.

iv) Device Mobility:

User should be able to move from one device to another and use the same service. For eg. User could be a representative using his desktop at his office and during the day work outside his office, uses his palmtop or laptop to access the same application.

v) Session Mobility:

User's session should be moved from one environment to another. For eg. User was using the service through CDMA network, He entered into basement are and got disconnected from the network. He then goes to his office and uses his desktop. The unfinished session moves from mobile device to desktop.

vi) Service Mobility: User should be able to move from one service to an-other. For eg. User is writing mail. For getting some information he switches over to some other application and returns back and completes his mail sending process same way users should be able to switch between applica-tions in wireless devices.

The Mobile Computing functions can be logically divided into following major segments. The below fig. shows the segments:

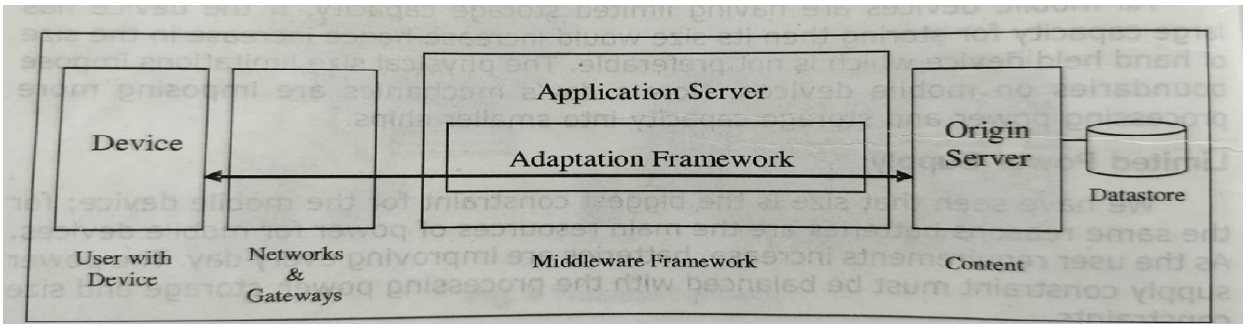


Fig. 1.3: Mobile Computing Functions Logical Division

i)User with Device: The user could have a fixed device like desktop computer or a portable or mobile device like mobile phone.

ii)Network: Whenever a user is mobile, he will be using different networks at different places at different time.

iii) Gateway: This is required to interface different transport bearers. These gateways convert one specific transport bearer to another bearer. For ex-ample, from a fixed phone we access the service by pressing different keys on the telephone. These keys generate DTMF (Dual Tone Multi Frequency). These are analog signals which are then converted into digital by IVR (In-teractive Voice Response) gateway to interface with a compute application.

iv) Middleware: A s/w layer between a user application and operating system can be termed as middleware.

v)Content: This is the place or server where originally the content is stored. This could be an application, system or even a collection of systems. This server will access the data store for reference.

1.5 APPLICATIONS OF MOBILE COMPUTING

Mobile computing, which involves the use of portable devices like smartphones, tablets, laptops, and wearables to access and process data on the go, has transformed numerous industries and daily activities. Enabled by wireless communication, mobility, and powerful hardware, mobile computing has a wide range of applications. Below is a concise overview of key applications, organized by domain:

1. Communication and Social Interaction

- ***Instant Messaging and Social Media:*** Apps like WhatsApp, Telegram, and Instagram enable real-time text, voice, and video communication, fostering social connectivity across the globe.
- ***Email and Video Conferencing:*** Mobile email clients (e.g., Gmail) and platforms like Zoom or Microsoft Teams allow professionals and individuals to communicate seamlessly while mobile.
- ***VoIP and Unified Communications:*** Apps like Skype and Google Meet leverage mobile devices for cost-effective voice and video calls over the internet.

2. Business and Productivity

- ***Remote Work and Collaboration:*** Tools like Slack, Trello, and Google Workspace enable employees to manage tasks, collaborate on projects, and access documents from anywhere.
- ***Mobile Banking and Finance:*** Apps like PayPal, Google Pay, and banking apps allow users to manage accounts, transfer money, pay bills, and invest on the go.
- ***E-commerce:*** Platforms like Amazon and Flipkart enable shopping, price comparison, and order tracking via mobile apps.
- ***Customer Relationship Management (CRM):*** Mobile CRM apps (e.g., Salesforce) help businesses manage customer interactions and sales pipelines remotely.

3. Entertainment and Media

- ***Streaming Services:*** Apps like Netflix, YouTube, and Spotify provide on-demand access to movies, music, and podcasts.
- ***Gaming:*** Mobile games (e.g., PUBG, Candy Crush) leverage powerful mobile hardware for immersive experiences.
- ***Augmented Reality (AR) and Virtual Reality (VR):*** AR apps like Pokémon Go or VR experiences use mobile sensors for interactive entertainment.

4. Healthcare

- ***Telemedicine:*** Mobile apps enable remote consultations, prescription management, and health monitoring (e.g., Teladoc, Practo).
- ***Fitness and Wellness:*** Wearables and apps like Fitbit and MyFitnessPal track physical activity, heart rate, and diet.
- ***Medical Records and Diagnostics:*** Mobile devices allow doctors to access patient records and diagnostic tools (e.g., portable ultrasound devices) in real time.

5. Education

- ***E-Learning:*** Platforms like Coursera, Khan Academy, and Duolingo provide access to courses and learning materials on mobile devices.
- ***Virtual Classrooms:*** Apps like Google Classroom and Zoom facilitate remote learning and interactive sessions.
- ***Educational Tools:*** Mobile apps for note-taking (e.g., Evernote) and language learning (e.g., Babbel) enhance accessibility.

6. Navigation and Location-Based Services

- ***GPS and Mapping:*** Apps like Google Maps and Waze provide real-time navigation, traffic updates, and route planning.
- ***Location-Based Services:*** Apps like Uber and Yelp use geolocation for ride-hailing, finding nearby restaurants,

or checking local events.

- ***Geotagging and Tracking:*** Mobile devices enable location tracking for logistics, fleet management, and personal safety.

7. Transportation and Logistics

- ***Ride-Sharing and Mobility:*** Apps like Uber, Lyft, and Ola streamline transportation services.
- ***Fleet Management:*** Mobile apps track vehicle locations, optimize routes, and manage delivery schedules.
- ***Public Transit:*** Apps like Citymapper provide real-time transit schedules and ticketing.

8. Retail and Marketing

- ***Mobile Payments:*** Contactless payment apps like Apple Pay and Samsung Pay simplify transactions.
- ***Personalized Marketing:*** Retailers use mobile apps to send targeted promotions based on user preferences and location.
- ***Inventory Management:*** Mobile devices help retailers track stock and manage supply chains.

9. Smart Cities and IoT

- ***Smart Home Control:*** Mobile apps control IoT devices like smart lights, thermostats, and security cameras (e.g., Google Home, Amazon Alexa).
- ***Urban Services:*** Mobile computing supports smart parking, waste management, and public safety apps.
- ***Environmental Monitoring:*** Mobile devices collect data on air quality, weather, and energy usage.
  10. Emergency Services and Public Safety
- ***Emergency Alerts:*** Mobile apps broadcast alerts for natural disasters, amber alerts, or public safety warnings.
- ***First Responder Tools:*** Mobile devices provide real-time data to police, firefighters, and paramedics (e.g., incident reporting, location tracking).
- ***Personal Safety Apps:*** Apps like bSafe allow users to share locations or trigger emergency alerts.

11. Agriculture

- ***Precision Farming:*** Mobile apps monitor soil conditions, weather, and crop health (e.g., FarmLogs).
- ***Market Access:*** Farmers use mobile platforms to check commodity prices and connect with buyers.
- ***Livestock Management:*** Apps track animal health and breeding schedules.

12. Travel and Tourism

- ***Travel Planning:*** Apps like TripAdvisor and Booking.com assist with hotel bookings, flight tracking, and itinerary planning.
- ***Translation and Guides:*** Mobile apps like Google Translate and travel guides enhance the travel experience.
- ***Augmented Reality Tours:*** AR apps provide interactive guides for historical sites and museums.

****

Chapter- 2

INTRODUCTION TO MOBILE DEVELOPMENT FRAMEWORK

2.1 C/S architecture
2.2 n-tier architecture
2.3 n-tier architecture and www
2.4 Peer-to Peer architecture
2.5 Mobile agent architecture

What is mobile development framework?

A mobile development framework is a software framework that is designed to support mobile app development. It is a software library that provides a fundamental structure to support the development of applications for a specific environment. Frameworks can be in three categories: native frameworks for platform-specific development, mobile web app frameworks, and hybrid apps, which combine the features of both native and mobile web app frameworks.

2.1 CLIENT-SERVER ARCHITECTURES

The Client-server architecture is a distributed application structure that partitions task or workload between the client and server.

In a client-server model there are two different programs residing on separate machines. One program is said to be the client and the other is said to be the server.

The client generates the request and the server serves the client's request. In the real world there is one server and more than one client.

Client: Client is a computer (Host) i.e. capable of receiving information or using a particular service from the service providers (Servers).

Servers: Server is a remote computer which provides information (data) or access to particular services. So, it is basically the Client requesting something and the Server serving it as long as its present in the database.

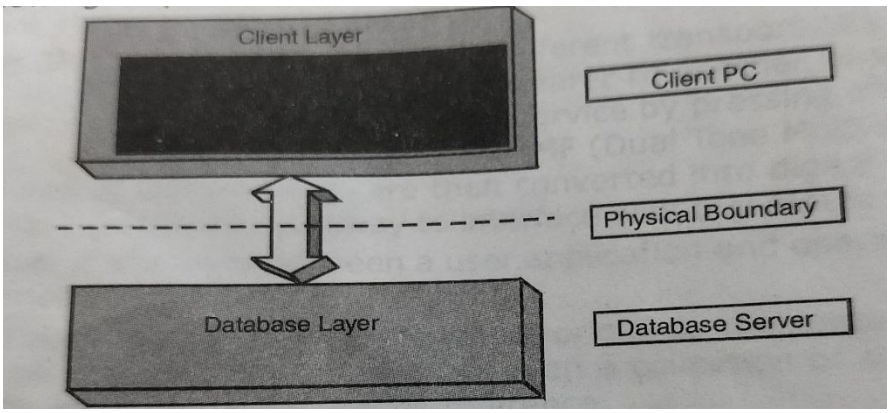


Fig. 2.1 Client-Server Architecture

There are few steps to follow to interact with the servers a client.

Working of C/S architecture:

- User enters the URL(Uniform Resource Locator) of the website or file.

-The Browser then requests the DNS(DOMAIN NAME SYSTEM) Server.

-DNS Server lookup for the address of the WEB Server.

- DNS Server responds with the IP address of the WEB Server.

-Browser sends over an HTTP/HTTPS request to WEB Server's IP (provided by DNS server). Server sends over the necessary files of the website.

-Browser then renders the files and the website is displayed. This rendering is done with the help of DOM (Document Object Architecture) interpreter, CSS interpreter and JS Engine collectively known as the JIT or (Just in Time) Compilers.

Advantages of Client-Server architecture:

Centralized system with all data in a single place.

Cost efficient requires less maintenance cost and Data recovery is possible.

The capacity of the Client and Servers can be changed separately.

Disadvantages of Client-Server architecture:

Clients are prone to viruses, Trojans and worms if present in the Server or uploaded into the Server.

Server are prone to Denial of Service (DOS) attacks.

Data packets may be spoofed or modified during transmission.

Phishing or capturing login credentials or other useful information of the user are common and MITM (Man in the Middle) attacks are common.

2.2 N-TIER ARCHITECTURES

The tier architecture, is the breaking down of an application into logical chunks that are called tiers. Tiers can exist on the same computer and be connected virtually or logically or on different machines,

The simplest examples of tier architecture are 1-tier, 2-tier, and 3-tier.

Presentation Tier (Client Layer):

- Purpose: Handles user interaction and displays data.
- Components: User interfaces (e.g., web browsers, mobile apps, desktop GUIs).
- Technologies: HTML, CSS, JavaScript, React, Angular, or native mobile frameworks.
- Example: A web form where users input data or view results.

Application Tier (Business Logic Layer):

- Purpose: Processes business rules, logic, and computations.
- Components: Application servers, APIs, or middleware that execute the core functionality.
- Technologies: Java, Python (e.g., Django, Flask), Node.js, .NET, or PHP.
- Example: Validating user inputs or calculating a shopping cart total.

Data Tier (Data Storage Layer):

- Purpose: Manages data storage, retrieval, and persistence.
- Components: Databases, file systems, or data warehouses.

- Technologies: SQL databases (e.g., MySQL, PostgreSQL), NoSQL databases (e.g., MongoDB), or cloud storage.
- Example: Storing user profiles or transaction records.

1-tier architecture is the simplest, single tier on single user, and is the equivalent of running an application on a personal computer. All the required components to run the application are located within it. User interface, business logic, and data storage are all located on the same machine. They are the easiest to design, but the least scalable. Because they are not part of a network, they are useless for designing web applications.

2-tier architectures provide network between a client and a server.

The basic web model is a 2-tier architecture. A web browser makes a request from a web server, which then processes the request and returns the desired response, in this case, web pages.

In this case the client directly communicates with a server. This is useful for smaller applications with limited users and data. It is less scalable and secure compared to 3-tier architecture.

Ex: Library management system, websites with smaller no of users.

3-tier architecture is most commonly used to build web applications. In this model, the browser acts like a client, middleware or an application server contains the business logic, and database servers handle data functions. This approach separates business logic from display and data.

More complex to build and maintain. It offers better scalability, security and performance. It is suitable for larger applications and large user base.

Ex: Modern e-commerce website

Benefits of N-Tier Architecture:

- ***Scalability:***
  - Each tier can be scaled independently (e.g.,
  - adding more database servers without changing the application logic).
  - Supports horizontal scaling (e.g., load balancers for the application tier).
- ***Modularity:***
  - Changes in one tier (e.g., updating the UI) don't affect others.
  - Facilitates code reuse and maintenance.
- ***Flexibility:***
  - Tiers can use different technologies (e.g., a Python backend with a React frontend).
  - Easy to integrate new features or third-party services.
- ***Security:***
  - Sensitive data and logic are isolated in the application and data tiers, reducing exposure.
  - Security mechanisms (e.g., firewalls) can be applied between tiers.
- ***Maintainability:***
  - Developers can work on specific tiers without impacting others.
  - Simplifies debugging and testing.
- ***Reusability:***
  - Business logic in the application tier can be reused across multiple presentation layers (e.g., web and mobile apps).

Drawbacks of N-Tier Architecture

- ***Complexity:***
  - Designing and managing multiple tiers increases system complexity.
  - Requires careful planning for inter-tier communication.
- ***Latency:***
  - Communication between tiers (especially if physically separated) can introduce delays.
- ***Cost:***
  - Deploying and maintaining multiple servers or cloud instances increases infrastructure costs.
- ***Development Overhead:***
  - Initial setup and configuration of tiers require more effort compared to monolithic architectures.

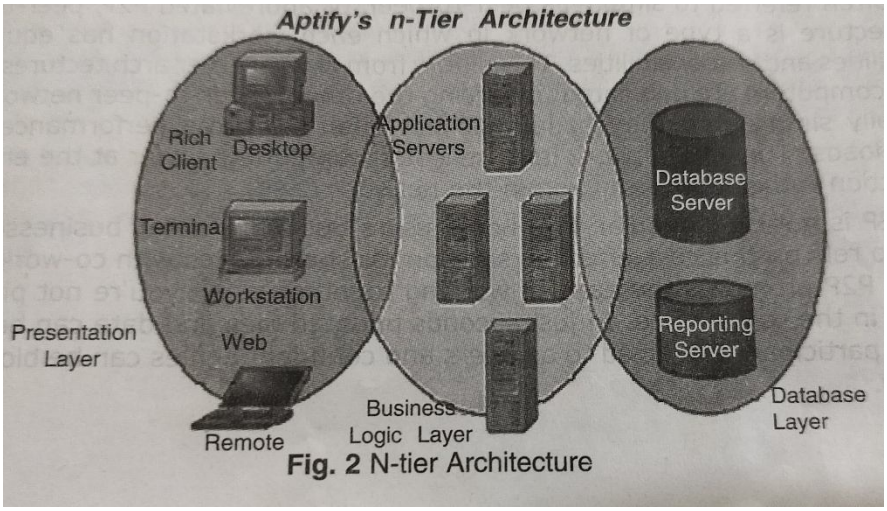


Fig. 2.2 N-tier Architecture

Today a large portion of the infrastructure of the WWW is based on N-tier architecture. Let us have a look at it.

2.3 N-TIER ARCHITECTURES AND THE WWW

The web is a client-server mechanism where the client and server communicate through HTTP (Hyper Text Transfer Protocol). The clients are the browsers which interpret the user interface in HTML and other client side scripting languages for rendering user interface. The servers are the Web Servers which serves the client request coming from HTTP with HTML response.

There are 3 components of web:

- Uniform Resource Locator (URL): serves as system for resources on web.
- HyperText Transfer Protocol (HTTP): specifies communication of browser and server.
- Hyper Text Markup Language (HTML): defines structure, organization and content of webpage

Ex: the shopping-cart web application.

The *client tier* interacts with the user through GUIs and with the application and the application server. In web applications*, this client tier* is a web browser.

The client tier communicates with the application server.

The business logic tier controls an application's functionality by performing detailed processing. In the shopping cart example, this tier completes credit card authorization and calculates things like shipping costs and sales tax.

The business logic tier then communicates with the database server and completes the task.

2.4 PEER-TO-PEER ARCHITECTURE

Peer-to-peer architecture is a type of network in which each workstation has equivalent capabilities and responsibilities.

Peers (Nodes):

- Individual devices (computers, smartphones, etc.) that participate in the network.
- Each peer can initiate requests, provide resources, and store data.
- Example: A computer sharing files in a BitTorrent network.

Peer-to-peer networks are generally simpler but they usually do not offer the same performance under heavy loads. The P2P network itself relies on computing power at the ends of a connection rather than from within the network itself.

P2P is used for personal file sharing. P2P promotes the ease of working together when you're not physically located in the same office. In just seconds updated files and data can be shared with all participants referred to as peers and confidential files can be blocked for security.

One could view the peer-to-peer architecture as placing a server module as well as a client module on each computer. Thus each computer can access services from the software modules on another computer, as well as providing services to the other computer.

The below fig. depicts peer-to-peer architecture:

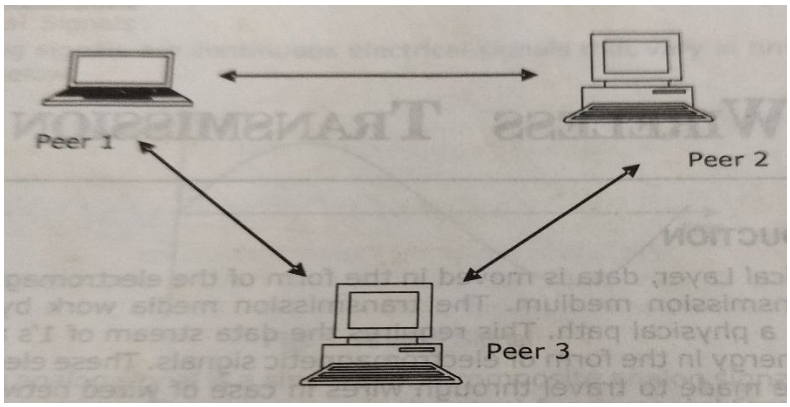


Fig. 2.3 Peer-to-Peer Architecture

The advantages of peer-to-peer include:

- No need for a network administrator
- Network is fast/inexpensive to setup & maintain
- Each PC can make backup copies of its data to other PCs for security.
- Easiest type of network to build, peer-to-peer is perfect for both home and office use.

Disadvantages:

Security:

- Lack of central control makes it harder to enforce security policies.
- Risks include malware distribution, unauthorized access, or data integrity issues.
- Example: Malicious files shared in P2P file-sharing networks.

Performance Variability:

- Dependent on peer availability and resources, leading to inconsistent performance.
- Example: Slow downloads if few peers have the desired file.

Peer Discovery:

- Finding peers with specific resources can be complex, especially in unstructured P2P systems.

Freeloading:

- Some peers may consume resources without contributing (e.g., downloading without uploading).
- Example: BitTorrent uses tit-for-tat mechanisms to discourage freeloading.

Complexity:

- Managing dynamic peer connections and ensuring data consistency is challenging.

Legal Issues:

- P2P systems are often associated with illegal file sharing (e.g., copyrighted content).

2.5 MOBILE AGENT ARCHITECTURE

A mobile agent is a self-contained program that can autonomously migrate from one computer to another within a network, executing tasks at each host.

Mobile agents have the following properties:

A self-contained program with code, data, and execution state.

Capable of migrating between hosts, making decisions, and performing tasks autonomously.

Example: An agent collecting stock market data from multiple servers.

- They are the programs which hide data and code which are transported from client machine to remote server for execution.

- They execute asynchronously.

  They are software components which move from server to server in a network while keeping the state of application intact.

  Example Flow:
  - An agent is created to monitor server health across a network.
  - It migrates to Server A, collects CPU usage data, then moves to Server B.
  - After collecting data from all servers, it returns to the origin with results.

  Advantages of Mobile Agent Architecture:
  - Reduced Network Bandwidth:
    - Agents move to data sources, minimizing data transfer over the network.
    - Example: Instead of transferring a large dataset, an agent processes it locally.
  - Autonomy and Flexibility:
    - Agents operate independently, adapting to changing conditions without constant server interaction.
    - Example: An agent rerouting to a new server if one is unavailable.
  - Scalability:
    - Distributes computation across nodes, reducing load on any single server.
    - Example: Multiple agents collecting data from distributed sensors.
  - Fault Tolerance:
    - Agents can continue tasks by migrating to operational hosts if a node fails.
    - Example: An agent resuming data collection on another server after a crash.
  - Asynchronous Operation:
    - Agents can work offline or in disconnected environments, resuming when connectivity is restored.
  - Dynamic Adaptation:
    - Agents can modify their behavior based on local conditions (e.g., resource availability).

  Disadvantages of Mobile Agent Architecture
  - Security Risks:
    - Malicious Agents: Agents may harm hosts (e.g., injecting malware).
    - Hostile Hosts: Hosts may tamper with or steal agent data.
    - Solution: Strong authentication, encryption, and sandboxing.
  - Complexity:
    - Designing and managing mobile agents is complex, especially for migration and state management.
    - Example: Ensuring state consistency during network interruptions.
  - Platform Dependency:
    - Agents require compatible platforms on all hosts, limiting interoperability.
    - Example: Java-based agents may not run on non-Java platforms.
  - Performance Overhead:
    - Migration (serialization, transfer, deserialization) can introduce latency.
    - Example: Slow migration over low-bandwidth networks.
  - Resource Management:
    - Hosts must allocate resources (CPU, memory) for agents, which can strain low-power devices.
  - Debugging and Monitoring:
    - Tracking mobile agents across nodes is challenging, complicating error detection.

****

Chapter- 3
WIRELESS TRANSMISSION

3.1 INTRODUCTION

Wireless transmission is a form of unguided media. Wireless signals are spread over in the air and are received and interpreted by appropriate antennas.

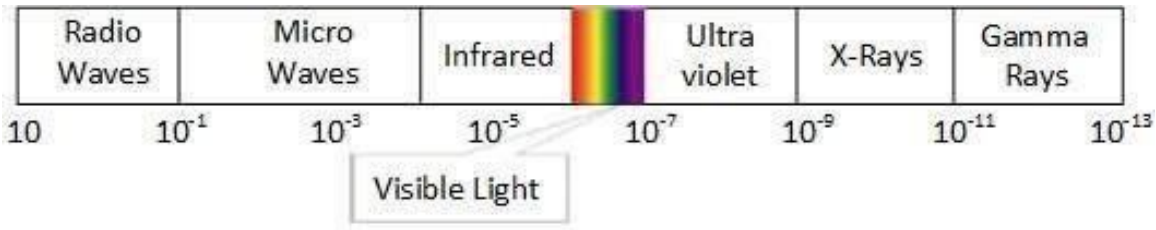
When an antenna is attached to electrical circuit of a computer or wireless device, it converts the digital data into wireless signals and spread all over within its frequency range. The receptor on the other end receives these signals and converts them back to digital data.

3.1 INTRODUCTION

At Physical Layer, data is moved in the form of the electromagnetic signals across a transmission medium. This requires the data stream of 1's and O's to be turned into energy in the form of electromagnetic signals. These electromagnetic signals can be made to travel through wires in case of wired networks and can be made to travel through open space in case of wireless networks.

Radio transmission (traveling of radio waves through air) can take place from many different frequency bands. Each frequency band has certain advantages with regards to data transmission. Each frequency range has a band designator and each range of frequencies behaves differently and performs different functions. The frequency spectrum is shared by civil, government, and military users of all nations according to International Telecommunications Union (ITU) regulations.

A little part of electromagnetic spectrum can be used for wireless transmission.



3.2 SIGNALS

Signals are the physical representation of the data. When users of a communication system want to exchange data, this is made possible through the transmission of signals. Signals are functions of time and location. Signal parameters represent the data values. Data can be analog or digital signals. For example, human voice is analog data (signals). When anyone speaks in the microphone, the speech signals are converted to analog signals. These analog signals can later on be converted to digital signals for processing. In the memory of computer, digital signals are stored for the purpose of processing.

The signals of interest for radio transmission are periodic signals. Periodic Signals are signals that repeat themselves after a certain amount of time. The signal parameters are the amplitude A, the frequency F and the phase shift j. Sine wave is a periodic signals and that is why they are of special interest. It is possible to construct a periodic signal using sine and cosine functions. The time domain representation of a signal depicts the amplitude of a signal versus time. This is used in oscilloscope where amplitude is measured in volts.

In a communication system, a transmitter encodes a message into a signal, which is carried to a receiver by the communications channel. For example, the WIRELESS TRANSMISSION words "Ba Ba Black Sheep" might be the message spoken into a telephone. The telephone transmitter converts the sounds into electrical signals. These signals are transmitted to the receiving telephone by wires; and at the receiving end, it is reconverted into sounds.

There are two types of signals:

Analog Signals
Digital Signals
Analog signals are continuous electrical signals that vary in time as shown In figure below.

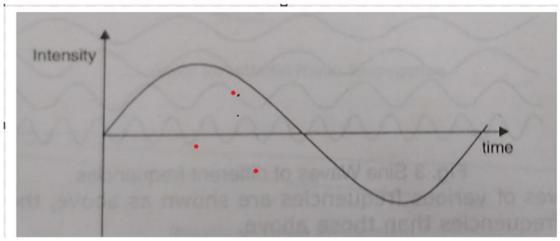


Fig. 1 Analog Signal

A simple analog signal is a sine wave. A composite analog signal is composed of multiple sine waves. The sine wave is the most fundamental form of a periodic analog signal. A periodic signal completes a pattern within a time frame called a period and this pattern is repeated over subsequent identical periods. The completion of one full pattern is called a cycle. An aperiodic signal changes without exhibiting a pattern or cycle that repeats over time. Both analog and digital signals can be periodic and aperiodic. In data communication we use periodic analog signals and aperiodic digital signals.

Analog signals require much less bandwidth, only about 4.5 MHz with a 143.2 mbps of data rate. Because the circuitry required for analog transmission is less complex, the cost is lower compared to that of digital signals. For example, telephone voice signal is analog.

Digital signals are transmission signals that carry information in a discontinuous stream of on/off pulses. They consist of pulses or digits with discrete levels or values. The value of each pulse is constant, but there is an abrupt change from one digit to the next. Digital signals have two amplitude levels called nodes, the value of which are specified as one of two possibilities such as 1 or 0, high or low, true or false. Digital signals require much high bandwidth, as much as 74.25 MHz with a data rate of 1485 mbps. The circuitry required for digital transmission is more complex, the cost may be higher.

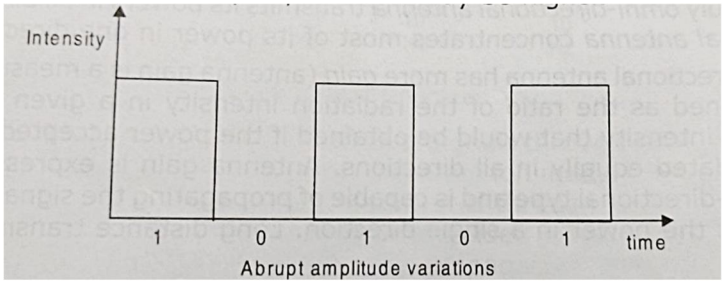


Fig. 2 Digital Signal

3.3 PERIOD AND FREQUENCY

As mentioned earlier, period refers to the amount of time (in seconds) a signal needs to complete one cycle. Frequency is the measurement of the number of occurrences of a repeated event per unit of time. It can also be defined as number of periods in one second. The result is measured in hertz (Hz). 1 Hz means that an event repeats once per second, 2 Hz is twice per second, and so on.

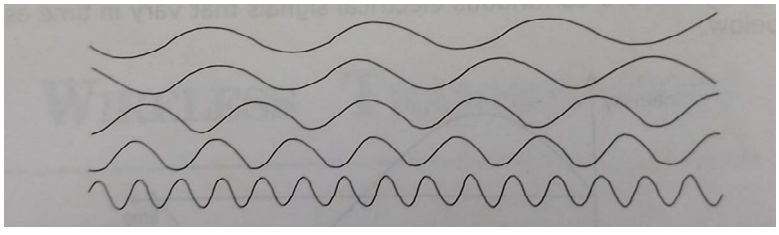


Fig. 3 Sine Waves of different frequencies

Sine waves of various frequencies are shown as above, the bottom waves have higher frequencies than those

above.

Bandwidth

The range of frequencies that a medium can pass is called its bandwidth. It is a property of a medium. It is the difference between the highest and the lowest frequencies that a medium can satisfactorily pass. For example if a medium can pass frequencies between 1000 and 5000, its bandwidth is 5000-1000 i.e. 4000 Hz. We can say that we need a medium with a bandwidth of 4000 Hz if we want to send signal without losing a significant part of it.

3.4 ANTENNAS

An antenna (popularly known as aerial) is a transducer (a device for converting energy from one form to another for the purpose of measurement of a physical quantity or for information transfer) designed to transmit or receive radio waves. Antennas are used in systems such as radio and television broadcasting, point-to-point radio communication, wireless LAN, radar, and space exploration. Antennas usually work in air or outer space. Antennas have practical uses for the transmission and reception of radio frequency signals (radio, TV, etc.), which can travel over great distances at the speed of light.

There are two types of antennas:

Omni-directional (radiates equally in all directions)

Directional (radiates more in one direction than in the other)

A truly omni-directional antenna transmits its powers in all directions whereas directional antenna concentrates most of its power in one direction.

A directional antenna has more gain (antenna gain is a measure of directivity. It is defined as the ratio of the radiation intensity in a given direction to the radiation intensity that would be obtained if the power accepted by the antenna were radiated equally in all directions. Antenna gain is expressed in dBi) than the omni-directional type and is capable of propagating the signal farther because It focuses the power in a single direction. Long distance transmissions require high power and directive radiation pattern. Wireless LANs and WANs use omni-directional antennas and wireless MANs use antennas that are directive.

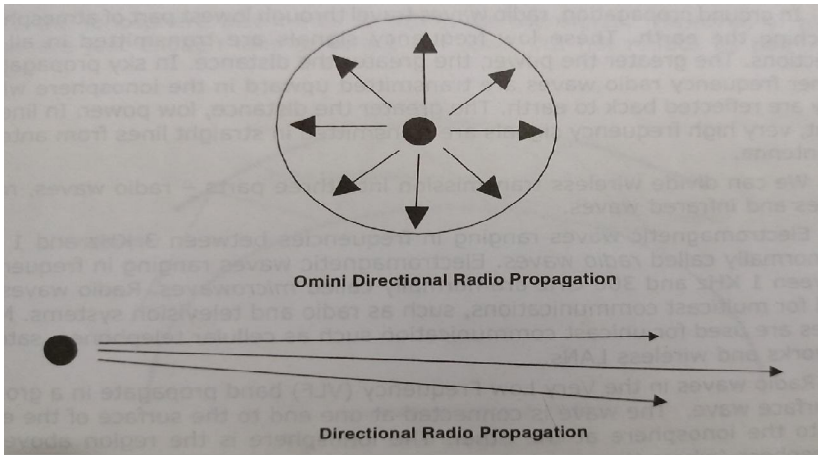


Fig. 4 Two types of Antennae

An antenna array is two or more antennas coupled to a common source or load to produce a specific directional radiation pattern.

3.5 SIGNAL PROPAGATION

The electromagnetic spectrum classifies electromagnetic energy according to frequency. As shown in fig. below, the electromagnetic spectrum ranges from energy waves having extremely low frequency to energy waves having much higher frequency, such as x-rays.

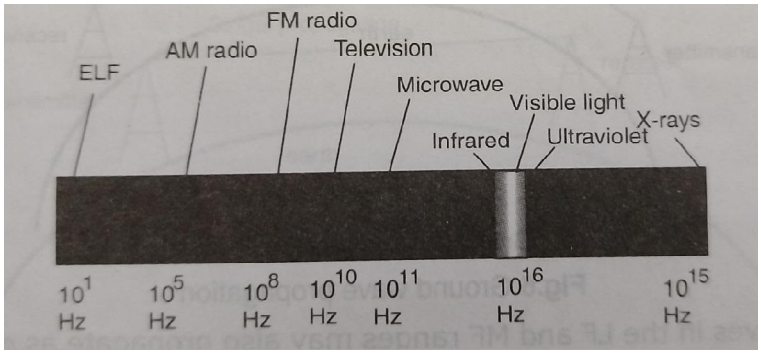


Fig. 5 Electromagnetic Spectrum

Signal Propagation is the traveling of signals through some medium In case of both wired and wireless networks. In case of guided media, it is through various types of cables like twisted pair, coaxial etc. In case of unguided media, signals travel through air. There is ground propagation, sky propagation and line-of-sight propagation.

i) Ground propagation:

In ground propagation, radio waves travel through lowest part of atmosphere, touching the earth. These low frequency signals are transmitted in all the directions. The greater the power, the greater the distance.

- Effective for long-distance communication over land.
- Affected by terrain, vegetation, and ground conductivity.
- Signal strength decreases with distance due to absorption by the Earth.

Up to 2 MHz (mainly for AM radio broadcasting).

AM radio, maritime communication.

ii) Sky propagation:

In sky propagation, higher frequency radio waves are transmitted upward in the Ionosphere where they are reflected back to earth. The greater the distance, low power.

2 MHz – 30 MHz (shortwave).

- Allows long-distance communication (hundreds to thousands of miles) by "bouncing" signals off the ionosphere.
- Affected by time of day, season, and solar activity (e.g., sunspots).
- Susceptible to fading due to ionospheric variations.

International broadcasting, amateur radio, long-distance military communication.

iii) Line-of-sight propagation:

In line-of-sight, very high frequency signals are transmitted in straight lines from antenna to antenna.

Above 30 MHz (VHF, UHF, microwaves).

: Limited by the horizon and obstacles; needs towers or satellites for longer distances.

- Limited by the horizon (typically 20–50 miles, depending on antenna height).
- Obstacles like buildings or mountains block the signal.
- Minimal signal distortion in clear conditions.

FM radio, TV broadcasting, cellular networks, satellite communication, Wi-Fi.

We can divide wireless transmission into three parts radio waves, micro waves and infrared waves.

Electromagnetic waves ranging in frequencies between 3 KHz and 1 GHz are normally called **radio waves**. Electromagnetic waves ranging in frequencies between 1 KHz and 300 GHz are normally called **microwaves**. Radio waves are used for multicast communications, such as radio and television systems. Micro waves are used for unicast communication such as cellular telephones, satellite networks and wireless LANS.

Radio waves in the Very Low Frequency (VLF) band propagate in a ground, or surface wave. The wave is connected at one end to the surface of the earth and to the ionosphere at the other. The Ionosphere is the region above the troposphere (where the air is), from about 50 to 250 miles above the earth. It is a collection of ions, which are atoms that have some of their electrons stripped off leaving two or more electrically charged objects. The sun's rays cause the ions to form which slowly recombine. The propagation of radio waves in the presence of ions is drastically different than in air, which is why the ionosphere plays an important role in most modes of propagation. Ground waves travel between two limits, the earth and the ionosphere, which acts like a duct. Since

the channel curves with the earth, the ground wave will follow. Therefore very long range propagation is possible using ground waves.

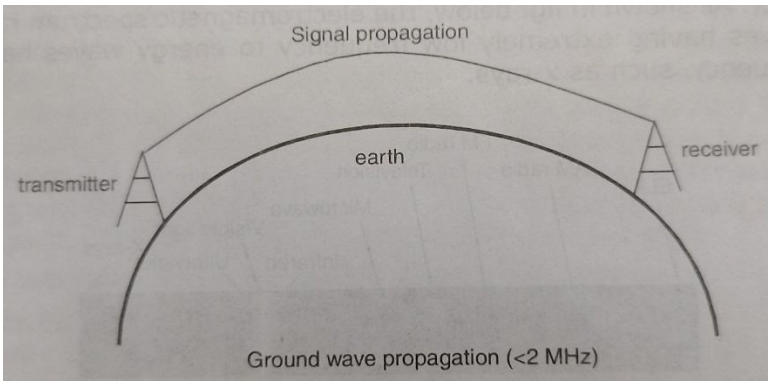


Fig.6 Ground wave propagation

Radio waves in the LF and MF ranges may also propagate as ground waves, but suffer significant losses, or are attenuated, particularly at higher frequencies. But as the ground wave mode fades out, a new mode develops: the sky wave. Sky waves are reflections from the ionosphere. While the wave is in the ionosphere, it is strongly bent, or refracted, ultimately back to the ground. From a long distance away this appears as a reflection. Long ranges are possible in this mode also, up to hundreds of miles. Sky waves in this frequency band are usually only possible at night, when the concentration of ions is not too great since the ionosphere also tends to attenuate the signal. However, at night, there are just enough ions to reflect the wave but not reduce its power too much.

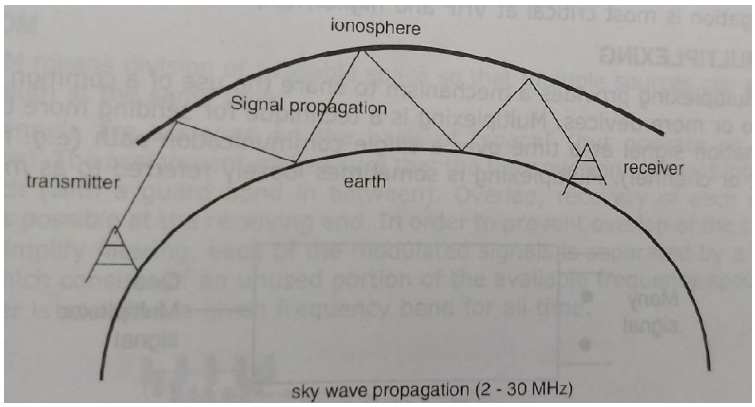


Fig.7 Sky wave propagation

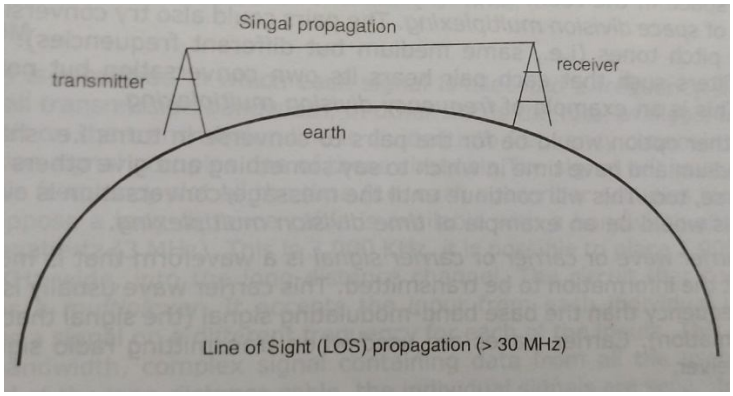


Fig.8 LOS propagation

3.6 MULTIPLEXING

Multiplexing provides a mechanism to share the use of a common channel by two or more devices. Multiplexing is a technique for sending more than one information signal at a time over a single communication path (e.g. medium, circuit or channel). Multiplexing is sometimes loosely referred to as many into one.

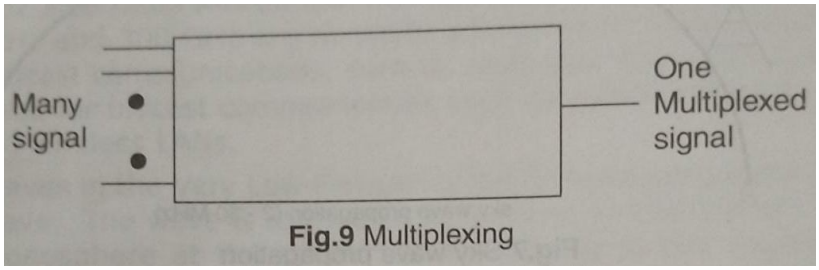


Fig.9 Multiplexing

Let us now look at basic examples of multiplexing. People who share an office in their workplaces also share a communication medium (air inside the room) to converse at the same time.

If there are six people in the office and they all want to talk at the same time, there obviously will be some interference between the conversations taking place. To reduce the interference they may divide themselves into three groups of two, such that the conversation is between each pair of people. If the pairs continue, talking whilst sitting next to each other, the interference would still be present.

The best way for each pair to converse with minimal interference would be to sit a few feet away from the other pairs (within the same room) and converse. They would still be sharing the same medium for their conversations but the physical space in the room would be divided for each conversation. This is an example of space division multiplexing. The pairs could also try conversing using different pitch tones (i.e., same medium but different frequencies). This will require filters such that each pair hears its own conversation but not that of others. This is an example of frequency division multiplexing.

Another option would be for the pairs to converse in turns i.e. sharing the same medium and have time in which to say something and give others a chance to converse, too. This will continue until the message/conversation is over for all pairs. This would be an example of time division multiplexing.

A carrier wave or carrier or carrier signal is a waveform that is modified to represent the information to be transmitted. This carrier wave usually is of much higher frequency than the base band-modulating signal (the signal that contains the information). Carrier waves are used when transmitting radio signals to a radio receiver.

Mobile Cellular Systems use various techniques to allow multiple users to access the same radio spectrum at the same time. Multiplexing can be achieved in a number of ways. The various techniques used in the systems are as follows:

- Space Division Multiplexing (SDM)
- Frequency Division Multiplexing (FDM)
- Time Division Multiplexing (TDM)
- Code Division Multiplexing (CDM)

3.6.1 SDM

SDM means division of available space so that multiple sources can access the medium at the same time.

Channels are assigned on the basis of "space" (but operate on same frequency). The assignment makes sure that the transmission does not interfere with each (with a guard band in between). Overlap, recovery of each of the signals is possible at the receiving end. In order to prevent overlap of the signals and to simplify filtering, each of the modulated signals is separated by a guard band, which consists of an unused portion of the available frequency spectrum. Each user is assigned a given frequency band for all time.

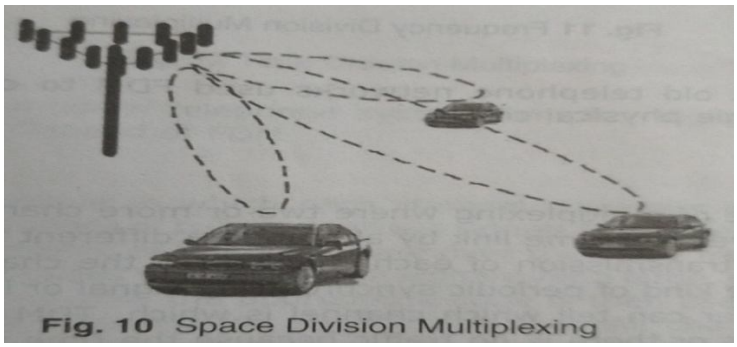


Fig. 10 Space Division Multiplexing

From the above fig. it is clear that each user, here each Mobile Station is using the same frequency band

for a piece of time.

3.6.2 FDM

FDM is a method in which each signal is allocated a frequency slot within the overall transmission bandwidth, in other words the total available frequency bandwidth on the transmission line is divided into frequency channels and each Information signal occupies one of these channels The signal will have exclusive use of this frequency slot all the time (i.e. each subscriber occupies his/her own slot). Suppose a long-distance cable is available with a bandwidth allotment of three megahertz (3 MHz). This is 3,000 KHz, it is possible to place 1,000 signals, each 3 KHz wide, into the long-distance channel. The circuit that does this is known as a multiplexer. It accepts the input from each individual user, and generates a signal on a different frequency for each of the inputs. This results in a high-bandwidth, complex signal containing data from all the users. At the other end of the long-distance cable, the individual signals are separated out by means of a circuit called a demultiplexer, and routed to the proper end users.

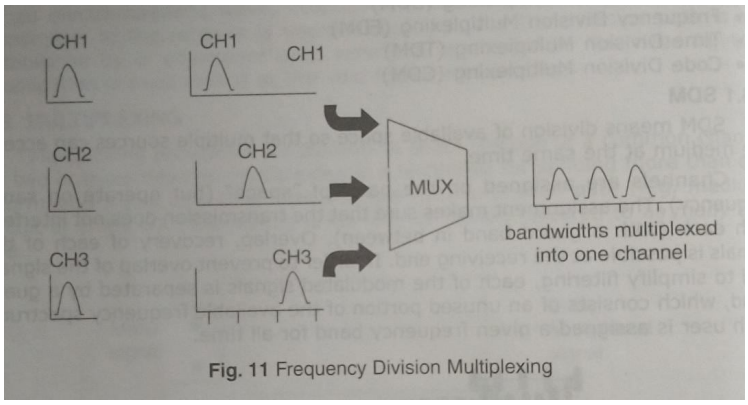


Fig. 11 Frequency Division Multiplexing

For example, old telephone networks used FDM to carry several voice channels on a single physical circuit.

3.6.3 TDM

TDM is a type of multiplexing where two or more channels of information are transmitted over the same link by allocating a different time interval ("slot" or "slice") for the transmission of each channel i.e. the channels take turns to use the link. Some kind of periodic synchronizing signal or identifier is required so that the receiver can tell which channel is which. TDM becomes inefficient when traffic is less or there is no traffic because the time slot is still allocated even when the channel has no data to transmit.

Suppose a channel is capable of transmitting 192 kbit/sec from Chicago to New York. Suppose that three sources, all located in Chicago, each have 64 kbit/sec of data that they want to transmit to individual users in New York. The channel can be divided into a series of time slots, and the time slots can be alternately used by the three sources. The three sources are thus capable of transmitting all of their data across the single, shared channel. At the other end of the channel (in this case, in New York), the process must be reversed (i.e., the system must divide the 192 kbit/sec multiplexed data stream back into the original three 64 kbit/sec data streams, which are then provided to three different users). This reverse process is called demultiplexing.

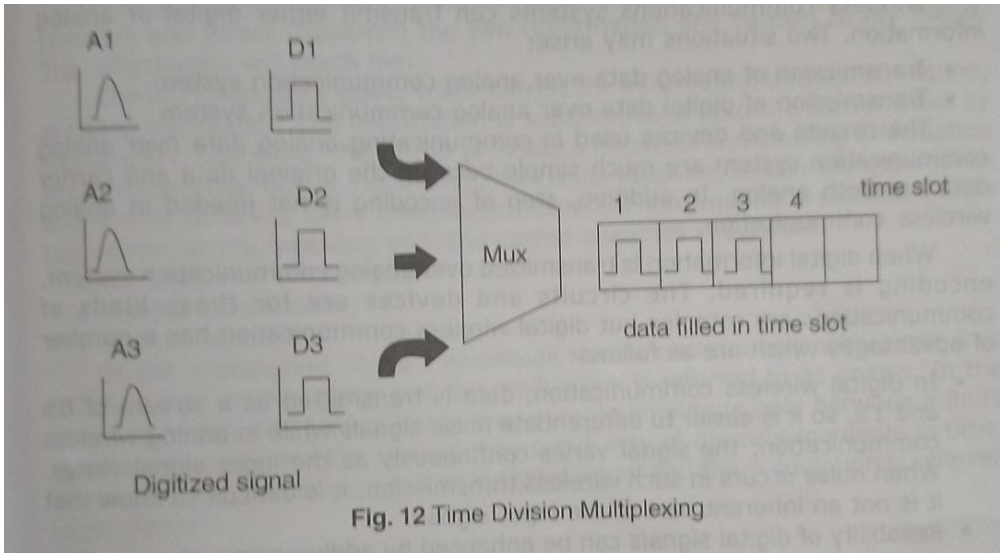


Fig. 12 Time Division Multiplexing

For example, modern telephone systems employ digital transmission, in which TDM is used instead of FDM.

3.6.4 CDM

CDM is a technique where multiple signals are transmitted simultaneously over a shared frequency band by encoding each signal with a unique code. At the receiver, the desired signal is extracted by correlating it with the same code, while other signals appear as noise.

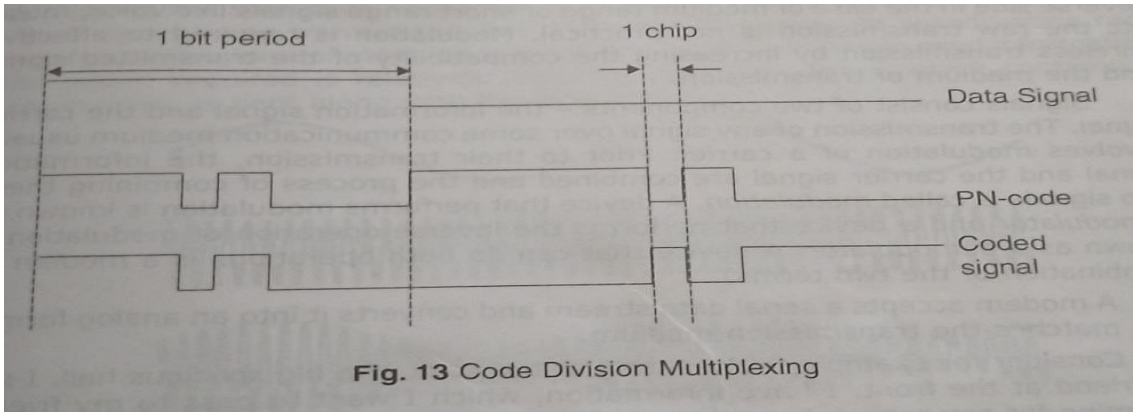


Fig. 13 Code Division Multiplexing

Each user or signal is assigned a unique pseudorandom noise (PN) code (also called a spreading code), which spreads the signal across a wide bandwidth. This allows multiple signals to coexist without significant interference.

Each communicating station is assigned a unique code. The codes stations have the following properties

- If code of one station is multiplied by code of another station, it yields 0.
- If code of one station is multiplied by itself, it yields a positive number equal to the number of stations.

The communication technique can be explained by the following example

Consider that there are four stations w, x, y and z that have been assigned the codes c_w , c_x, c_y and c_z and need to transmit data d_w , d_x, d_y and d_z respectively. Each station multiplies its code with its data and the sum of all the terms is transmitted in the communication channel.

Thus, the data in the communication channel is $d_w . c_w + d_x . c_x + d_y . c_y + d_z . c_z$

Suppose that at the receiving end, station z wants to receive data sent by station y. In order to retrieve the data, it will multiply the received data by the code of station y which is d_y.

$data = (d_w . c_w + d_x . c_x + d_y . c_y + d_z . c_z) . c_y$

$= d_w . c_w . c_y + d_x . c_x . c_y + d_y . c_y . c_y + d_z . c_z . c_y$

$=0 + 0 + d_y . 4 + 0 = 4d_y$

Thus, it can be seen that station z has received data from only station y while neglecting the other codes.

Advantages of CDM

- It has better signal quality.

- Since the sender and receiver only know the spreading code, it prevents eavesdropping and disturbance.
- Protected from hackers.
- Adding users is easy and there is no limit to the number of users.
- Enhance security, avoid crashes and collisions, and use bandwidth effectively. CDMA's spread spectrum technology makes it difficult for eavesdroppers to catch signals, and the special spread spectrum code makes it possible to avoid interference and block transmission.

Disadvantages of CDM

- As the number of users increases, the overall service quality will decrease.
- It needs time synchronization.
- In CDM, the transmitted bandwidth of each user is increased than the digital data speed of the source.
- The data transfer rate is low.
- CDM is complex mechanism.

3.7 MODULATION

Size of antenna required for wireless transmission is inversely proportional to the frequencies of the transmitted signal. So we can take the conclusion that low frequency signals need very large antenna for their transmission. Due to the properties of signal propagating medium, very low frequency signals can not be transmitted across long distances without the loss in the signal strength. On the reverse side in the case of medium range or short range signals like voice, music etc the raw transmission is not practical. Modulation is required to effective wireless transmission by increasing the compatibility of the transmitted signal and the medium of transmission.

Signals consist of two components - the information signal and the carrier signal. The transmission of any signal over some communication medium usually involves modulation of a carrier. Prior to their transmission, the information signal and the carrier signal are combined and the process of combining these two signals is called modulation. A device that performs modulation is known as a modulator and a device that performs the inverse operation of modulation is known as a demodulator. A device that can do both operations is a modem (a combination of the two terms).

A modem accepts a serial data stream and converts it into an analog format that matches the transmission medium.

Consider for example, I am sitting at the back of a big spacious hall. I see my friend at the front. I have information, which I want to pass to my friend. Assuming for any reason I cannot get close to my friend. I write the information

I want to pass to my friend on a piece of paper and wrap the paper around a pen (carrier) and throw (transmit) the two (information and carrier) to my friend. The information will reach him.

The high frequency wave, which carries the information through a medium, is called the carrier. The information is superimposed onto the carrier wave by modulation. Therefore, the carrier provides a means of transferring information at high frequency. Before modulation, the carrier does not contain any intelligence and it only serves to carry information. Once the information is extracted from the carrier at the receiving end, the carrier becomes redundant.

Modulation is of two types:

- Analog Modulation
- Digital Modulation

If the modulating signal's amplitude varies continuously with time, it is said to be an analog signal and the modulation is referred to as analog. In the case where the modulating signal may vary its amplitude only between a finite number of values and the change may occur only at discrete moments in time, the modulating signal is said to be a digital signal and the modulation is referred to as digital.

3.7.1 Analog Modulation

Modulation of an analog signal or analog to analog conversion is the representation of analog information by an analog signal. Analog modulation is of the following types:

- Amplitude Modulation (AM)
- Frequency Modulation (FM)
- Phase Modulation (PM)

3.7.1.1 Amplitude Modulation

The encoding of a carrier wave by variation of its amplitude in accordance with an input signal. It is the process or result of the process where the amplitude of a carrier wave is changed in accordance with a modulating wave. In amplitude modulation (AM), auditory or visual information is impressed on a carrier wave by varying the amplitude of the carrier to match the fluctuations in the audio or video signal being transmitted. AM is the oldest method of broadcasting radio programs. This form of modulation is not a very efficient way to send information; the power required is relatively large because the carrier, which contains no information, is sent along with the information.

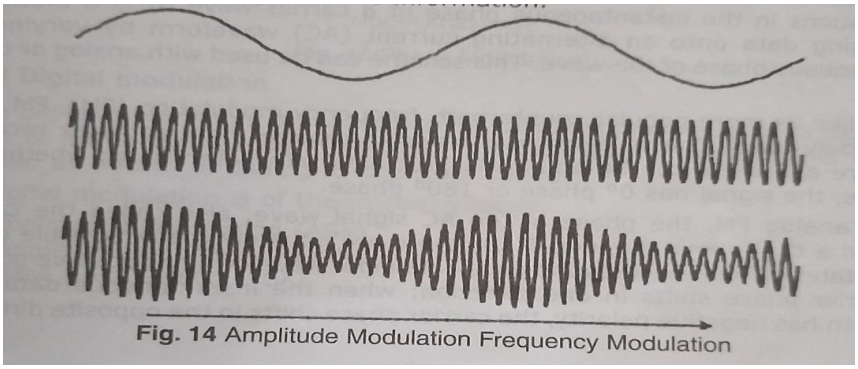


Fig. 14 Amplitude Modulation Frequency Modulation

In frequency modulation (FM), the frequency of the carrier wave is varied in such a way that the change in frequency at any instant is proportional to another signal that varies with time. It is the process of encoding of a carrier wave by variation of its frequency in accordance with an input signal. This means that in frequency modulation (FM), unlike AM, the amplitude of the carrier is kept constant, but its frequency is altered in accordance with variations in the audio signal being sent. This form of modulation was developed to overcome interference and noise that affect AM radio reception. FM is less susceptible than is AM to certain kinds of interference, such as that caused by thunderstorms as well as random electrical currents from machinery and other etc. These noise-producing signals affect the amplitude of a radio wave but not its frequency, and so an FM signal remains virtually unchanged. The FM band has become the choice of music listeners because of its low-noise, wide-bandwidth qualities; it is also used for the audio portion of a television broadcast.

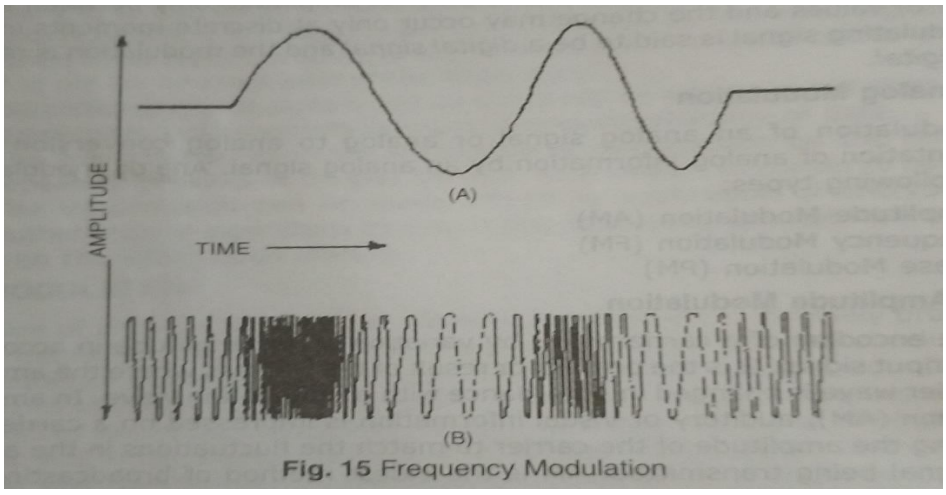


Fig. 15 Frequency Modulation

Phase modulation (PM) is a form of modulation that represents Information as variations in the instantaneous phase of a carrier wave. It is a method of impressing data onto an alternating-current (AC) waveform by varying the instantaneous phase of the wave. This scheme can be used with analog or digital data

Unlike its more popular counterpart, frequency modulation (FM), PM is not very widely used. This is because it tends to require more complex receiving hardware and there can be ambiguity problems with determining whether, for example, the signal has 0º phase or 180° phase.

In analog PM, the phase of the AC signal wave, also called the carrier, varies in a continuous manner. Thus, there are infinitely many possible carrier phase states. When the instantaneous data input waveform has positive polarity, the camer phase shifts in one direction, when the instantaneous data input waveform has negative polarity, the carrier phase shifts in the opposite direction.

At every instant in time, the extent of carrier-phase shift (the phase angle) is directly proportional to the

extent to which the signal amplitude is positive or negative.

In digital PM, the carrier phase shifts abruptly, rather than continuously back and forth. The number of possible carrier phase states is usually a power of 2. If there are only two possible phase states, the mode is called biphase modulation. In more complex modes, there can be four, eight, or more different phase states. Each phase angle (that is, each shift from one phase state to another) represents a specific digital input data state.

Phase modulation is similar in practice to frequency modulation (FM). When the instantaneous phase of a carrier is varied, the instantaneous frequency changes as well. When the instantaneous frequency is varied, the instantaneous phase changes. But PM and FM are not exactly equivalent, especially in analog applications. When an FM receiver is used to demodulate a PM signal, or when an FM signal is intercepted by a receiver designed for PM, the audio is distorted.

This is because the relationship between phase and frequency variations is not linear; that is, phase and frequency do not vary in direct proportion.

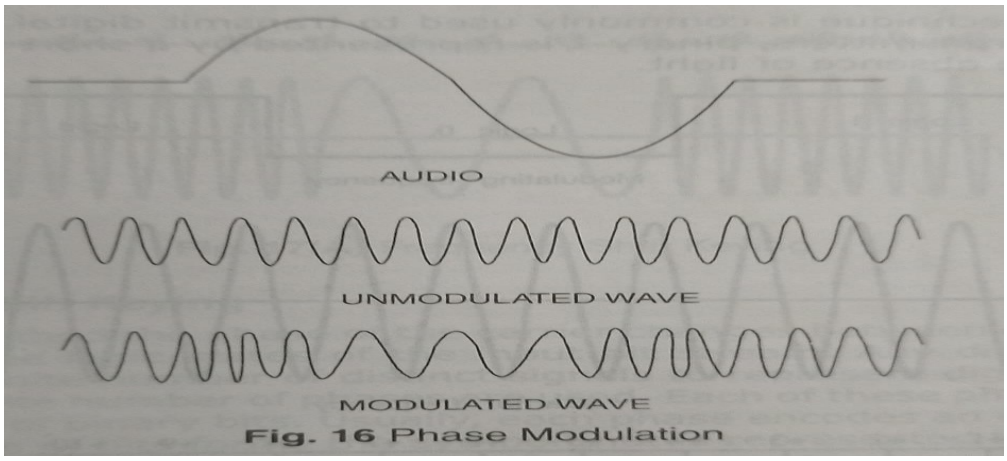


Fig. 16 Phase Modulation

3.7.1.3 Digital modulation

In digital modulation, an analog carrier signal is modulated by a digital bit stream of either equal length signals or varying length signals. This can be described as a form of analog-to-digital conversion.

Digital modulation is of the following types:

- Amplitude Shift Keying (ASK)
- Frequency Shift Keying (FSK)
- Phase Shift Keying (PSK)

3.7.1.4 Amplitude Shift Keying

ASK is the most simple digital modulation scheme. Two binary values, 0 and 1, are represented by two different amplitude. In wireless, constant amplitude cannot be guaranteed, so ASK is typically not used. It is a form of modulation that represents digital data as variations in the amplitude of a carrier wave. Here, the strength of the carrier signal is varied to represent binary 1 or O. A typical output waveform of an ASK modulator is shown in the figure below. The frequency components are the MSB and LSB with a residual carrier frequency. The low amplitude carrier is allowed to be transmitted to ensure that at the receiver the logic 1 and logic 0 conditions can be recognized uniquely. Both frequency and phase remains constant while amplitude changes. ASK transmission is highly susceptible to noise interference.

The amplitude of an analog carrier signal varies in accordance with the bit stream (modulating signal), keeping frequency and phase constant. The level of amplitude can be used to represent binary logic Os and 1s. We can consider a carrier signal as an ON or OFF switch. In the modulated signal, logic 0 is represented by the absence of a carrier, thus giving OFF/ON keying operation and hence the name given.

The ASK technique is commonly used to transmit digital data over optical fiber. For LED transmitters, binary 1 is represented by a short pulse of light and binary 0 by the absence of light.

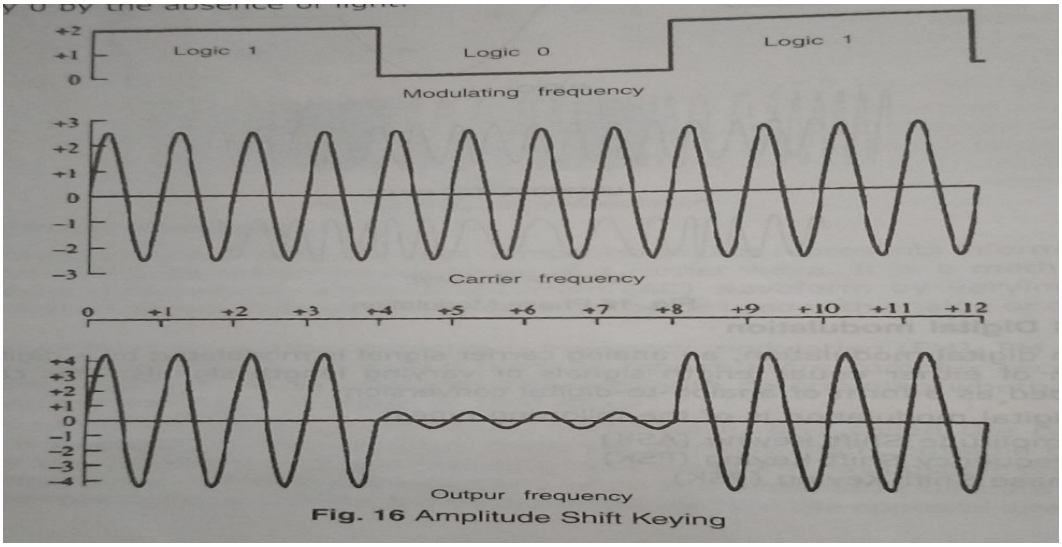


Fig. 16 Amplitude Shift Keying

3.7.1.5 Frequency Shift Keying

In this method the frequency of the carrier is changed to two different frequencies depending on the logic state of the input bit stream. The typical output waveform of an FSK is shown below. Notice that logic high causes the centre frequency to increase to a maximum and a logic low causes the centre frequency to decrease to a minimum.

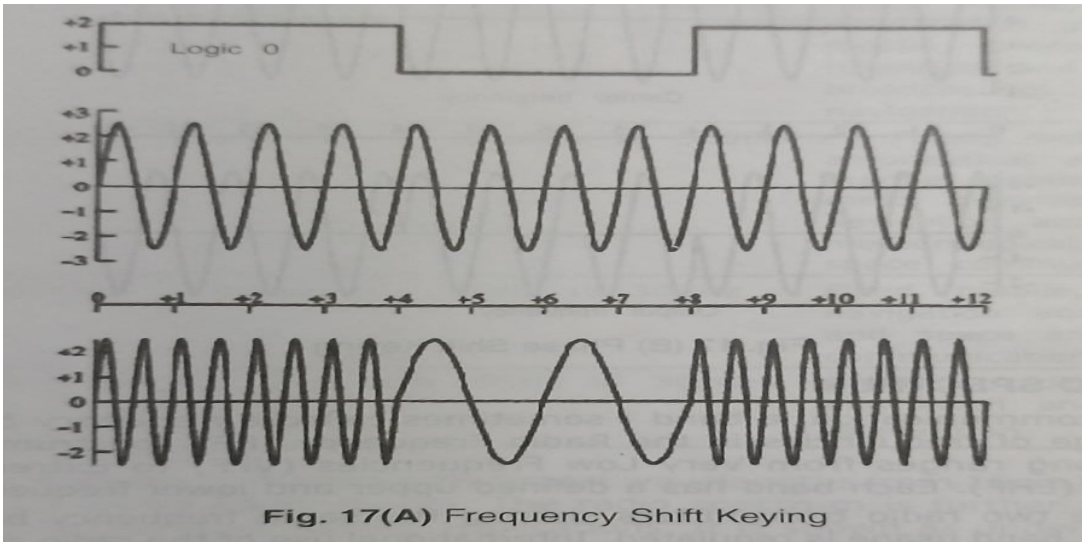


Fig. 17(A) Frequency Shift Keying

3.7.1.6 Phase Shift Keying

With this method the phase of the carrier changes between different phases determined by the logic states of the input bit stream. Any digital modulation scheme uses a finite number of distinct signals to represent digital data. In the case of PSK, a finite number of phases are used. Each of these phases is assigned a unique pattern of binary bits. Usually, each phase encodes an equal number of bits. Each pattern of bits forms the symbol that is represented by the particular phase.

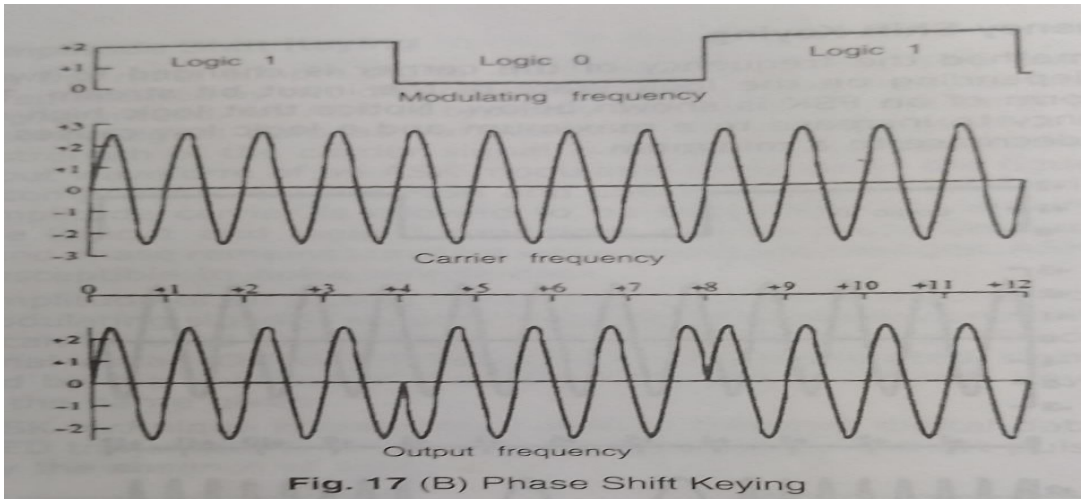


Fig. 17 (B) Phase Shift Keying

3.8 SPREAD SPECTRUM

In telecommunication, a band sometimes called a frequency band - is a specific range of frequencies in the Radio Frequency (RF) spectrum, which is divided among ranges from Very Low Frequencies (VLF) to Extremely High Frequencies (EHF). Each band has a defined upper and lower frequency limit. Because two radio transmitters sharing the same frequency band cause interference, band usage is regulated. International use of the radio spectrum is regulated by the International Telecommunication Union (ITU).

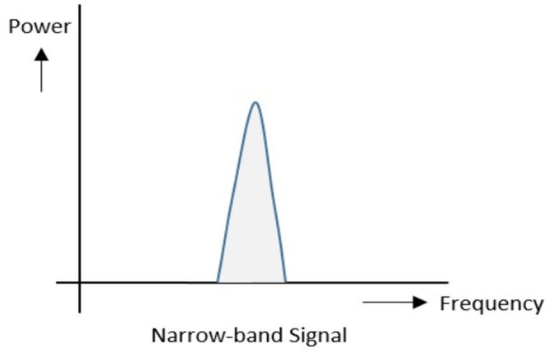
Designation		Frequency	Users
ELF	extremely low frequency	3Hz to 30Hz	-
SLF	superlow frequency	30Hz to 300Hz	-
ULF	ultralow frequency	300Hz to 3000Hz	-
VLF	very low frequency	3kHz to 30kHz	Time signals and standard frequencies
LF	low frequency	30kHz to 300kHz	Fixed, maritime mobile and navigational systems and radio broadcasting
MF	medium frequency	300kHz to 3000kHz	Land, maritime mobile and radio broadcasting
HF	high frequency	3MHz to 30MHz	Fixed, mobile, aeronautical and marine mobile, amateur radio, and radio broadcasting
VHF	very high frequency	30MHz to 300MHz	Fixed, mobile, aeronautical and marine mobile, amateur radio, television and radio broadcasting, and radio navigation
UHF	ultrahigh frequency	300MHz to 3000MHz	Fixed, mobile, aeronautical and marine mobile, amateur radio, television, radio navigation and location, meteorological, and space communication
SHF	superhigh frequency	3GHz to 30GHz	Fixed, mobile, radio navigation and location, and space and satellite communication
HF	extremely high frequency	30GHz to 300GHz	Amateur radio, atellite, and earth and space exploration

Electro Magnetic spectrum with largest wavelengths from 10cm to 300000m and more are called Radio Waves. The radio spectrum is further divided into bands that are useful for specific applications. It is shown as under:

Gamma-Rays	X-Rays	Ultra Violet	Visible Light	Infrared	Micro Wave	Radio
10^{-11}	10^{-9}	10^{-7}	10^{-5}	10^{-3}	10^{-1}	10^{3}

Narrow-band Signals

The Narrow-band signals have the signal strength concentrated as shown in the following frequency spectrum figure.

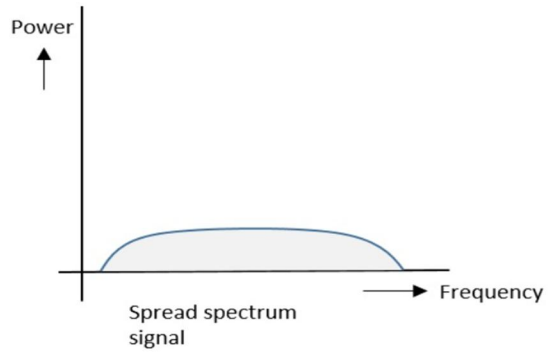


- Band of signals occupy a narrow range of frequencies.
- Power density is high.
- Spread of energy is low and concentrated.

Though the features are good, these signals are prone to interference.

Spread Spectrum is a technique in which the transmitted signals of specific frequencies are varied slightly to obtain greater bandwidth as compared to initial bandwidth.

The spread spectrum signals have the signal strength distributed as shown in the following frequency spectrum figure.



- Band of signals occupy a wide range of frequencies.
- Power density is very low.
- Energy is wide spread.

  It helps to achieve secure communications, increasing resistance to natural interference and jamming, and to prevent detection.

To apply an SS technique, corresponding Spread Spectrum (SS) code is injected somewhere in the transmitting chain before the antenna. (That injection is called the spreading operation) The effect is to diffuse the information in a larger bandwidth. Conversely, you can remove the SS code (despreading operation) at a point in the receive chain before data retrieval. The effect of a despreading operation is to reconstitute the information in its original bandwidth. Obviously, the same code must be known in advance at both ends of the transmission channel. (In some circumstances, it should be known only by those two parties.)

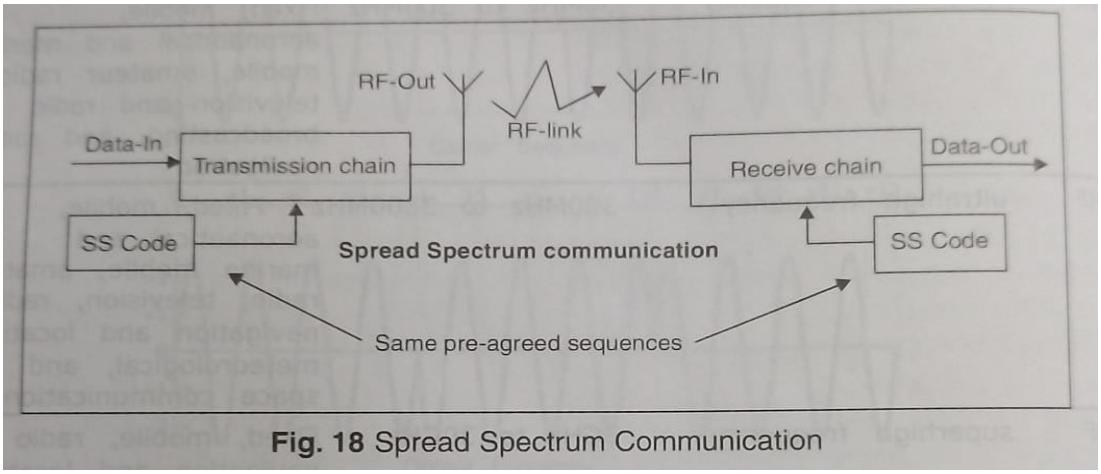


Fig. 18 Spread Spectrum Communication

Different SS techniques are distinguished according to the point in the system at which a Pseudo-Random Number (PRN) is inserted in the communication channel.

Various Spread Spectrum methods are as follows:

- Direct Sequence Spread Spectrum (DSSS)
- Frequency Hopping Spread Spectrum (FHSS)

3.8.1 DSSS

Whenever a user wants to send data using this DSSS technique, each and every bit of the user data is multiplied by a secret code, called as chipping code. This chipping code is nothing but the spreading code which is multiplied with the original message and transmitted. The receiver uses the same code to retrieve the original message.

In wireless LAN, the sequence with n = 11 is used. The original data is multiplied by **chips** (spreading code) to get the spread signal. The required bandwidth of the spread signal is 11 times larger than the bandwidth of the original signal.

Advantages of DSSS

- The DSSS System combats the jamming most effectively.
- The performance of DSSS in presence of noise is superior to FHSS.
- Interference is minimized against the signals.

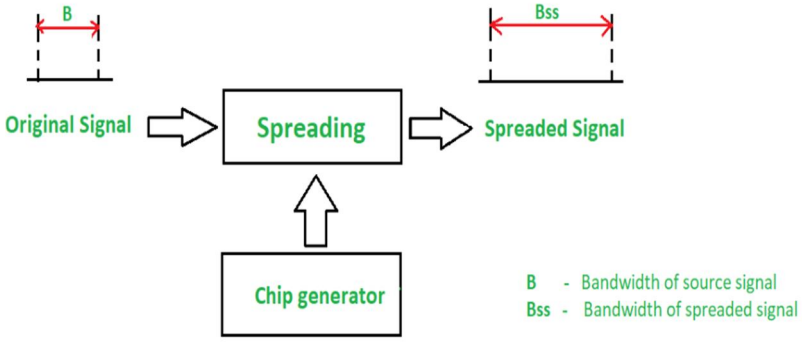
Disadvantages of DSSS

- Processing Gain is lower than FHSS.
- Channel Bandwidth is less than FHSS.
- Synchronization is affected by the variable distance between the transmitter and receiver.

Applications of DSSS

- GPS (Global Positioning System)
- CDMA (Code Division Multiple Access) Cellular Networks
- Satellite Communication
- Wireless Sensor Networks

DSSS is generally used to transmit digital information. Here, the digital information channel is mixed with a pseudo random code whose bandwidth is much greater than that of the signal itself.



This method uses a wide frequency band together with Code Division Multiple Access (CDMA). Signals from

different units are transmitted at a given frequency range. The power levels of these signals are very low (just above background noise). A code is transmitted with each signal so that the receiver can identify the appropriate signal transmitted by the sender unit.

The frequency at which such signals are transmitted is called the ISM (Industrial, Scientific and Medical) band. This frequency band is reserved for ISM devices. The ISM band has three frequency ranges: 902-928, 2400-2483.5 and 5725-5850 MHz. An exception to this is Motorola's ALTAIR which operates at 18GHz.

In this technique, the PRN/ Pseudo Random Code are applied directly to data entering the carrier modulator. These codes are not required to provide call security, but create a uniqueness to enable call identification. Codes should not correlate to other codes or other versions of it. Spreading codes are noise like pseudo-random codes, channel codes are designed for maximum separation from each other and cell identification codes are balanced not to correlate to other codes of it. The rate of a spreading code is referred to as chip rate rather than bit rate. The result of modulating is a RF carrier with such a code sequence is to produce a direct-sequence-modulated spread spectrum.

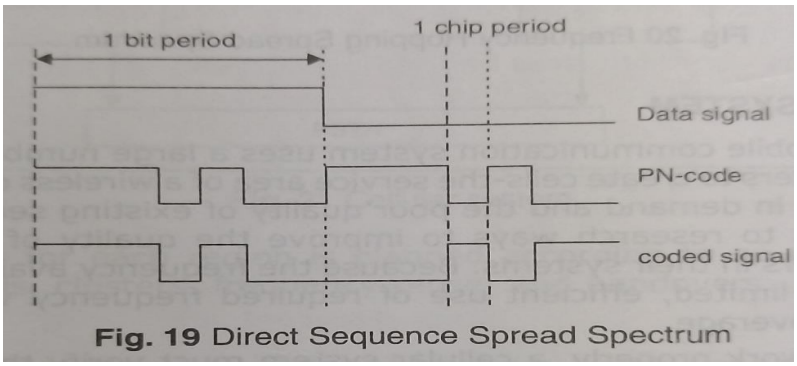


Fig. 19 Direct Sequence Spread Spectrum

3.8.2 FHSS

FHSS is a form of spreading in which the frequency of a carrier is altered many times within a fixed time period in accordance with a pseudo-random list of channels. The signal jumps from one frequency to another within a given. frequency range. The transmitter device "listens" to a channel, if it detects an idle time (I.e. no signal is transmitted), it transmits the data using the full channel bandwidth. If the channel is full, it "hops" to another channel and repeats the process. The transmitter and the receiver "jump" in the same manner.

For example, a frequency was allotted to sender 1 for a particular period of time. Now, after a while, sender 1 hops to the other frequency and sender 2 uses the first frequency, which was previously used by sender 1. This is called as frequency reuse.

Total available bandwidth is split into many channels of smaller bandwidth and guard spaces. Transmitter and receiver stay on one of these channels for a certain time and then hop to another channel. It implements FDM and TDM Pattern of channel usage is hopping sequence.

Advantages of FHSS

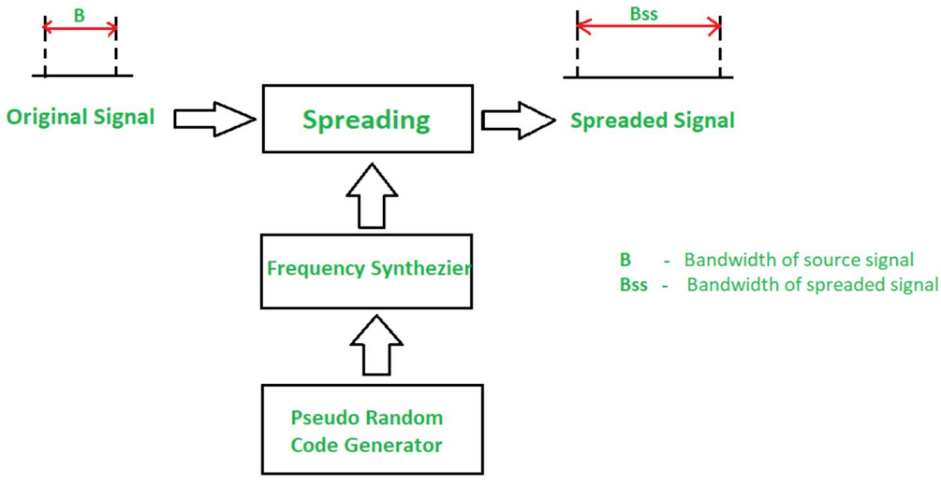
- Synchronization is not greatly dependent on distance.
- Processing Gain is higher than DSSS.

Disadvantages of FHSS

- The bandwidth of the FHSS system is too large (in GHz).
- Complex and expensive Digital frequency synthesizers are required.

Applications of FHSS

- FHSS is used in Bluetooth
- Military Communications
- Walkie-Talkies
- Wireless Local Area Networks (WLANs)
- Remote Controls



Transmitter and receivers have to stay synchronized within smaller tolerances. They are better immune to narrow band interference as they stick to one frequency for a very short period. Receiver must know the hopping sequence and stay synchronized with the transmitter. It is used by Bluetooth.

This method does exactly what its name implies; it causes the carrier to hop from frequency to frequency over a wide band according to a sequence defined by the PRN. The speed at which the hops are executed depends on the data rate of the original information, but one can distinguish between Fast Frequency Hopping (FFHSS) and Low Frequency Hopping (LFHSS). The latter method (the most common) allows several consecutive data bits to modulate the same frequency. FFHSS, on the other hand, is characterized by several hops within each data bit.

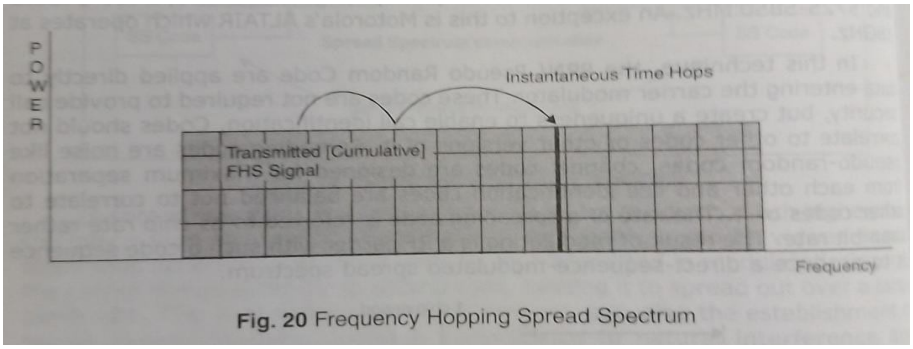


Fig. 20 Frequency Hopping Spread Spectrum

FHSS	**DSSS / CDMA**
Multiple frequencies are used	Single frequency is used
Hard to find the users frequency at any instant of time	User frequency, once allotted is always the same
Frequency reuse is allowed	Frequency reuse is not allowed
Sender need not wait	Sender has to wait if the spectrum is busy
Power strength of the signal is high	Power strength of the signal is low
Stronger and penetrates through the obstacles	It is weaker compared to FHSS
It is never affected by interference	It can be affected by interference
It is cheaper	It is expensive

This is the commonly used technique	This technique is not frequently used

3.9 CELLULAR SYSTEM

A cellular mobile communication system uses a large number of low-power wireless transmitters to create cells-the service area of a wireless communications system. Increase in demand and the poor quality of existing service led mobile service providers to research ways to improve the quality of service and to support more users in their systems. Because the frequency available for mobile cellular use was limited, efficient use of required frequency was needed for mobile cellular coverage.

In order to work properly, a cellular system must verify the following two main conditions:

The power level of a transmitter within a single cell must be limited in order to reduce the interference with the transmitters of neighboring cells.

Neighboring cells cannot share the same channels. In order to reduce the interference, the frequencies must reuse only a certain pattern.

A cellular network is a radio network made up of a number of radio cells (or Just cells) each served by a fixed transmitter, known as a cell site or base station. These cells are used to cover different areas in order to provide radio coverage over a wider area than the area of one cell.

Cellular networks offer a number of advantages:

- Increased capacity
- Reduced power usage
- Better coverage

A good and simple example of a cellular system is an old taxi driver's radio system where the taxi company will have several transmitters based around a city each operated by an individual operator.

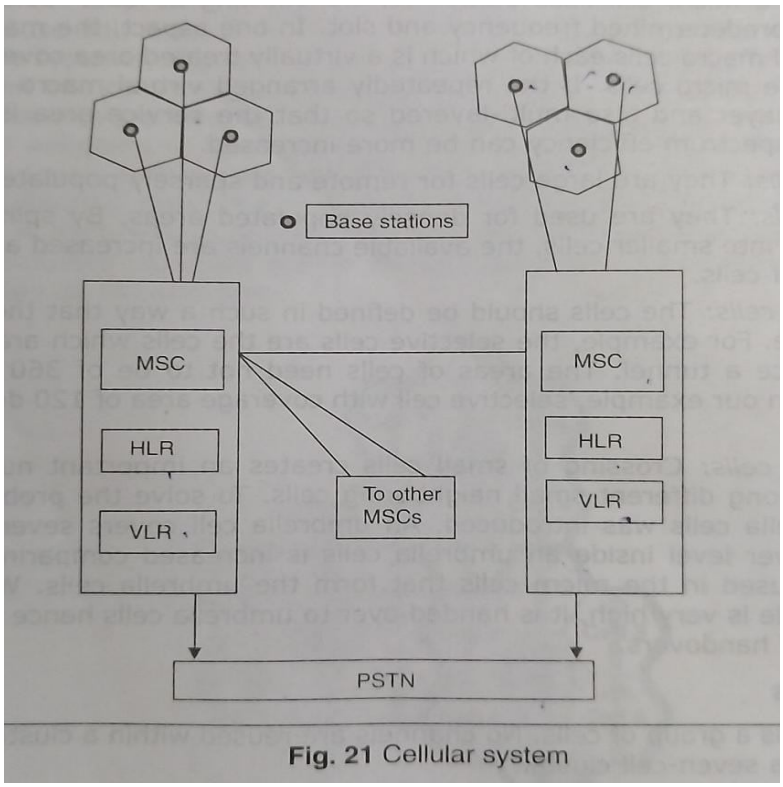


Fig. 21 Cellular system

Provisioning for each region is planned according to an engineering plan that includes cells, clusters, frequency reuse, and handovers.

3.9.1 Cells

A cell is the basic geographic unit of a cellular system. Cells are base stations transmitting over small geographic areas that are represented as hexagons. Each cell size varies depending on the landscape. Because of constraints imposed by natural terrain and man-made structures, the true shape of cells is not a perfect hexagon. Different types of cells are used:

- Macro cells
- Micro cells
- Selective cells
- Umbrella cells

A mobile communication system has a cell structure constituted by integrating macro cells and micro cells, and at least one mobile station. The cell structure is made to cover a service area by a plurality of the micro cells each having a predetermined size and to cover the same service area by the single macro cell having a larger size than the size of the micro cell. Each of the micro cells includes a micro cell base station for transmitting at least radio control channel at a predetermined frequency and slot. In one aspect, the macro cells may be virtual macro cells each of which is a virtually treated area covered by a plurality of the micro cells. If the repeatedly arranged virtual macro cells are formed as a layer and also multi-layered so that the service area is closely covered, the spectrum efficiency can be more increased.

Macro cells: They are large cells for remote and sparsely populated areas.

Micro cells: They are used for densely populated areas. By splitting the existing areas into smaller cells, the available channels are increased as well as the capacity of cells.

Selective cells: The cells should be defined in such a way that they prove their existence. For example, the selective cells are the cells which are located at the entrance a tunnel. The areas of cells need not to be of 360 degrees always. Here in our example, selective cell with coverage area of 120 degrees is used.

Umbrella cells: Crossing of small cells creates an important number of handovers among different small neighboring cells. To solve the problem, the idea of umbrella cells was introduced. An umbrella cell covers several micro cells. The power level Inside an umbrella cells is increased comparing to the power levels used in the micro cells that form the umbrella cells. When the speed of mobile is very high, it is handed over to umbrella cells hence reducing the number of handovers.

3.9.2 Clusters

A cluster is a group of cells. No channels are reused within a cluster. Below fig. Ilustrates a seven-cell cluster.

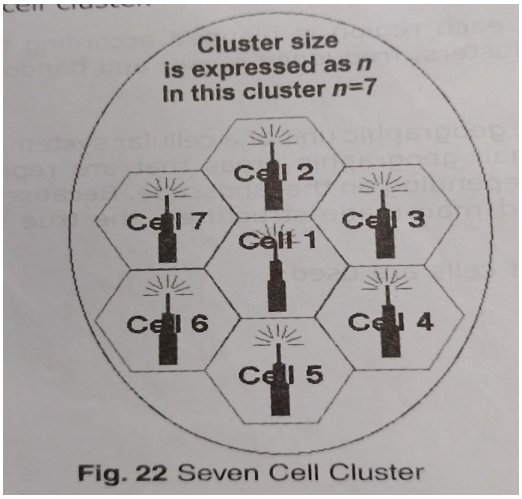


Fig. 22 Seven Cell Cluster

Number of cells in a cluster plays very important role. As there will be smaller number of cells in cluster, bigger will be the number of channels per cell. Therefore each cells capacity will be increased. One thing to take care is to avoid the interference that might occur due to neighboring clusters.

3.9.3 Frequency Reuse

Because only a small number of radio channel frequencies were available for mobile systems, engineers had to find a way to reuse radio channels to carry more than one conversation at a time. The solution the industry adopted was called frequency planning or frequency reuse. The concept of frequency reuse is based on assigning to each cell a group of radio channels used within a small geographic area. Cells are assigned a group of channels that is completely different from neighboring cells. The coverage area of cells is called the footprint. This footprint is limited by a boundary so that the same group of channels can be used in different cells that are far enough away from each other so that their frequencies do not interfere.

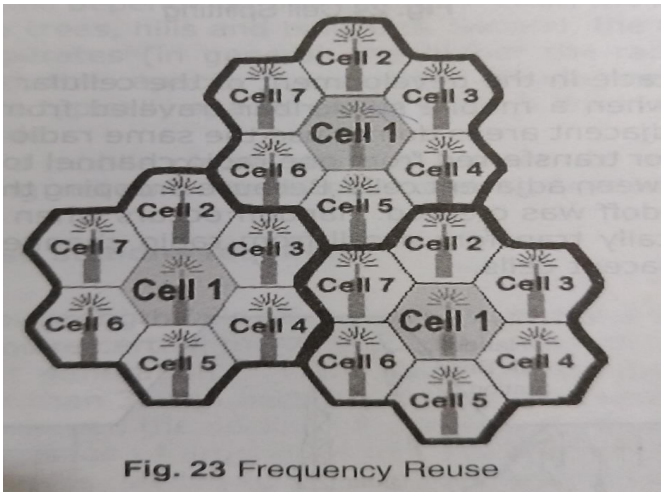


Fig. 23 Frequency Reuse

3.9.4 Cell Splitting

Economic considerations made the concept of creating full systems with many small areas impractical. To overcome this difficulty, system operators developed the idea of cell splitting. As a service area becomes full of users, this approach is used to split a single area into smaller ones. In this way, urban centers can be split into as many areas as necessary to provide acceptable service levels in heavy-traffic regions, while larger, less expensive cells can be used to cover remote rural regions.

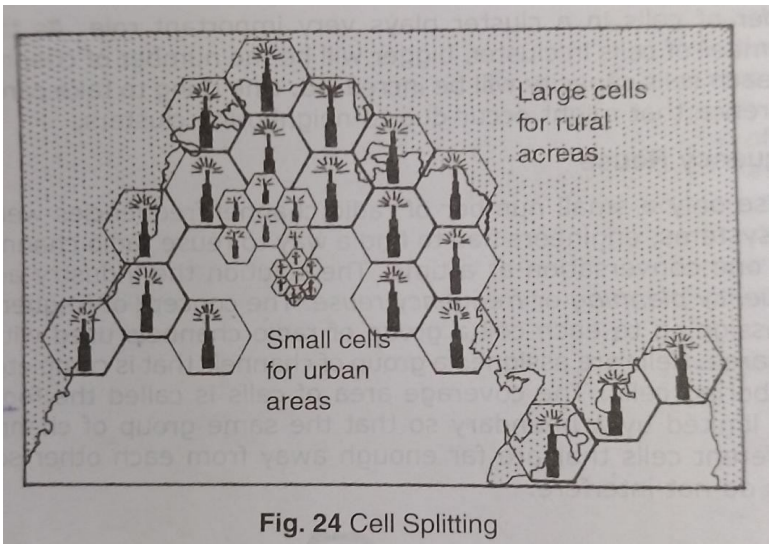


Fig. 24 Cell Splitting

3.9.5 Handoff

The final obstacle in the development of the cellular network involved the problem created when a mobile subscriber traveled from one cell to another duning a call. As adjacent areas do not use the same radio channels, a call must either be dropped or transferred from one radio channel to another when a user crosses the line between adjacent cells. Because dropping the call is unacceptable, the process of handoff was created. Handoff occurs when the mobile telephone network automatically transfers a call from radio channel to radio channel as mobile crosses adjacent cells.

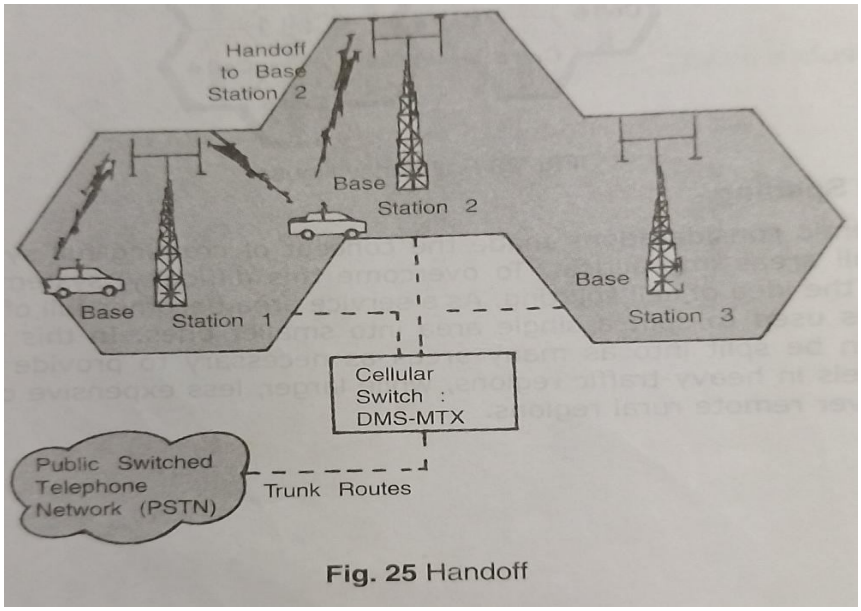


Fig. 25 Handoff

During a call, two parties are on one voice channel. When the mobile unit moves out of the coverage area of a given cell site, the reception becomes weak. At this point, the cell site in use requests a handoff. The system switches the call to a stronger-frequency channel in a new site without interrupting the call or alerting the user. The call continues as long as the user is talking, and the user does not notice the handoff at all.

3.9.6 Cellular Radio

Each base station provides radio coverage to a geographical area known as a cell. Base stations are connected to one another by central switching centers, which track calls and transfer them as the caller moves from one cell to the next. An ideal network may be envisaged as consisting of a mesh of hexagonal cells, each with a base station at its centre. The cells overlap at the edges to ensure the mobile phone users always remain within range of a base station. Without sufficient base stations in the right locations, mobile phones will not work.

The size of each cell depends on three factors. First, the local terrain; radio signals are blocked by trees, hills and buildings. Second, the frequency band in which the network operates (in general, the higher the radio frequency, the smaller the cell). Third, the capacity (I.e. number of calls) needed in any given area. Base stations are typically spaced about 0.2-0.5 km in towns and 2-5 km apart in the countryside.

If a person with a mobile phone starts to moves out of one cell and into another, the controlling network hands over communications to the adjacent base station.

Why are so many base stations required?

Hexagonal Cell

Transmitted signal strength falls off rapidly with distance from base stations, and mobile phones require certain minimum signal strength to ensure adequate reception. The current generation of GSM base stations cannot communicate over distances greater than 35 km because the delay in receiving radio signals becomes too great. However, the decline of signal strength with distance places a practical limit on coverage of around 10 km. For these reasons an extensive network of base stations is needed to ensure coverage throughout the UK.

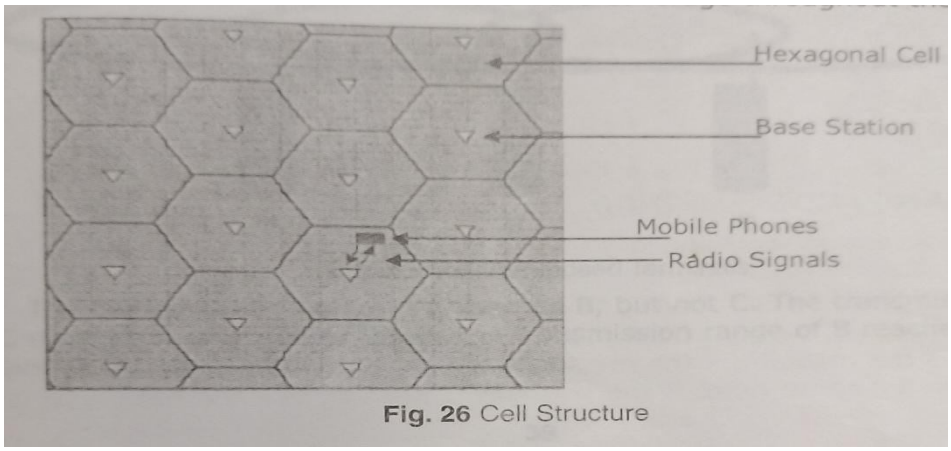


Fig. 26 Cell Structure

Why can't one base station serve my town?

Radio spectrum is a precious natural resource with many different demands upon it (for example, radio and TV broadcasting, emergency communication, navigation aids etc). Consequently the amount made available to each mobile phone operator is limited and this means base stations can only carry a limited number of calls at any one time.

To accommodate the steadily increasing volume of users, network operators have to use the limited number of radio frequencies licensed to them to support the maximum number of mobile phone users. This is achieved by re-using any given radio frequency many times in a network and carefully controlling base station power so that signals arising in different parts of the network do not interfere with each other. This concept of frequency re-use is illustrated in figure 3. The cells are grouped into clusters, with the frequencies allocated to a particular cell within a cluster not being re-used until the corresponding cell in adjacent clusters. This gives a repeating pattern of cells and clusters which can be expanded to provide national coverage.

To increase the capacity of their networks, operators have to build additional base stations and thus reduce cell size. It is for this reason that one large base station cannot serve a whole town.

Chapter - 4

MEDIUM ACCESS CONTROL

4.1 Introduction
4.2 Hidden/ Exposed Terminals
4.3 The basic Access Method
4.4 Near / Far Terminals
4.5 SDMA, FDMA,TDMA, CDMA

4.1 INTRODUCTION

When a no. of signal sources attempt to access a wireless medium simultaneously, networks encounter the problem of receiving signals from each radio carrier distinctly. This is because of the signals (electromagnetic signals) tend to interfere with each other when they are transmitted simultaneously through the medium. Also networks encounter the problems of signals from hidden and exposed terminals as well as near and far terminals.

To overcome these problems, communication system receivers extract distinct signals from various terminals in presence of signals divided into different cells, time slots, frequencies and codes (SDMA, TDMA, FDMA and CDMA signals). CDMA is a big step forward for medium access control during access to the transmission medium by multiple wireless systems at a given instant and frequency band.

4.2 HIDDEN/EXPOSED TERMINALS

This problem does not occur on a wired LAN.

Consider the scenario with three mobile phones.

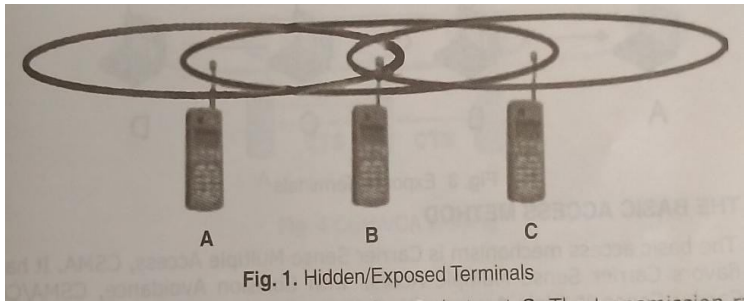


Fig. 1. Hidden/Exposed Terminals

The transmission range of A reaches B, but not C. The transmission range of C reaches B, but not A. Finally the transmission range of B reaches A and C. A cannot detect C and C can not detect A.

A starts sending to B, C does not receive this transmission. C also wants to send some data to B and senses the medium. Thus C starts sending causing a collision at B. But A can not detect this collision and continues with its transmission. A is hidden for C and vice versa. While hidden terminals cause collision, the next effect is unnecessary delay. Now, B sends something to A and C wants to send data to some other mobile phone outside the range of A, B and C. C senses the carrier and detects that carrier is busy. Hence, C posts pones its transmission. But as A is outside the interference range of C, waiting is not necessary. Causing a collision at B does not matter because the collision is too weak to propagate to A. In this situation, C is exposed to B.

Carrier Sense Multiple Access with Collision Detection CSMA/CD...

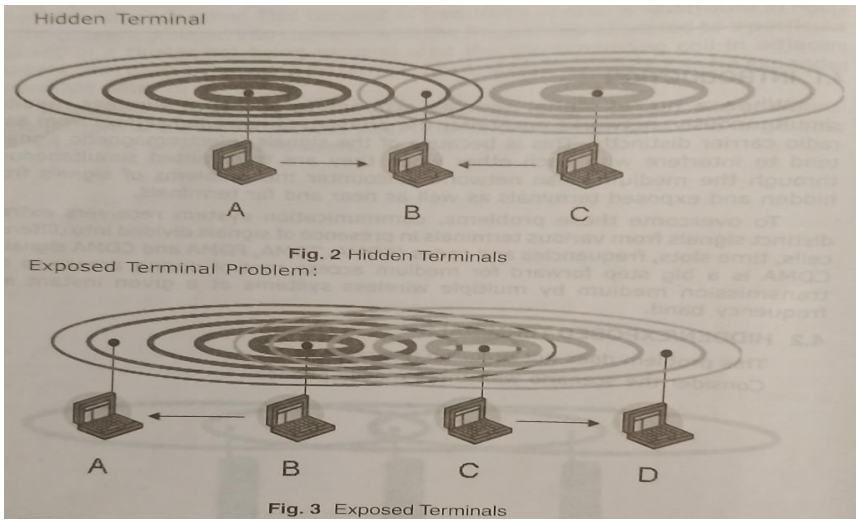


Fig. 2 Hidden Terminals

Fig. 3 Exposed Terminals

4.3 THE BASIC ACCESS METHOD

The basic access mechanism is Carrier Sense Multiple Access, CSMA. It has two flavors Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA and Carrier Sense Multiple Access with Collision Detection, CSMA/CD.

CSMA protocol works as follows: A station, which wants to transmit the data, senses the medium, if the medium is busy then the station will pause its transmission for some time, if the medium is sensed free then the station is MEDIUM ACCESS CONTROL allowed to transmit. This kind of protocol is very effective when the medium is not heavily loaded, as it allows the stations to transmit with minimum delay, but there is always a chance of stations transmitting at the same time (collision).

Problems in wireless networks:

Signal strength decreases as the distance increases. The sender would apply CS and CD, but the collisions happen at the receiver due to a second sender It might be the case that a sender cannot hear the collision, i.e., CD does not work. Further, CS might not work if, e.g., a terminal is hidden. The solution is CSMA/CA.

CSMA/CD protocol works as follows:

A sender senses the medium to see if it is free. If the medium is busy, the sender waits until it is free. If the medium is free, the sender starts transmitting data and continues to listen the medium. If the sender detects a collision while sending, it stops at once.

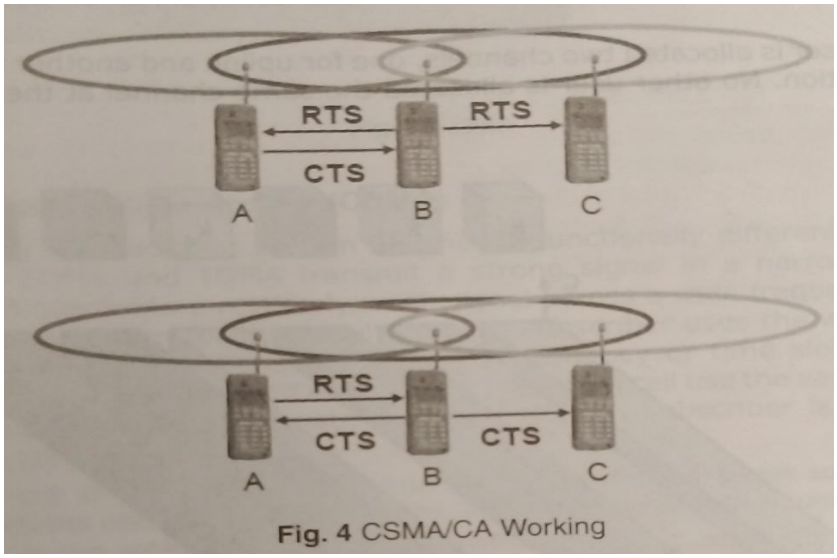


Fig. 4 CSMA/CA Working

CSMA/CA protocol works as follows:

It uses two short signaling packets for collision avoidance. They are Request To Send (RTS) and Clear To Send (CTS). The sender requests the right to send from a receiver with a short RTS packet before it sends a data packet. The receiver grants the right to send as soon as it is ready to receive. Signaling packets contain sender address, receiver address and packet length (the length of the future transmission). It avoids the problem of Hidden and Exposed Terminals.

4.4 NEAR/FAR TERMINALS

Consider the following scenario.

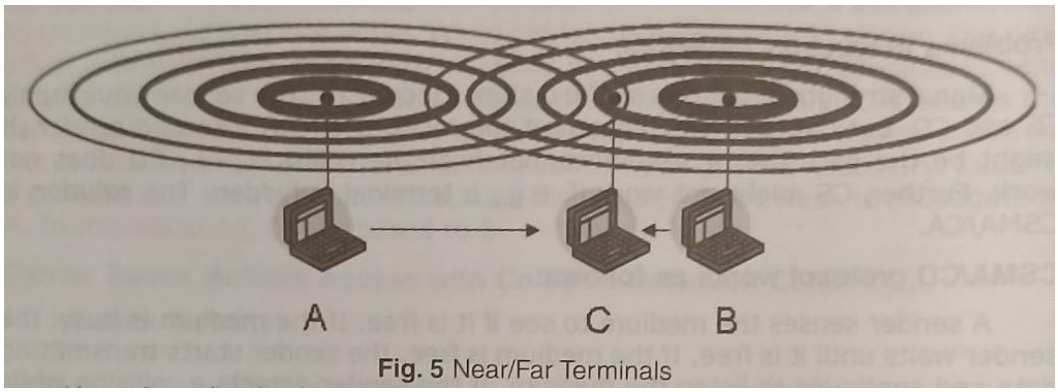


Fig. 5 Near/Far Terminals

Here A and B both are sending signals with same transmission power. As the signal strength decreases proportionally to the square of the distance, B's signal drowns out A's signal. As a result C can not receive A's transmission.

Frequency Division Multiple Access (FDMA)

It is one of the most common multiplexing techniques. The available frequency band is divided into channels of equal bandwidth so that each communication is carried on a different frequency. This multiplexing technique is used in all the first generation analog mobile networks like Advanced Mobile Phone System (AMPS) in USA and Total Access Communication System (TACS) in UK.

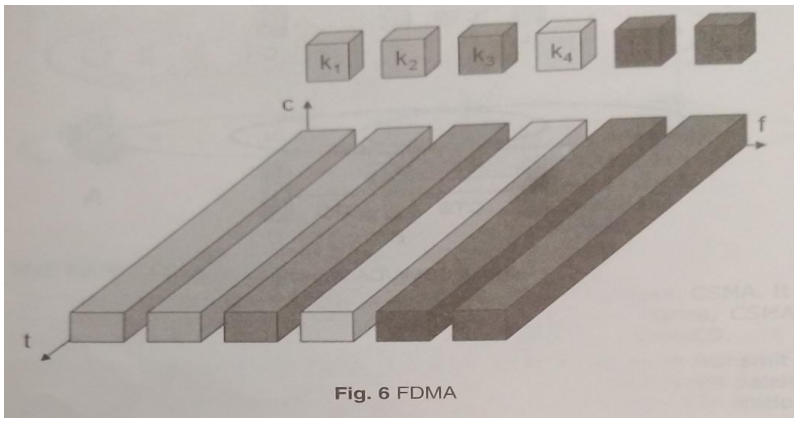


Fig. 6 FDMA

Each user is allocated two channels, one for uplink and another for downlink communication. No other user is allocated the same channel at the same time.

4.5 TIME DIVISION MULTIPLE ACCESS (TDMA)

It is more expensive technique compared to FDMA as it needs proper synchronization between sender and receiver. TDMA is access method for shared medium (usually radio) networks. It allows several users to share the same frequency channel by dividing the signal into different timeslots I.e. each channel is split up into time segments, and a transmitter is given exclusive use of one or more channels only during a particular time period. TDMA is used in the digital 2G cellular systems such as Global System for Mobile Communications (GSM), Personal Digital Cellular (PDC) etc. It is also used extensively in satellite systems.

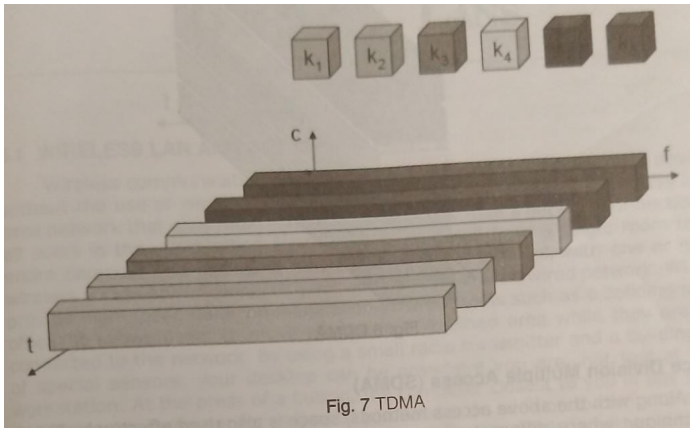


Fig. 7 TDMA

Code Division Multiple Access (CDMA)

CDMA is a broadband system and hence functionally different from FDMA and TDMA. FDMA and TDMA transmit a strong signal in a narrow frequency band; CDMA transmits a relatively weak signal across a wide frequency band. It uses spread spectrum technique where each subscriber uses the whole system bandwidth. Unlike TDAM and FDMA where frequency or time slot is assigned exclusively to a subscriber, in CDMA all subscribers in a cell use the same frequency band simultaneously. To separate the signals, each subscriber is assigned an orthogonal code called chip.

They are difficult to detect and jam. CDMA has been used in many communications and navigation systems, including the Global Positioning System (GPS) and in the satellite system for transportation.

Space Division Multiple Access (SDMA)

Along with the above access methods, space is also used effectively. This is a technique where different parts of space are used for multiplexing. It is a technique in which a transmitter transmits the modulated signal and accesses a slot of space and another transmitter uses another slot of space such that both the signals can propagate in two separate spaces in the medium without affecting each other. It is used in radio transmission and is more useful in satellite communication to optimize the use of radio spectrum by using directional properties of antenna. In SDMA, antennas are highly directional, allowing duplicate frequencies to be used at the same time for multiple surface zones on earth. Precise antenna alignment is also required.

Chapter-5
WIRELESS LAN

5.1 Wireless LAN and communication
5.2 Infrared
5.3 Radio Frequency
5.4 IR Advantages and Disadvantages
5.5 RF Advantages and Disadvantages
5.6 Wireless Network Architecture Logical
5.7 Types of WLAN
5.8 IEEE 802.11
5.9 MAC layer
5.10 Security
5.11 Synchronization
5.12 Power Management
5.13 Roaming
5.14 Bluetooth Overview

WIRELESS LAN AND COMMUNICATION

Wireless Communication is a method of transmitting information from one point to other, without using any connection like wires, cables or any physical medium.

What is WLAN???

A wireless local area network(LAN) is a flexible data communications system implemented as an extension to, or as an alternative for, a wired LAN.Using radio frequency (RF) technology, wireless LANs transmit and receive data over the air, minimizing the need for wired connections.

Thus, combining data connectivity with user mobility.

Advantages of WLAN

- Productivity, convenience, and cost advantages
- Installation speed and simplicity.
- Installation flexibility.
- Reduced cost-of-ownership.
- Mobility.
- Scalability.

Disadvantages of WLAN

- Cost
- Wireless network cards cost 4 times more than wired network cards.
- The access points are more expensive than hubs and wires.
- Signal Bleed Over
- Access points pick up the signals of adjacent access points or overpower their signal.
- Environmental Conditions
- Susceptible to weather and solar activity.
- Constrained by buildings, trees, terrain.
- Less Capacity

- Slower bandwidth.
- Limit to how much data a carrier wave can transmit without lost packets impacting performance.

Wireless LAN Applications

Medical Professionals
Corporate
Education
Temporary Situations
Airlines
Security Staff
Emergency Centers

INFRARED COMMUNICATION (IR)

This is one of the earliest types of optical communication and is still very much in use today. It is found in remote controls for televisions, dvd players and most other entertainment devices.Dimmer lights and other facilities can be also be controlled using infrared. Infrared uses light that is invisible to us and is just above the red end of the colour spectrum.The key component of an infrared system is an infrared LED (Light Emitting Diode) to emit the light and a photo- diode in the television or equipment to receive the light.A digital code within the controller switches the light on and off, this is then picked up as a digital code at the other end. The communication standard is called 'IrDA' short for Infrared Digital Association and it allows wire-less communication between Mouse, keyboard, joysticks, gamepads etc and receiving equipment such as PC, Laptop, game console.Bandwidth is normally quite modest, around 115.2 kbps (IrDA serial infrared standard). Although IrDA does define a fast data transfer standard of up to 14 Mbps, this is rarely used.IR works only up to about 10 metres but that is fine for the type of applications it is mainly used for. It will only work line-of-sight.Technologies such as Bluetooth has largely supplanted infrared as a communication method for mobiles and computers.

5.4 IR ADVANTAGES AND DISADVANTAGES

Advantages	Disadvantages
Inexpensive compared to other technologies	Only works line-of-sight
Works over a moderate bandwidth 115 kbps	Short range - a few metres
Works well over a short distance	Low bandwidth

5.3 RADIO FREQUENCY

RF is the short form of radio frequency. RF is used in wireless communications of every kind. The medium of communication is popularly called as RF wave similar to cable for wired communication.

It is all around us when we use cell phone, when we use Bluetooth device, when we use remote control, when we watch TV, when we listen radio, when we USE microwave oven. It has many applications and day by day it is increasing.

The unit of radio frequency is Hertz (Hz) i.e. no of oscillations or cycles per second. There is one more term which is often used interchangeably to mention RF and is called 'wavelength'. The relationship between wavelength and radio frequency is mentioned below.

Wavelength=C/Frequency,

Where C is the speed of light and is 3 x 10^8 meter/second.

Radio frequency is allocated and administered by FCC (Federal Communications Commission) and many such frequencies w l form electromagnetic spectrum. This spectrum is labeled with different names as below.

Designation	Frequency Range
Extremely Low Frequency (ELF)	3-30Hz
Super Low Frequency (SLF)	30-300Hz

Ultra Low Frequency (ULF)	300-3000Hz
Very Low Frequency (VLF)	3-30 KHz
Low Frequency (LF)	30-300 KHz
Medium Frequency (MF)	300KHz-3 MHz
High Frequency (HF)	3-30 MHz
Very High Frequency (VHF)	30 MHz-300 MHz
Ultra High Frequency (UHF)	300 MHz-3 GHz
Super High Frequency (SHF)	3-30 GHz
Extremely High Frequency (EHF)	30-300 GHz

Note:1000Hz=1KHz, 1000KHz=1MHz, 1000MHz=1GHz

The device which receives and transmits this radio frequency (RF) is called as antenna which everyone is familiar. There are different antennas designed to transmit and receive different RF frequencies as mentioned in the table.

RF ADVANTAGES AND DISADVANTAGES

Advantages of RF

Following are the advantages of RF:

=>It has different penetration through the walls of the buildings or houses based on the frequency. Hence used for radio and television transmission and for cellular mobile phone service.

=>Used in various medical applications. It is used in Diathermy instrument for surgery. It is used in MRI for taking images of human body. It is also used for skin tightening.

=>It is used in radar for object detection.

=>It is used for satellite communication.

=>It is used in microwave line of sight communication system.

Disadvantages of RF

Following are the disadvantages of RF:

=>Uncontrolled radiation of RF affects pre-adolescent childrens, pregnant women, elderly humans, patients with pace makers, small birds, flora and fauna, small insects etc.

=>The areas near RF cellular towers have been observed with more lightening compare to other areas.

=>It also affects some of the fruits grown near the RF tower areas.

=>As RF waves are available both in LOS and non LOS regions of transmitter, it can be easily intruded by the hackers and crucial personal/official data can be decoded for malicious motives. In order to avoid this situation, radio frequency wave based transmission is used with highly secured algorithms such as AES, WEP, WPA etc. RF signal can also be modulated either using frequency hopping or spread spectrum techniques to avoid this kind of eavesdropping.

WIRELESS NETWORK ARCHITECTURE LOGICAL

IEEE 802.11 Architecture

The components of an IEEE 802.11 architecture are as follows –

Stations (STA) – Stations comprises of all devices and equipment that are connected to the wireless LAN. A station can be oftwo types–

Wireless Access Point (WAP) – WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.

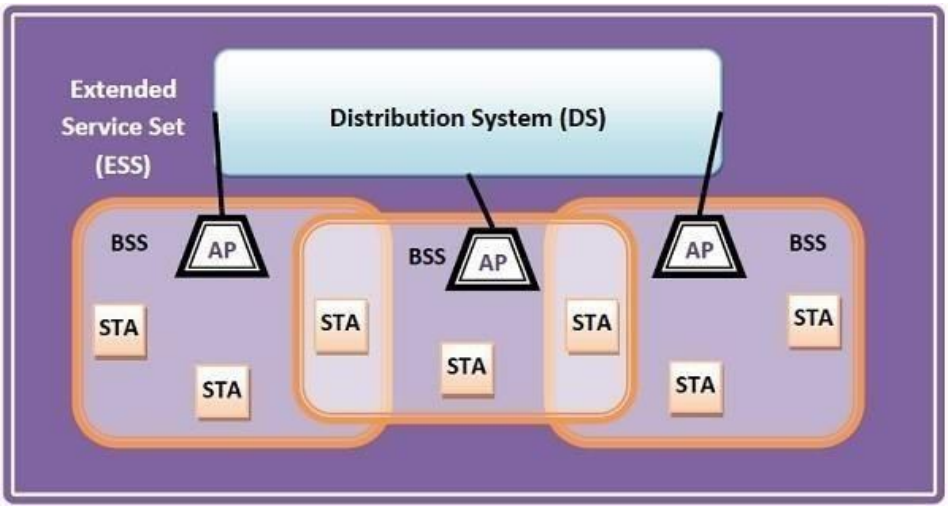
Client. Clients are workstations, computers, laptops, printers, smartphones, etc.Each station has a wireless network interface controller.

Basic Service Set (BSS) – A basic service set is a group of stations communicating at the physical layer level. BSS can be of two categories depending upon the mode of operation–

Infrastructure BSS – Here, the devices communicate with other devices through access points. Independent BSS – Here, the devices communicate in a peer-to-peer basis in an ad hoc manner.Extended Service Set (ESS) – It is a set of all connected BSS.

Distribution System (DS) – It connects access points in ESS.

Portal- Logical entity where 802.11 network integrates with a non 802.11 network.



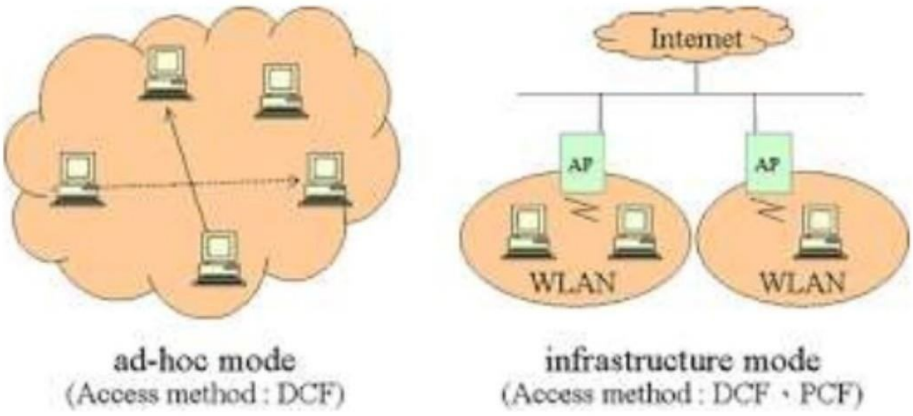
Types of WLAN

IEEE 802.11 Infrastructure

802.11 networks can be used in two modes: Infrastructure and Ad hoc Mode Infrastructure mode requires a central access point that all devices connect to.

Ad-hoc mode is also known as "peer-to-peer" mode. Ad-hoc networks don't require a centralized access point. Instead, devices on the wireless network connect directly to each other.

WLAN Topology Ad-Hoc Network and WLAN Topology Infrastructure



In infrastructure mode, each station computer (STA for short) connects to an access point via a wireless link. The set-up formed by the access point and the stations located within its coverage area are called the basic service set, or BSS for short. They form one cell.

Each BSS is identified by a BSSID, a 6-byte (48-bite) identifier. In infrastructure mode, the BSSID corresponds to the access point's MAC address.

- It is possible to link several access points together (or more precisely several BSS's) using a connection called a distribution system (DS for short) in order to form an extended service set or ESS. The distribution system can also be a wired network, a cable between two access points or even a wireless network.
- An ESS is identified with an ESSID (Extended Service Set Identifier), a 32-character identifier (in ASCII format) which acts as its name on the network. The ESSID, often shortened to SSID, shows the network's name, and in a way acts a firstlevel security measure, since it is necessary for a station to know the SSIDin order to connect to the extended network.
- In ad hoc mode, wireless client machines connect to one another in order to form a peer-to-peer network,i.e. a network in which every machine acts as both a client and an access point at the same time.
- The set-up formed by the stations is called the independent basic service set, or IBSS for short. An IBSS is a wireless network which has at least two stations and uses no access point. The IBSS therefore forms a temporary network which lets people in the same room exchange data. It is identified by an SSID, just like an ESS in infrastructure mode. In an ad hoc network, the range of the independent BSS is determined by each station's range. That means that if two of the stations on the network areoutside each other's range,they will not be able to communicate, even if they can "see" other stations. Unlike infrastructure mode, ad hoc mode has no distribution system that can send data frames from one station to another. An IBSS, then, is by definition a restricted wireless network.

5.8 IEEE 802.11

Wireless LAN Standard

In response to lacking standards, IEEE developed the first internationally recognized wireless LAN standard – IEEE 802.11 .IEEE published 802.11 in 1997, after seven years of work

Scope of IEEE 802.11 is limited to Physical and Data Link Layers.

IEEE 802.11 standard, popularly known as WiFi, lays down the architecture and specifications of wireless LANs (WLANs). WiFi or WLAN uses high frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage.

IEEE 802 LAN Standards Family:

MAC layer:

The 802.11 MAC sublayer provides an abstraction of the physical layer to the logical link control sublayer and upper layers of the OSI network. It is responsible for encapsulating frames and describing frame formats.

MAC Sublayer Frame Format of IEEE 802.11:

The main fields of a frame of wireless LANs as laid down by IEEE 802.11 are –

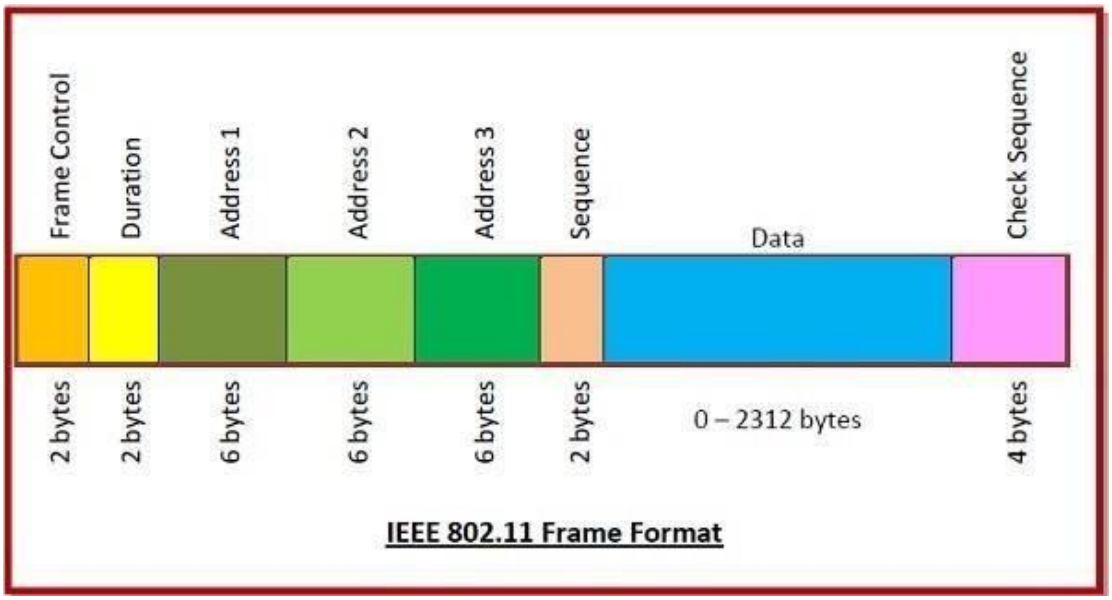
Frame Control – It is a 2 bytes starting field composed of 11 subfields. It contains control information of the frame.

Duration – It is a 2-byte field that specifies the time period for which the frame and its acknowledgment occupy the channel. Address fields – There are three 6-byte address fields containing addresses of source, immediate destination, and final endpoint respectively.

Sequence – It a 2 bytes field that stores the frame numbers.

Data – This is a variable-sized field that carries the data from the upper layers. The maximum size of the data field is 2312 bytes.

Check Sequence – It is a 4-byte field containing error detection information.



IEEE 802.11 Frame Format

Avoidance of Collisions by 802.11 MAC Sublayer

In wireless systems, the method of collision detection does not work. It uses a protocol calledcarrier sense multiple access with collision avoidance (CSMA/CA).

The method of CSMA/CA is –

When a frame is ready, the transmitting station checks whether the channel is idle or busy.If the channel is busy, the station waits until the channel becomes idle.

If the channel is idle, the station waits for an Inter-frame gap (IFG) amount of time and then sends the frame.After sending the frame, it sets a timer.

The station then waits for acknowledgement from the receiver. If it receives the acknowledgement before expiry of timer, it marks a successful transmission.

Otherwise, it waits for a back-off time period and restarts the algorithm.Co-ordination Functions in 802.11 MAC Sublayer

IEEE 802.11 MAC Sublayer uses two co-ordination functions for collision avoidance before transmission –

Distributed Coordination Function (DCF) –

It is a mandatory function used in CSMA/CA.

It is used in distributed contention-based channel access.

It is deployed in both Infrastructure BSS (basic service set) as well as Independent BSS.Point Coordination Function (PCF) –

It is an optional function used by 802.11 MAC Sublayer. It is used in centralized contention-free channel access. It is deployed in Infrastructure BSS only.

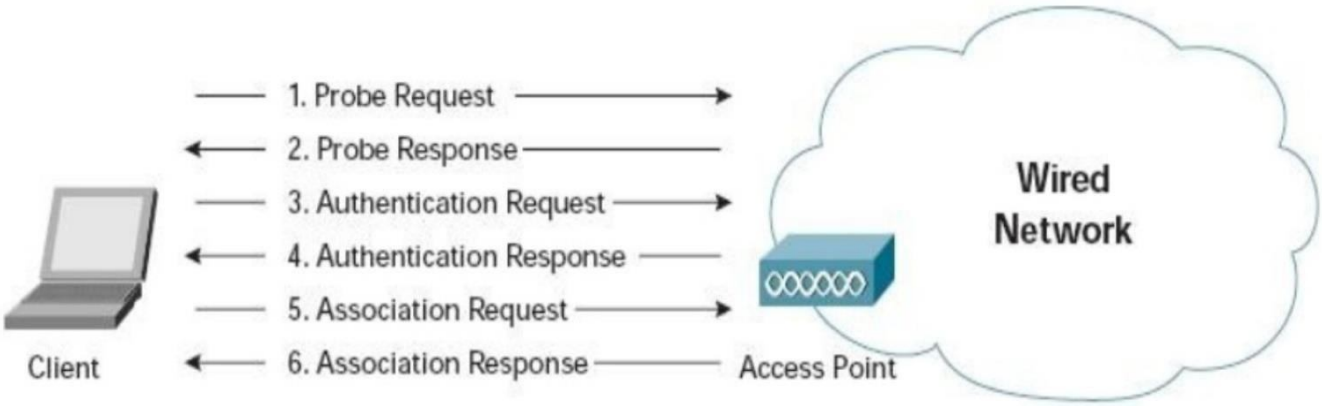
IEEE 802.11 standard, popularly known as WiFi, lays down the architecture and specifications of wireless LANs (WLANs). WiFi or WLAN uses high-frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage.

SECURITY

Wireless local area network security (WLAN security) is a security system designed to protect networks from the security breaches(/leakage) to which wireless transmissions are susceptible. This type of security is necessary because WLAN signals have no physical boundary limitations, and are prone to illegitimate access over network resources, resulting in the vulnerability of private and confidential data. Network operations and availability can also be compromised in case of a WLAN security breach. To address these issues, various authentications, encryption, invisibility and other administrative controlling

techniques are used in WLANs. Business and corporate WLANs in particular require adequate security measures to detect, prevent and block piggy backers, eavesdroppers and other intruders.

Security has remained a major concern in WLANs around the globe. While wireless networks provide convenience and flexibility, they also increase network vulnerability. Security threats such as unauthorized access, denial of service attacks, IP and MAC spoofing, session hijacking and eavesdropping can all be problems for WLANs. To counter these threats, various standard authentication and encryption techniques are combined with other access control mechanisms. These protocols, devices and techniques collectively secure the WLAN a level that equals and even exceeds wired LAN security.



Client Authentication Process

Some of the technologies employed in WLAN security include:

Wired Equivalent Privacy (WEP): An old encryption standard used to overcome security threats. WEP provides security to WLAN by encrypting the information transmitted over the air so that only the receivers with the correct encryption key can decrypt the information.

WPA/WPA2 (WI-FI Protected Access): Improved on WEP by introducing Temporal Key Integrity Protocol (TKIP). While still using RC4 encryption, TKIP uses a temporal encryption key that is regularly renewed, making it more difficult to steal. In addition, data integrity was improved through the use of a more robust hashing mechanism.

Wireless Intrusion Prevention Systems/Intrusion Detection Systems: Intrusion detection and prevention focuses on radio frequency (RF) levels. This involves radio scanning to detect rogue access points or ad hoc networks to regulate network access. Advanced implementations are able to visually represent the network area along with potential threats, and have automatic classification capabilities so that threats can be easily identified.

SYNCHRONIZATION:

Timing synchronization function (TSF) is specified in IEEE 802.11 wireless local area network (WLAN) standard to fulfill timing synchronization among users. A TSF keeps the timers for all stations in the same basic service set (BSS) synchronized. All stations shall maintain a local TSF timer. Each mobile host maintains a TSF timer with modulus 264 counting in increments of microseconds. The TSF
is based on a 1-MHz clock and "ticks" in microseconds. On a commercial level, industry vendors assume the 802.11 TSF's synchronization to be within 25 microseconds.

Timing synchronization is achieved by stations periodically exchanging timing information through beacon frames. In (infra) BSS, the AP sends the TSF information in the beacons. In Independent Basic Service Set (IBSS, ad-hoc), each station competes to send the beacon.

Each station maintains a TSF timer counting in increments of microseconds (μs). Stations adopt a received timing if it is later than the station's own TSF timer.

POWER MANAGEMENT

Power management is the feature that turns off the power or switches the system to a low power state when inactive.The basic idea to save power in WLAN is to switch off the transceiver whenever it is not needed.

Power management in infrastructure based network:

In infrastructure based network, an access point is responsible for the power management.Access point buffers data packet for all sleeping station.

Access point transmits a Traffic Indication Map (TIM) with a beacon frame.TIM consists of a list of destination of buffered data.

Additionally, the access point also maintains a Delivery Traffic Indication Map(DTIM)interval.

DTIM is used for sending broadcast/multicast frames. The DTIM interval is always a multiple of TIM interval. All station wakes up prior to an expected TIM and DTIM. Power management in Ad-hoc network

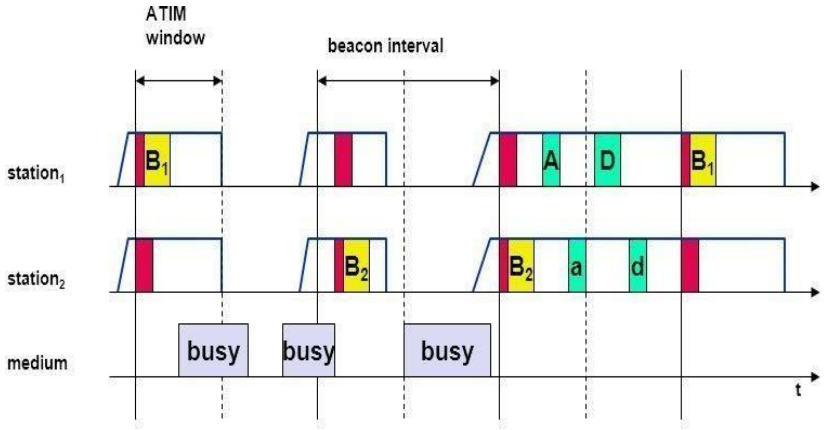
In ad-hoc network, each station buffers data packet that it wants to send to power saving station.

There is no access point.

In Ad-hoc network, all station announces a list of buffered frame during a period when they are all awake.

All station announce destination for which packets are buffered using Ad-hoc Traffic Indication Map (ATIM) during the ATM interval.

Figure shows Power Management in IEEE 802.11 Ad-hoc Network.



ROAMING:

Roaming refers to the ability for a cellular customer to automatically make and receive voice calls, send and receive data, or access other services, including home data services, when travelling outside the geographical coverage area of the home network, by means of using a visited network.

When a roaming user goes from one BSS to another while moving within the ESS, his or her machine's wireless network adapter is able to switch access points depending on the quality of the signal it receives from different access points. Access points communicate with one another using a distribution system in order to trade information about the stations and, if necessary, to transmit data from mobile stations. This feature which lets stations move "transparently" from one access point to another is called roaming.

BLUETOOTH OVERVIEW:

- Bluetooth technology is a short-range wireless communications technology to replace the cables connecting electronic devices, allowing a person to have a phone conversation via a headset, use a wireless mouse and synchronize information from a mobile phone to a PC, all using the same core system.

- Bluetooth wireless technology is a short range communications technology intended to replace the cables connectingportable unit and maintaining high levels of security. Bluetooth technology is based on Ad-hoc technology also known as Ad- hoc Pico nets, which is a local area network with a very limited coverage.

History of Bluetooth

- WLAN technology enables device connectivity to infrastructure based services through a wireless carrier provider. The need for personal devices to communicate wirelessly with one another without an established infrastructure has led to the emergence of Personal Area Networks (PANs).

- Ericsson's Bluetooth project in 1994 defines the standard for PANs to enable communication between mobile phones using low power and low cost radio interfaces.

- In May 1988, Companies such as IBM, Intel, Nokia and Toshiba joined Ericsson to form the Bluetooth Special Interest Group (SIG) whose aim was to develop a defacto standard for PANs.

- IEEE has approved a Bluetooth based standard named IEEE 802.15.1 for Wireless Personal Area Networks (WPANs). IEEE standard covers MAC and Physical layer applications.

- Bluetooth specification details the entire protocol stack. Bluetooth employs Radio Frequency (RF) for communication.It makes use of frequency modulation to generate radio waves in the ISM band.

- The usage of Bluetooth has widely increased for its special features.

- Bluetooth offers a uniform structure for a wide range of devices to connect and communicate with each other.

- Bluetooth technology has achieved global acceptance such that any Bluetooth enabled device, almost everywhere in the world, can be connected with Bluetooth enabled devices.

- Low power consumption of Bluetooth technology and an offered range of up to ten meters has paved the way for several usage models.

Bluetooth offers interactive conference by establishing an adhoc network of laptops.

Bluetooth usage model includes cordless computer, intercom, cordless phone and mobile phones.

Piconets and Scatternets:

- Bluetooth enabled electronic devices connect and communicate wirelessly through shortrange devices known as Piconets. Bluetooth devices exist in small ad-hoc configurations with the ability to act either as master or slave the specification allows a mechanism for master and slave to switch their roles. Point to point configuration with one master and one slave is the simplest configuration.

- When more than two Bluetooth devices communicate with one another, this is called a PICONET. A Piconet can contain up to seven slaves clustered around a single master. The device that initializes establishment of the Piconet becomes the master.

- The master is responsible for transmission control by dividing the network into a series of time slots amongst the network members, as a part of time division multiplexing scheme which is shown below.

The features of Piconets are as follows –

- Within a Piconet, the timing of various devices and the frequency hopping sequence of individual devices is determined by the clock and unique 48-bit address of master.

- Each device can communicate simultaneously with up to seven other devices within a single Piconet.

- Each device can communicate with several piconets simultaneously.

- Piconets are established dynamically and automatically as Bluetooth enabled devices enter and leave piconets.

- There is no direct connection between the slaves and all the connections are essentially master- to-slave or slave-to- master.Slaves are allowed to transmit once these have been polled by the master.Transmission starts in the slave-to-master time slot immediately following a polling packet from the master.A device can be a member of two or more piconets, jumping from one piconet to another by adjusting the transmission regime-timing and frequency hopping sequence dictated by the master device of the second piconet.

- It can be a slave in one piconet and master in another. It however cannot be a master in more than once piconet.

- Devices resident in adjacent piconets provide a bridge to support inner-piconet connections, allowing assemblies of linked piconets to form a physically extensible communication infrastructure known as Scatternet.

Spectrum:

- Bluetooth technology operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHZ, using a spread spectrum hopping, full-duplex signal at a nominal rate of 1600 hops/sec. the 2.4 GHZ ISM band is available andunlicensed in most countries.

Range:

- Bluetooth operating range depends on the device Class 3 radios have a range of up to 1 meter or 3 feet Class 2 radios are most commonly found in mobile devices have a range of 10 meters or 30 feet Class 1 radios are used primarily in industrial use cases have a range of 100 meters or 300 feet.

Data rate:

- Bluetooth supports 1Mbps data rate for version 1.2 and 3Mbps data rate for Version 2.0 combined with Error Data Rate.

****

Chapter-6

UBIQUITOUS WIRELESS COMMUNICATION

Mobile Communication Generations 1G to
3G 3rd Generation Mobile Communication
Network
Universal Mobile telecommunication System (UMTS)

INTRODUCTION:

Ubiquitous networking, also known as pervasive networking, is the distribution of communications infrastructure and wireless technologies throughout the environment to enable continuous connectivity.
Ubiquitous applications need to access relevant remote external information and tasks, anywhere and anytime.
Different applications require different combinations of network functions and services, e.g., data streaming, minimal jitter, specific media access control etc.
Different networks support different sets of communication functions in different ways.

SCENARIO OF MOBILE COMMUNICATION:

In order to tackle these challenges and target the right enabling technology components, the following five scenarios have been specified:
"Amazingly fast" focuses on providing very high data-rates for future mobile broadband users so as to experience instantaneous connectivity without delays.
"Great service in a crowd" focuses on providing reasonable mobile broadband experiences even in crowded areas such as stadiums, concerts or shopping malls.
"Best experience follows you" focuses on providing end-users on the move, e.g. in cars or trains, with high levels of service experience.
"Super real-time and reliable connections" focuses on new applications and use cases with very strict requirements on latency and reliability.
"Ubiquitous things communicating" focuses on the efficient handling of a very large number of devices (including e.g. machinetype of devices, and sensors) with widely varying requirements.

MOBILE COMMUNICATION GENERATIONS 1G TO 3G:

Since the introduction of first commercial mobile phone in 1983 by Motorola, mobile technology has come a long way. Be it technology, protocols, services offered or speed, the changes in mobile telephony have been recorded as generation of mobilecommunication. Here we will discuss the basic features of these generations that differentiate it from the previous generations.

1G Technology:

1G refers to the first generation of wireless mobile communication where analog signals were used to transmit data. It was introduced in the US in early 1980s and designed exclusively for voice communication. Some characteristics of 1G communication are –
Speeds up to 2.4
kbps Poor voice
quality
Large phones with limited
battery lifeNo data security

2G Technology:

2G refers to the second generation of mobile telephony which used digital signals for the first time. It was launched in Finland in1991 and used GSM technology. Some prominent characteristics of 2G communication are -
Data speeds up to 64 kbps
Text and multimedia messaging possible

Better quality than 1G
When GPRS technology was introduced, it enabled web browsing, e-mail services and fast upload/download speeds. 2G with GPRS is also referred as 2.5G, a step short of next mobile generation.

3G Technology:

Third generation (3G) of mobile telephony began with the start of the new millennium and offered major advancement over previous generations. Some of the characteristics of this generation are –
Data speeds of 144 kbps to 2 Mbps High speed web browsing
Running web based applications like video conferencing, multimedia e-mails, etc.Fast and easy transfer of audio and video files
3D gaming
Every coin has two sides. Here are some downsides of 3G technology –Expensive mobile phones
High infrastructure costs like licensing fees and mobile towers Trained personnel required for infrastructure set up
The intermediate generation, 3.5G grouped together dissimilar mobile telephony and data technologies and paved way for thenext generation of mobile communication.

3RD GENERATION MOBILE COMMUNICATION NETWORK:

Third generation mobile phones, or "3G Internet" mobile phones, is a set of standards for wireless mobile communication systems, that promises to deliver quality multimedia services along with high quality voice transmission.
Features
3G systems comply with the International Mobile Telecommunications-2000 (IMT- 2000) specifications by the International Telecommunication Union (ITU).
The first 3G services were available in 1998.
It provides high speed transmission having data transfer rate more than 0.2Mbps. Global roaming services are available for both voice and data.
It offers advanced multimedia access like playing music, viewing videos, television services etc.
It provides access to all advanced Internet services, for example surfing webpages with audio and video.
It paved the way for the increased usage of smartphones with wide screens as they provided better viewing of mobile webpages, videos and mobile televisions.

Specifications for 3G:

3G specifications are laid down by two groups, 3GPP and 3GPP2.
3GPP (Third Generation Partnership Project) – These specifications are based upon Global System for Mobile (GSM) communications, and are known as Universal Mobile Telecommunications Systems (UMTS). The technologies are :
Universal Terrestrial Radio Access (UTRA) General Packet Radio Service (GPRS)
Enhanced Data rates for GSM Evolution (EDGE)
3GPP2 – These specifications are based upon Code Division Multiple Access (CDMA). Two main specifications under this are –Wideband CDMA (WCDMA)
CDMA2000:
Areas of Application
Wireless voice telephony
Fixed wireless Internet access
Mobile Internet access
Video calls

Video conferencing
Tele-medicine
Global Positioning System (GPS) Location-based services

UNIVERSAL MOBILE TELECOMMUNICATION SYSTEM (UMTS):

The Universal Mobile Telecommunications System (UMTS) is a broadband, packet- based, 3G mobile cellular system based upon GSM standards. The specifications of UMTS covers the entire network system, including the radio access network, the core network and user authentication.

Features

UMTS is a component of IMT-2000 standard of the International Telecommunications Union (ITU), developed by 3GPP. It uses wideband code division multiple access (W-CDMA) air interface.
It provides transmission of text, digitized voice, video and multimedia.It provides high bandwidth to mobile operators.

It gives a high data rate of 2Mbps. For High-Speed Downlink Packet Access (HSDPA) handsets, the data-rate is as high as 7.2 Mbps in the downlink connection.
It is also known as Freedom of Mobile Multimedia Access (FOMA).
It encompasses specifications for the entire mobile network system –
Radio access network specified by UTRAN (UMTS Terrestrial Radio Access Network)Core network specified by MAP (Mobile Application Part)

****

Chapter 8
WORLD WIDE WEB ARCHITECTURE

The WWW architecture provides a very flexible and powerful programming model. Applications and content are presented in standard data formats, and are browsed by applications known as web browsers. The web browser is a networked application, i.e., it sends requests for named data objects to a network server and the network server responds with the data encoded using the standard formats.

The WWW standards specify many of the mechanisms necessary to build a general-purpose application environment.All servers and content on the WWW are named with-an Internet-standard Uniform Resource Locator (URL). All content on the WWW is given specific type thereby allowing web browsers to correctly process the content based on its type. All web browsers support a set of standard content formats. These include the Hyper Text Mark up Language (HTML) scripting languages (JavaScript) and a large number of other formats. Standard networking protocols allow any web browser To communicate with any web server. The most commonly used protocol on the WWW is the Hyper Text Transport Protocol (HTTP), operating on top of the TCP/IP protocol Suite.

NEED OF WAP

THE WIRELESS APPLICATION PROTOCOL (WAP) One obvious approach for such a common platform seems to be the Internet. The prevailed communication protocol in the Internet is TCP/IP, which offers a unified interface for transmitting data, independent of the underlying network. This idea has several advantages: All Internet-based applications such as WWW or e- mail can be used, and the integration of new applications is very easy by using TCP/IP, e.g., telephony via Internet using Voice over IP [V5]. However, using the Internet has one main disadvantage: The protocols for communication are optimised for fixed networks with high reliability and low error rates. In mobile environments, this property is very disadvantageous and affects the behaviour of applications in several negative ways:

• TCP/IP works very ineffective in wireless environments. IP is based on a hierarchical addressing scheme; thus, supporting mobility is hard to achieve. A solution for this problem might be Mobile IP [6]; but the deployment of Mobile IP raises several other problems, e.g. in security support [6]. Compared to fixed networks, wireless links usually have higher delays and frequent transient interruptions. In those cases, TCP supposes congestion on the link and immediately slows down the data rate to its minimum. The slow-start-algorithm implemented in TCP prevents an increase in performance, thus the overall performance is by far lower than technically feasible.

• Security mechanisms in the Internet, such as SSL (Secure Socket Layer), are not sufficient for applications that handle personal information, such as online banking or electronic commerce. Mechanisms for the authentication of mobile devices are not provided, and meanwhile, further less expendable encryption algorithms exist.

• On the higher layers, HTTP that transports WWW content works stateless and does not perform any compression, which blows up the data volume that has to be transmitted. Additionally, HTML used for describing WWW pages contains a lotof information useless for today's mobile devices, such as colourful pictures or java applets. Those disadvantages show the need for an alternative architecture with standardised protocols that are optimised for the use in mobile and wireless environments. Thus, in 1997, the WAP Forum was founded by a few companies in order to create an open, global specification that empowers mobile users with wireless devices to easily access and interact with information and services instantly. This aspect makes it interesting for the use in vehicles. Meanwhile, over 200 companies joined the forum, representing over 90 % of the global handset market, carriers with more than 100 million subscribers, leading infrastructure providers, software developers and other organizations providing solutions to the wireless industry. Figure 2 gives an overviewof a typical WAP infrastructure. A mobile device communicates with, e.g., a Web server via a WAP proxy. Thus, a set of new techniques can be used for the wireless network, such as protocols optimised for wireless links, or, as shown in figure 2, the use of the Wireless Markup Language (WML) instead of the unsuitable HTML for describing 4 the information. The WAP proxy is also integrated in the Internet environment, i.e., it can access Web Servers by simply using the Internet protocols, i.e., TCP/IP and HTTP. The basic communication interaction between mobile device and Web Server works in the following way. The mobile device sends an encoded request to the WAP Proxy, which decodes the request and translates it from the WAP protocol stack to the Internet protocol stack. The WAP Proxy passes the new request to the specified Web Server, which sendsthe requested information in a response back to the WAP Proxy. The information will be translated to the WAP protocols, encoded, and finally sent to the mobile device. There are two ways to create WML content. The first is to write raw WML code, which is stored directly on a Web Server. The WAP Proxy downloads this code via HTTP and sends it directly to the

mobile device, using the protocols defined in the WAP architecture. Alternatively, the WAP Proxy requests common HTML code, and converts it to WML code using specific filters. From the outset, WAP integrates speech services for telephony using WTA Servers (Wireless Telephony Application). This empowers the WAP architecture as one common platform for supporting voice and data communication and, thus, takes the preceding integration of voice and data services into account.

The WAP Architecture Starting with version 1.0 in 1999, version 1.1 is currently implemented in common mobile devices. Meanwhile, the standardisation of version 1.2 has been finished. Basically, version 1.1 and version 1.2 of WAP describe the same architecture and protocols; version 1.2 can be seen as an extension in order to support more features. The WAP architecture comprises six layers as can be seen in figure 3. The stack on the left hand compares the protocols used in the Internet with the layers of the WAP architecture. One main idea of WAP is the independence of communication protocols from the employed bearer service used for transmitting data. WAP only specifies the adaptation to those different bearers. In WAP 1.2, the adaptation to the following bearers is specified: various GSM services (e.g., GSM-CSD, GSM-GPRS, GSM-SMS, etc.), IS-136, CDPD, CDMA, PDC, iDEN, FLEX and ReFLEX, PHS, DataTAC, TETRA, and DECT. The WAP architecture is open in a way, that services and applications can be implemented using parts of the architecture, or have direct access to the bearer services.

Wireless Application Protocol (WAP) in Mobile Computing:

Wireless Application Protocol or WAP is a programming model or an application environment and set of communication protocols based on the concept of the World Wide Web (WWW), and its hierarchical design is very much similar to TCP/IP protocol stack design. The most prominent features of Wireless Application Protocol or WAP in Mobile Computing:

WAP is a De-Facto standard or a protocol designed for micro-browsers, and it enables the mobile devices to interact, exchange and transmit information over the Internet.

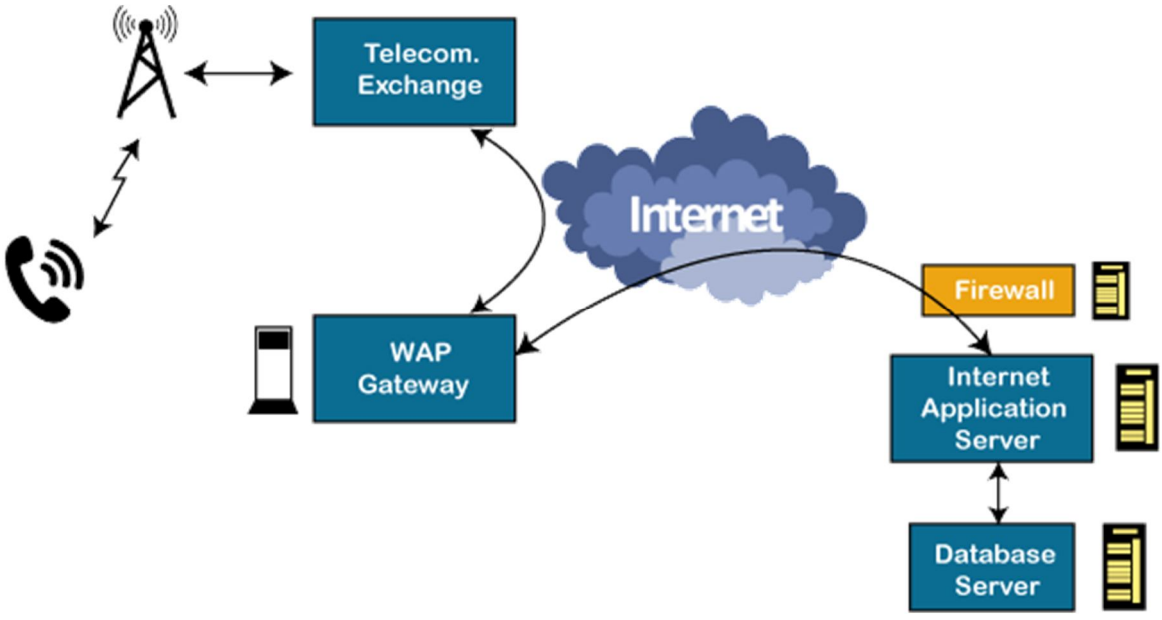
WAP is based upon the concept of the World Wide Web (WWW), and the backend functioning also remains similar to WWW, but it uses the markup language Wireless Markup Language (WML) to access the WAP services while WWW uses HTML as a markup language. WML is defined as XML 1.0 application.

In 1998, some giant IT companies such as Ericson, Motorola, Nokia and Unwired Planet founded the WAP Forum to standardize the various wireless technologies via protocols.

After developing the WAP model, it was accepted as a wireless protocol globally capable of working on multiple wireless technologies such as mobile, printers, pagers, etc.

In 2002, by the joint efforts of the various members of the WAP Forum, it was merged with various other forums of the industry and formed an alliance known as Open Mobile Alliance (OMA).

WAP was opted as a De-Facto standard because of its ability to create web applications for mobile devices.



Working of Wireless Application Protocol or WAP Model:

The following steps define the working of Wireless Application Protocol or WAP Model:

The WAP model consists of 3 levels known as Client, Gateway and Origin Server.

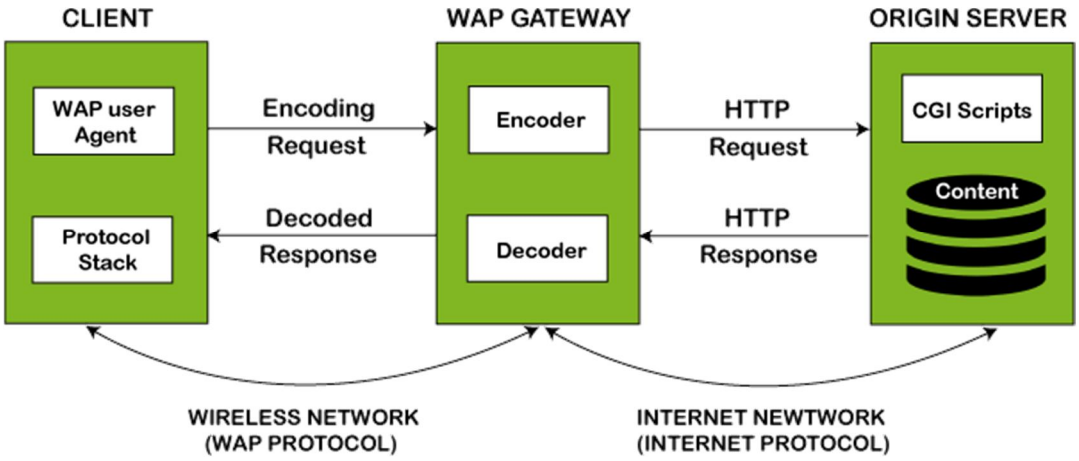
When a user opens the browser in his/her mobile device and selects a website that he/she wants to view, the mobile device sends the URL encoded request via a network to a WAP gateway using WAP protocol.

The request he/she sends via mobile to WAP gateway is called as encoding request.

The sent encoding request is translated through WAP gateway and then forwarded in the form of a conventional HTTP URL request over the Internet.

When the request reaches a specified Web server, the server processes the request just as it would handle any other requestand sends the response back to the mobile device through WAP gateway.

Now, the WML file's final response can be seen in the browser of the mobile users.



Benefits of Wireless Application Protocol (WAP):

Following is a list of some advantages of Wireless Application Protocol or WAP:

WAP is a very fast-paced technology.

It is an open-source technology and completely free of cost.It can be implemented on multiple platforms.

It is independent of network standards. It provides higher controlling options.

It is implemented near to Internet model.

By using WAP, you can send/receive real-time data.

Nowadays, most modern mobile phones and devices support WAP.

Disadvantages of Wireless Application Protocol (WAP):

Following is a list of some disadvantages of Wireless Application Protocol or WAP:The connection speed in WAP is slow, and there is limited availability also.

In some areas, the ability to connect to the Internet is very sparse, and in some other areas, Internet access is entirely unavailable.

It is less secured.

WAP provides a small User interface (UI).

Applications of Wireless Application Protocol (WAP)

The following are some most used applications of Wireless Application Protocol or WAP:

WAP facilitates you to access the Internet from your mobile devices. You can play games on mobile devices over wireless devices.

It facilitates you to access E-mails over the mobile Internet.

Mobile hand-sets can be used to access timesheets and fill expenses claims.Online mobile banking is very popular nowadays.

It can also be used in multiple Internet-based services such as geographical location, Weather forecasting, Flight information, Movie & cinema information, Traffic updates etc. All are possible due to WAP technology.

WAP architecture:

WAP is designed in a layered fashion, so that it can be extensible, flexible, and scalable. As a result, the WAP protocol stack is divided into five layers –

Layers of WAP Protocol:

Application Layer:

Wireless Application Environment (WAE). This layer is of most interest to content developers because it contains among other things, device specifications, and the content development programming languages, WML, and WMLScript.

Session Layer:

Wireless Session Protocol (WSP). Unlike HTTP, WSP has been designed by the WAP Forum to provide fast connection suspension and reconnection.

Transaction Layer:

Wireless Transaction Protocol (WTP). The WTP runs on top of a datagram service, such as User Datagram Protocol (UDP) and is part of the standard suite of TCP/IP protocols used to provide a simplified protocol suitable for low bandwidth wireless stations.

Security Layer:

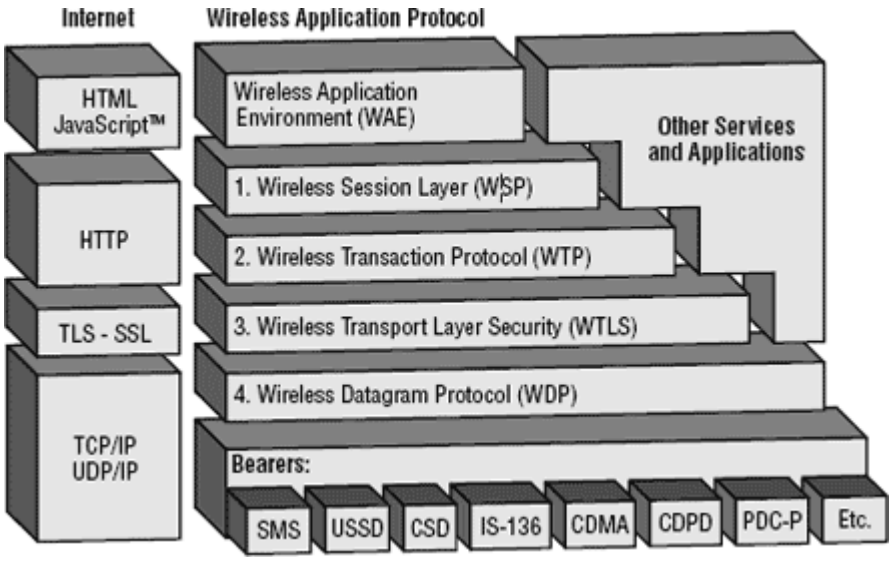
Wireless Transport Layer Security (WTLS). WTLS incorporates security features that are based upon the established Transport Layer Security (TLS) protocol standard. It includes data integrity checks, privacy, service denial, and authentication services.

Transport Layer:

Wireless Datagram Protocol (WDP). The WDP allows WAP to be bearer-independent by adapting the transport layer of the underlying bearer. The WDP presents a consistent data format to the higher layers of the WAP protocol stack, thereby offering the advantage of bearer independence to application developers.

Each of these layers provides a well-defined interface to the layer above it. This means that the internal workings of any layer are transparent or invisible to the layers above it. The layered architecture allows other applications and services to utilise the features provided by the WAP-stack as well. This makes it possible to use the WAP-stack for services and applications that currently are not specified by WAP.

The WAP protocol architecture is shown below alongside a typical Internet Protocol stack.



Note that the mobile network bearers in the lower part of the figure above are not part of the WAP protocol stack.WAP Protocol:

It specifies the different communications and data transmission layers used in the WAP model:

Application Layer : This layer consists of the Wireless Application Environment (WAE), mobile device specifications, and content development programming languages, i.e., WML.

Session Layer : The session layer consists of the Wireless Session Protocol (WSP). It is responsible for fast connection suspension and reconnection.

Transaction Layer: The transaction layer consists of Wireless Transaction Protocol (WTP) and runs on top of UDP (User Datagram Protocol). This layer is a part of TCP/IP and offers transaction support.

Security Layer: It contains Wireless Transaction Layer Security (WTLS) and responsible for data integrity, privacy and authentication during data transmission.

Transport Layer: This layer consists of Wireless Datagram Protocol (WDP). It provides a consistent data format to higher layers of the WAP protocol stack.

WML

The topmost layer in the WAP (Wireless Application Protocol) architecture is made up of WAE (Wireless Application Environment), which consists of WML and WML scripting language.

- WML stands for Wireless Markup Language
- WML is an application of XML, which is defined in a document-type definition.
- WML is based on HDML and is modified so that it can be compared with HTML.
- WML takes care of the small screen and the low bandwidth of transmission.
- WML is the markup language defined in the WAP specification.
- WAP sites are written in WML, while web sites are written in HTML.
- WML is very similar to HTML. Both of them use tags and are written in plain text format.
- WML files have the extension ".wml". The MIME type of WML is "text/vnd.wap.wml".
- WML supports client-side scripting. The scripting language supported is called WMLScript.

WML Versions:

WAP Forum has released a latest version WAP 2.0. The markup language defined in WAP 2.0 is XHTML Mobile Profile (MP). The WML MP is a subset of the XHTML. A style sheet called WCSS (WAP CSS) has been introduced alongwith XHTML MP. The WCSS is a subset of the CSS2.

Most of the new mobile phone models released are WAP 2.0-enabled. Because WAP 2.0 is backward compatible to WAP 1.x, WAP 2.0-enabled mobile devices can display both XHTML MP and WML documents.

WML 1.x is an earlier technology. However, that does not mean it is of no use, since a lot of wireless devices that only supports WML 1.x are still being used. Latest version of WML is 2.0 and it is created for backward compatibility purposes. So WAP site developers need not to worry about WML 2.0.

WML Decks and Cards:

A main difference between HTML and WML is that the basic unit of navigation in HTML is a page, while that in WML is a card. A WML file can contain multiple cards and they form a deck.

When a WML page is accessed from a mobile phone, all the cards in the page are downloaded from the WAP server. So if the user goes to another card of the same deck, the mobile browser does not have to send any requests to the server since the filethat contains the deck is already stored in the wireless device.

You can put links, text, images, input fields, option boxes and many other elements in a card.WML Program Structure:

Following is the basic structure of a WML program:

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.2//EN"
"http://www.wapforum.org/DTD/wml12.dtd">
<wml>
<card id="one" title="First Card">
<p>
This is the first card in the deck
</p>
 </card>
```

<card id="two" title="Second Card">

Ths is the second card in the deck

</card>
</wml>

The first line of this text says that this is an XML document and the version is 1.0. The second line selects the document type and gives the URL of the document type definition (DTD).

One WML deck (i.e. page) can have one or more cards as shown above. We will see complete details on WML document structure in subsequent chapter.

Unlike HTML 4.01 Transitional, text cannot be enclosed directly in the <card>...</card> tag pair. So you need to put a content inside ... as shown above.

WAP Site Design Considerations:

Wireless devices are limited by the size of their displays and keypads. It's therefore very important to take this into account when designing a WAP Site.

While designing a WAP site you must ensure that you keep things simple and easy to use. You should always keep in mind that there are no standard microbrowser behaviors and that the data link may be relatively slow, at around 10Kbps. However, with GPRS, EDGE, and UMTS, this may not be the case for long, depending on where you are located.

The following are general design tips that you should keep in mind when designing a service:Keep the WML decks and images to less than 1.5KB.

Keep text brief and meaningful, and as far as possible try to precode options to minimize the rather painful experience of user data entry.

Keep URLs brief and easy to recall.

Minimize menu levels to prevent users from getting lost and the system from slowing down. Use standard layout tags such as <big> and <b>, and logically structure your information.

Don't go overboard with the use of graphics, as many target devices may not support them.

WML – Environment:

To develop WAP applications, you will need the following:

A WAP enabled Web Server: You can enable your Apache or Microsoft IIS to serve all the WAP client request.A WAP Gateway Simulator: This is required to interact to your WAP server.

A WAP Phone Simulator: This is required to test your WAP Pages and to show all the WAP pages.You can write your WAP pages using the following languages:

Wireless Markup Language(WML) to develop WAP application. WML Script to enhance the functionality of WAP application. **Configuring Web Server:**

In normal web applications, MIME type is set to text/html, designating normal HTML code. Images, on the other hand, could be specified as image/gif or image/jpeg, for instance. With this content type specification, the web browser knowsthe data type that the web server returns.

To make your Apache WAP compatible, you have nothing to do very much. You simply need to add support for the MIME types and extensions listed below.

File Extension	MIME type
WML (.wml)	text/vnd.wap.wml
WMLScript (.wmls)	text/vmd.wap.wmlscript
WMLScriptc (.wmlsx)	application/vnd.wap.wmlscriptc
WMLC (.wmlc)	application/vnd.wap.wmlc

WBMP (.wbmp)	image/vnd.wap.wbmp

Configure Apache Web Server for WAP:

Assuming you have Apache Web server installed on your machine. So now we will tell you how to enable WAP functionality in your Apache web server.So locate Apache's file httpd.conf which is usually in /etc/httpd/conf, and add the following lines to the file and restart the server:

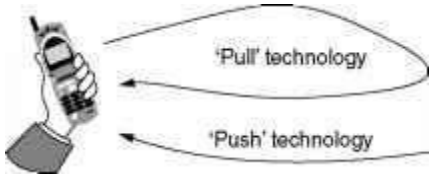
AddType text/vnd.wap.wml .wml
AddType text/vnd.wap.wmlscript
.wmls AddType
application/vnd.wap.wmlc .wmlc
AddType application/vnd.wap.wmlscriptc
.wmlsc AddType image/vnd.wap.wbmp
.wbmp

In dynamic applications, the MIME type must be set on the fly, whereas in static WAP applications the web server must beconfigured appropriately.

PUSH ARCHITECTURE

WAP Push Architecture:

The WAP Push framework introduces a means within the WAP effort to transmit information to a device without a previous user action. In the client/server model, a client requests a service or information from a server, which transmits information to the client. In this pull technology, the client pulls information from the server. An example of pull technology is WWW, in which a user enters a URL (the request), sent then to a server, which answers by sending a Web page (the response) to the user. In the push technology based on client/server model, there is no explicit request from the client before the server transmits its content.



Comparison of pull and push technology.Server

Pull and push technology:

Pull transactions are initiated by the client, whereas push transactions are initiated by the server.A push operation in WAP occurs when a Push Initiator transmits content to a client using either the Push OTA protocol or the Push Access Protocol (PAP). The Push Initiator does not share a protocol with the WAP client since the Push Initiator is on the Internet and the WAP client is on the WAP domain. The Push Initiator contacts the WAP Client through a translating Push Proxy Gateway (PPG) from the Internet side, delivering content for the destination client using Internet protocols. The PPG forwards the pushed content to the WAP domain, and the content is then transmitted over the air in the mobile network to the destination client. The PPG may be capable of notifying the Push Initiator about the final outcome of the push operation, and it may wait for the client to accept or reject the content in two-way mobile networks. It may also provide the Push Initiator with client capability lookup services by letting a Push Initiator select the optimal content for this client.

The Internet side PPG access protocol is called the PAP. The WAP side protocol is called OTAProtocol. The PAP uses XML messages that may be tunneled through various Internet protocols, for example, HTTP. The OTA protocol is based on WSP services. The PPG acts as an access point for content pushes from the Internet to the mobile network, and associated authentication, security, client control, and so on. The PPG owner decides the policies about who is able to gain access to the WAP network, who is able to push content, and so on. The PPG functionality may be built into the pull WAP gateway that givesthe benefit of shared resources and shared sessions over the air.

The PPG accepts pushed content from the Internet using the PAP. The PPG acknowledges successful parsing or reports unsuccessful parsing of the control information and may report debug information about the content. It may also perform a callback to the pushing server when the final status of the push submission has been reached, if the Push Initiator so requests.

When the content has been accepted for delivery, the PPG attempts to find the correct destination device and deliver the content to the client using the Push OTA protocol. The PPG attempts to deliver the content until a timeout expires, which can be set by the Push Initiator and/or the policies of the mobile operator.

The PPG may encode WAP content types into their binary counterparts. This transaction takes place before delivery over the air. Other content types may be forwarded as received. The Push Initiator may also precompile its content into binary form to take workload off the PPG, for example. When the PPG receives precompiled WML, WMLScript, or SIs, they are forwarded as received.

The PPG may implement addressing aliasing schemes to enable special multi- and broadcast cases, in which special addresses may translate to a broadcast operation.

A Push Initiator may query the PPG for client capabilities and preferences to create better formatted content for a particular WAP device. The PAP is used by an Internet-based Push Initiator to push content to a mobile network addressing its PPG. The PAP initially uses HTTP, but it can be tunneled through any other or future Internet protocol. The PAP carries an XML-style entity that may be used with other components in a multipart-related document. The PAP supports the following operations:

- Push Submission (Initiator to PPG)
- Result Notification (PPG to Initiator)
- Push Cancellation (Initiator to PPG)
- Status Query (Initiator to PPG)
- Client Capabilities Query (Initiator to PPG).

The push message contains three entities: a control entity, a content entity, and optionally a capability entity. They are used in a multipart-related message, which is sent from the Push Initiator to the PPG. The control entity is an XML document containing delivery instructions destined for the PPG, and the content entity is destined for the mobile device.

If the Push Initiator requested a confirmation of successful delivery, the message is transmitted from the PPG to the Push Initiator when the content is delivered to the mobile device over a two-way bearer, or transmitted to the device over a one- way bearer, and it contains an XML entity. The message is also transmitted in case of a detected delivery failure to inform the Initiator about it.

The Push Initiator relies on the response from the PPG; a confirmed push is then confirmed by the WAP device only when the target application has taken responsibility for the pushed content. Otherwise, the application must abort the operation and the Push Initiator knows that the content never reached its destination.

An XML entity can be transmitted from the Push Initiator to the PPG requesting cancellation of the previously submitted content. The PPG responds with an XML entity whether or not the cancellation was successful. An XML can also be transmitted from the Push Initiator to the PPG requesting status of the previously submitted content. The PPG responds with an XML entity. An XML entity transmitted from the Push Initiator to the PPG can request the capabilities of a device on the network. The PPG responds with a multipart related in two parts, in which the multipart root is the result of the request, and the second part is the capabilities of the device. The WAP is carried over HTTP/1.1 in this issue of WAP Push.

The SI content type provides the ability to send notifications to end users in an asynchronous manner. An SI contains a short message and a URI indicating a service. The message is presented to the end user upon reception, and the user is giventhe choice to either start the service indicated by the URI immediately or to postpone the SI for later handling. If the SI is postponed, the client stores it and the end user is given the possibility to act upon it at a later time.

The Push OTA protocol is a thin protocol layer on top of WSP, and it is responsible for transporting content from the PPG to the client and its user agents. The OTA protocol may use WSP sessions to deliver its content. Connection-oriented pushes require that an active WSP session is available, but a session cannot be created by the server. When there is no active WSP session, the Push framework introduces a Session Initiation Application (SIA) in the client that listens to session requests from the OTA servers and responds by setting up a WSP session for push purposes. The client may verify the identity information in this request against a list of recognized OTA servers before attempting to establish any push sessions. Push delivery may also be performed without the use of sessions in a connectionless manner, which is needed in one-way networks.

A connection-oriented push requires an active WSP session. Only the client can create sessions. If the server receives a requestfor a connection-oriented push to a client, and there are no active sessions to that client, the server cannot deliver the push content. A session request is sent to a special application in the client known as the SIA. This request contains information necessary for a client to create a push session. The SIA in the client after receiving a session request establishes a session with the PPG and indicates which applications accept content over the newly opened session. The SIA may also ignore the request if there is no suitable installed application as requested in the session request.When a client receives pushed content, a dispatcher looks at the push message header to determine its destination application. This dispatcher is responsible for rejecting content that does not have a suitable destination application installed, and for confirming push operations to the PPG when the appropriate application takes responsibility for pushed content.

****

CHAPTER 9
WIRELESS TELECOM NETWORK

GSM:

GSM stands for Global System for Mobile Communication. It is a digital cellular technology used for transmitting mobile voice and data services. Important facts about the GSM are given below –

The concept of GSM emerged from a cell-based mobile radio system at Bell Laboratories in the early 1970s.

GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard.GSM is the most widely accepted standard in telecommunications and it is implemented globally.

GSM is a circuit-switched system that divides each 200 kHz channel into eight 25 kHz time-slots. GSM operates on the mobile communication bands 900 MHz and 1800 MHz in most parts of the world. In the US, GSM operates in the bands 850 MHz and 1900 MHz.

GSM owns a market share of more than 70 percent of the world's digital cellular subscribers.

GSM makes use of narrowband Time Division Multiple Access (TDMA) technique for transmitting signals. GSM was developed using digital technology. It has an ability to carry 64 kbps to 120 Mbps of data rates.

Presently GSM supports more than one billion mobile subscribers in more than 210 countries throughout the world.

GSM provides basic to advanced voice and data services including roaming service. Roaming is the ability to use your GSM phone number in another GSM network.

GSM digitizes and compresses data, then sends it down through a channel with two other streams of user data, each in its own timeslot.

Why GSM :

Listed below are the features of GSM that account for its popularity and wide acceptance.

Improved spectrum efficiency International roaming

Low-cost mobile sets and base stations (BSs)High-quality speech

Compatibility with Integrated Services Digital Network (ISDN) and other telephone company services

Support for new services

A GSM network comprises of many functional units. These functions and interfaces are explainedThe GSM network can be broadly divided into –

- The Mobile Station (MS)
- The Base Station Subsystem (BSS)
- The Network Switching Subsystem (NSS)
- The Operation Support Subsystem (OSS)

GSM - The Mobile Station

The MS consists of the physical equipment, such as the radio transceiver, display and digital signal processors, and the SIM card. It provides the air interface to the user in GSM networks. As such, other services are also provided, which include –

Voice teleservices

Data bearer services

The features' supplementary services

The MS Functions

The MS also provides the receptor for SMS messages, enabling the user to toggle between the voice and data use. Moreover, the mobile facilitates access to voice messaging systems. The MS also provides access to the various data services available in a GSM network. These data services include –

X.25 packet switching through a synchronous or asynchronous dial-up connection to the PAD at speeds typically at 9.6 Kbps.

General Packet Radio Services (GPRSs) using either an X.25 or IP based data transfer method at the speed up to 115 Kbps.

High speed, circuit switched data at speeds up to 64 Kbps.

We will discuss more about GMS services in GSM - User Services.

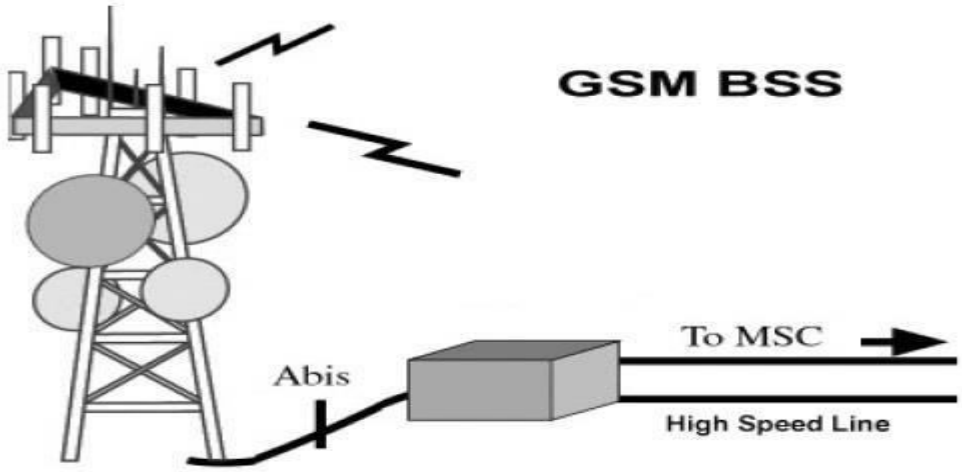
What is SIM:

The SIM provides personal mobility so that the user can have access to all subscribed services irrespective of both the location of the terminal and the use of a specific terminal. You need to insert the SIM card into another GSM cellular phone to receive calls at that phone, make calls from that phone, or receive other subscribed services.

GSM - The Base Station Subsystem (BSS)

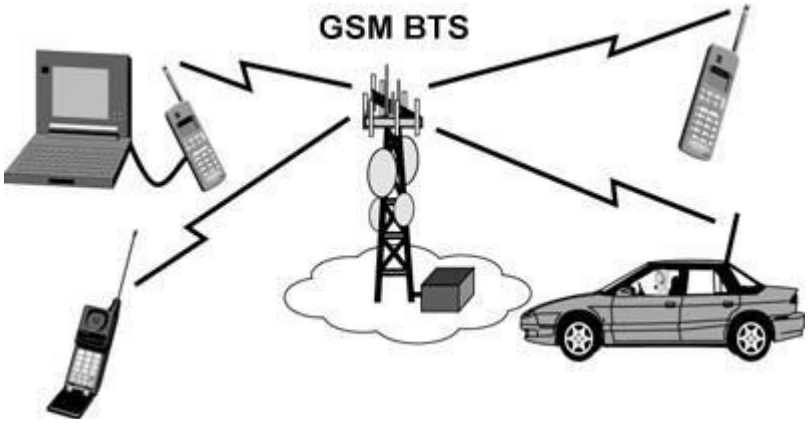
The BSS is composed of two parts –The Base Transceiver Station (BTS) The Base Station Controller (BSC)

The BTS and the BSC communicate across the specified Abis interface, enabling operations between components thatare made by different suppliers. The radio components of a BSS may consist of four to seven or nine cells. A BSS may have one or more base stations. The BSS uses the Abis interface between the BTS and the BSC. A separate high-speed line (T1 or E1) is then connected from the BSS to the Mobile MSC.



The Base Transceiver Station (BTS)

The BTS houses the radio transceivers that define a cell and handles the radio link protocols with the MS. In a large urban area,a large number of BTSs may be deployed.



The BTS corresponds to the transceivers and antennas used in each cell of the network. A BTS is usually placed in the center of a cell. Its transmitting power defines the size of a cell. Each BTS has between 1 and 16 transceivers, depending on thedensity of users in the cell. Each BTS serves as a single cell. It also includes the following functions – Encoding, encrypting, multiplexing, modulating, and feeding the RF signals to the antenna Transcoding and rate adaptation Time and frequency synchronizing Voice through full- or half-rate services Decoding, decrypting, and equalizing received signals Random access detection Timing advances Uplink channel measurements The Base Station Controller (BSC)

.The BSC manages the radio resources for one or more BTSs. It handles radio channel setup, frequency hopping, and handovers. The BSC is the connection between the mobile and the MSC. The BSC also translates the 13 Kbps voice channel used over the radio link to the standard 64 Kbps channel used by the Public Switched Telephone Network (PSDN) or ISDN.

It assigns and releases frequencies and time slots for the MS. The BSC also handles intercell handover. It controls the power transmission of the BSS and MS in its area. The function of the BSC is to allocate the necessary time slots between the BTS and the MSC. It is a switching device that handles the radio resources.

The additional functions include–

Control of frequency hopping

Performing traffic concentration to reduce the number of lines from the MSC Providing an interface to the Operations and Maintenance Center for the BSSReallocation of frequencies among BTSs

Time and frequency synchronization Power management Time-delay measurements of received signals from the MS

GSM - The Network Switching Subsystem (NSS)

The Network switching system (NSS), the main part of which is the Mobile Switching Center (MSC), performs the switching of calls between the mobile and other fixed or mobile network users, as well as the management of mobile services such as authentication.

The switching system includes the following functional elements –Home Location Register (HLR):

The HLR is a database used for storage and management of subscriptions. The HLR is considered the most important database, as it stores permanent data about subscribers, including a subscriber's service profile, location information, and activity status. When an individual buys a subscription in the form of SIM, then all the information about this subscription is registered in the HLR of that operator.

Mobile Services Switching Center (MSC):

The central component of the Network Subsystem is the MSC. The MSC performs the switching of callsbetween the mobile and other fixed or mobile network users, as well as the management of mobile services such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber. It also performs such functions as toll ticketing, network interfacing, common channel signaling, and others. Every MSC is identified by a unique ID.

Visitor Location Register (VLR):

The VLR is a database that contains temporary information about subscribers that is needed by the MSC in order to service visiting subscribers. The VLR is always integrated with the MSC. When a mobile station roams into a new MSC area, the VLR connected to that MSC will request data about the mobile station from the HLR. Later, if the mobile station makes a call, the VLR will have the information needed for call setup without having to interrogate the HLR each time.

Authentication Center (AUC):

The Authentication Center is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and ciphering of the radio channel. The AUC protects network operators from different types of fraud found in today's cellular world.

Equipment Identity Register (EIR):

The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where its International Mobile Equipment Identity (IMEI) identifies each MS. An IMEI is marked as invalid if it has been reported stolen or is not type approved.

GSM - The Operation Support Subsystem (OSS):

The operations and maintenance center (OMC) is connected to all equipment in the switching system and to the BSC. The implementation of OMC is called the operation and support system (OSS).

Here are some of the OMC functions–:

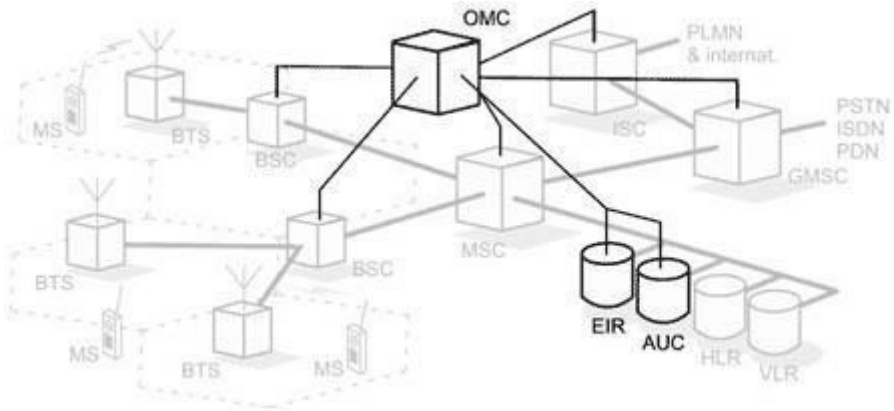
Administration and commercial operation (subscription, end terminals, charging, and statistics). Security Management.

Network configuration, Operation, and Performance Management.

Maintenance Tasks.

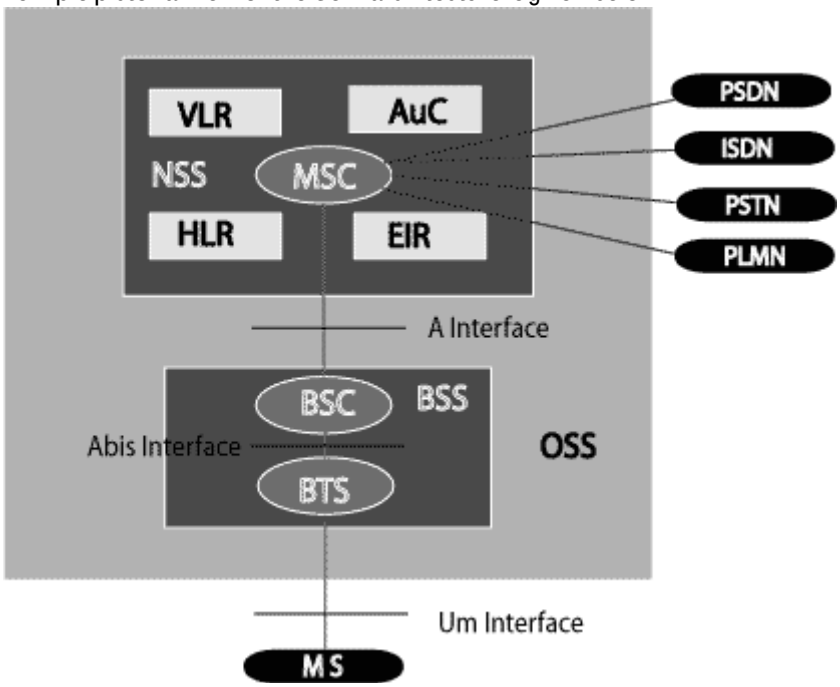
The operation and Maintenance functions are based on the concepts of the Telecommunication Management Network (TMN), which is standardized in the ITU-T series M.30.

Following is the figure, which shows how OMC system covers all the GSM elements.



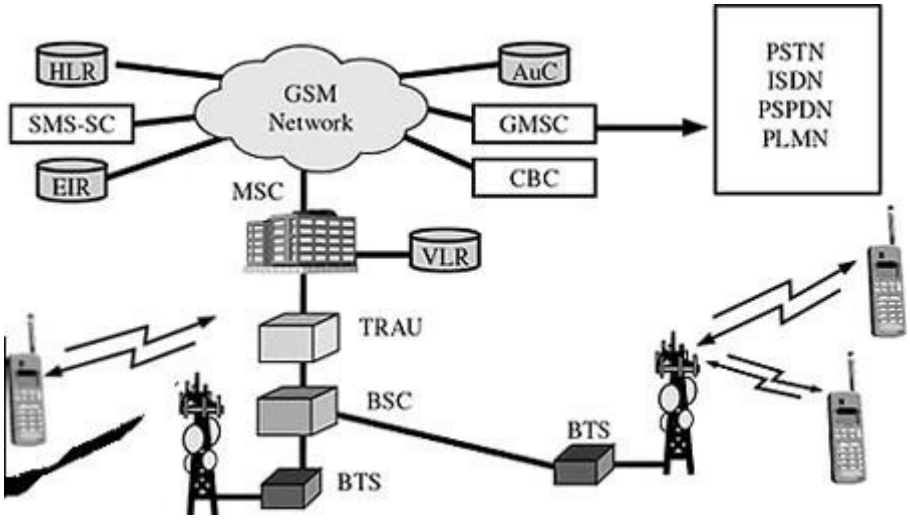
The OSS is the functional entity from which the network operator monitors and controls the system. The purpose of OSS is to offer the customer cost-effective support for centralized, regional, and local operational and maintenance activities that are required for a GSM network. An important function of OSS is to provide a network overview and support the maintenance activities of different operation and maintenance organizations.

A simple pictorial view of the GSM architecture is given below –



The additional components of the GSM architecture comprise of databases and messaging systems functions –Home Location Register (HLR)
Visitor Location Register (VLR) Equipment Identity Register (EIR) Authentication Center (AuC) SMS Serving Center (SMS SC) Gateway MSC (GMSC) Chargeback Center (CBC)
Transcoder and Adaptation Unit (TRAU)

The following diagram shows the GSM network along with the added elements –



The MS and the BSS communicate across the Um interface. It is also known as the air interface or the radio link.
TheBSS communicates with the Network Service Switching (NSS) center across the A interface.
GSM network areas
In a GSM network, the following areas are defined –
Cell – Cell is the basic service area; one BTS covers one cell. Each cell is given a Cell Global Identity (CGI), a number that uniquely identifies the cell.

Location Area – A group of cells form a Location Area (LA). This is the area that is paged when a subscriber gets an incoming call. Each LA is assigned a Location Area Identity (LAI). Each LA is served by one or more BSCs.
MSC/VLR Service Area – The area covered by one MSC is called the MSC/VLR service area.
PLMN – The area covered by one network operator is called the Public Land Mobile Network (PLMN). A PLMN can contain oneor more MSCs.

GPRS

General Packet Radio System is also known as GPRS is a third-generation step toward internet access. GPRS is also known as GSM-IP that is a Global-System Mobile Communications Internet Protocol as it keeps the users of this system online, allows to make voice calls, and access internet on-the-go. Even Time-Division Multiple Access (TDMA) users benefit from this system as it provides packet radio access.
GPRS also permits the network operators to execute an Internet Protocol (IP) based core architecture for integrated voice and data applications that will continue to be used and expanded for 3G services.
GPRS supersedes the wired connections, as this system has simplified access to the packet data networks like the internet. Thepacket radio principle is employed by GPRS to transport user data packets in a structure way between GSM mobile stations and external packet data networks. These packets can be directly routed to the packet switched networks from the GPRS mobile stations.
In the current versions of GPRS, networks based on the Internet Protocol (IP) like the global internet or private/corporate intranets and X.25 networks are supported.

Who owns GPRS ?

The GPRS specifications are written by the European Telecommunications Standard Institute (ETSI), the European counterpart of the American National Standard Institute (ANSI).

Key Features

Following three key features describe wireless packet data:
The always online feature - Removes the dial-up process, making applications only one click away.
An upgrade to existing systems - Operators do not have to replace their equipment; rather, GPRS is added on top of the existing infrastructure.
An integral part of future 3G systems - GPRS is the packet data core network for 3G systems EDGE and WCDMA.Goals of GPRS
GPRS is the first step toward an end-to-end wireless infrastructure and has the following goals:Open architecture
Consistent IP services
Same infrastructure for different air interfaces Integrated telephony and Internet infrastructure Leverage industry investment in IP
Service innovation independent of infrastructureBenefits of GPRS

Higher Data Rate

GPRS benefits the users in many ways, one of which is higher data rates in turn of shorter access times. In the typical GSM mobile, setup alone is a lengthy process and equally, rates for data permission are restrained to 9.6 kbit/s. The session establishment time offered while GPRS is in practice is lower than one second and ISDN-line data rates are up to many 10 kbit/s.

Easy Billing:

GPRS packet transmission offers a more user-friendly billing than that offered by circuit switched services. In circuit switched services, billing is based on the duration of the connection. This is unsuitable for applications with bursty traffic. The user must pay for the entire airtime, even for idle periods when no packets are sent (e.g., when the user reads a Web page).
In contrast to this, with packet switched services, billing can be based on the amount of transmitted data. The advantage for the user is that he or she can be "online" over a long period of time but will be billed based on the transmitted data volume.
GPRS has opened a wide range of unique services to the mobile wireless subscriber. Some of the characteristics that have opened a market full of enhanced value services to the users. Below are some of the characteristics:

Mobility - The ability to maintain constant voice and data communications while on the move.

Immediacy - Allows subscribers to obtain connectivity when needed, regardless of location and without a lengthy login session.

Localization - Allows subscribers to obtain information relevant to their current location.

Using the above three characteristics varied possible applications are being developed to offer to the mobile subscribers.

These applications, in general, can be divided into two high-level categories:

1. Corporation
2. Consumer

These two levels further include:

- Communications - E-mail, fax, unified messaging and intranet/internet access, etc.
- Value-added services - Information services and games, etc.
- E-commerce - Retail, ticket purchasing, banking and financial trading, etc.
- Location-based applications - Navigation, traffic conditions, airline/rail schedules and location finder, etc.
- Vertical applications - Freight delivery, fleet management and sales-force automation.

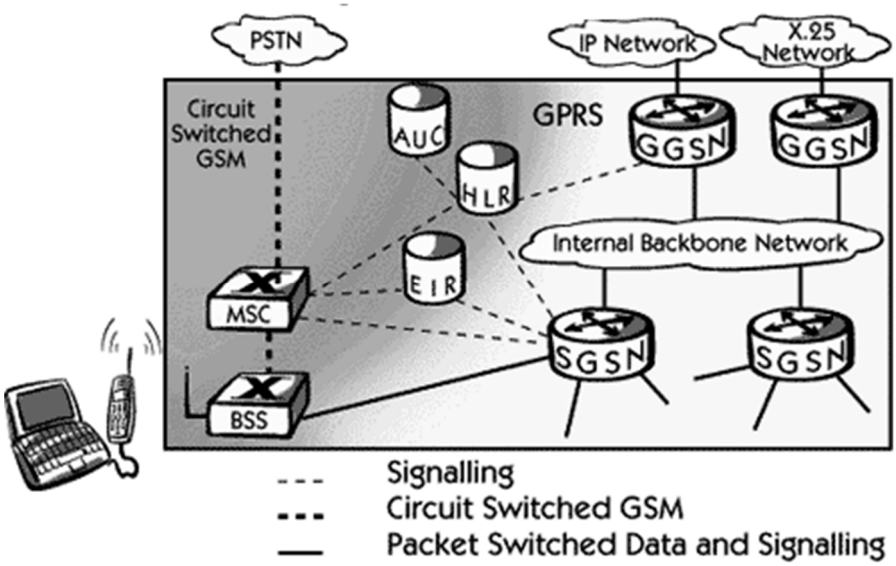
Advertising -: Advertising may be location sensitive. For example, a user entering a mall can receive advertisements specific to the stores in that mall.

Along with the above applications, non-voice services like SMS, MMS and voice calls are also possible with GPRS. Closed User Group (CUG) is a common term used after GPRS is in the market, in addition, it is planned to implement supplementary services, such as Call Forwarding Unconditional (CFU), and Call Forwarding on Mobile subscriber Not Reachable (CFNRc), and closed user group (CUG).

GPRS architecture works on the same procedure like GSM network, but, has additional entities that allow packet data transmission. This data network overlaps a second-generation GSM network providing packet data transport at the rates from

9.6 to 171 kbps. Along with the packet data transport the GSM network accommodates multiple users to share the same air interface resources concurrently.

Following is the GPRS Architecture diagram:



GPRS attempts to reuse the existing GSM network elements as much as possible, but to effectively build a packet-based mobile cellular network, some new network elements, interfaces, and protocols for handling packet traffic are required.Therefore, GPRS requires modifications to numerous GSM network elements as summarized below:

GSM Network Element	Modification or Upgrade Required for GPRS.
Mobile Station (MS)	New Mobile Station is required to access GPRS services. These new terminals will be backward compatible with GSM for voice calls.
BTS	A software upgrade is required in the existing Base Transceiver Station(BTS).
BSC	The Base Station Controller (BSC) requires a software upgrade and the installation of new hardware called the packet control unit (PCU). The PCU directs the data traffic to the GPRS network and can be a separate hardware element associated with the BSC.
GPRS Support Nodes (GSNs)	The deployment of GPRS requires the installation of new core network elements called the serving GPRS support node (SGSN) and gateway GPRS support node (GGSN).
Databases (HLR, VLR, etc.)	All the databases involved in the network will require software upgrades to handle the new call models and functions introduced by GPRS.

GPRS Mobile Stations:

New Mobile Stations (MS) are required to use GPRS services because existing GSM phones do not handle the enhanced air interface or packet data. A variety of MS can exist, including a high-speed version of current phones to support high-speed data access, a new PDA device with an embedded GSM phone, and PC cards for laptop computers. These mobile stations are backward compatible for making voice calls using GSM.

GPRS Base Station Subsystem:

Each BSC requires the installation of one or more Packet Control Units (PCUs) and a software upgrade. The PCU provides a physical and logical data interface to the Base Station Subsystem (BSS) for packet data traffic. The BTS can also require a software upgrade but typically does not require hardware enhancements.

When either voice or data traffic is originated at the subscriber mobile, it is transported over the air interface to the BTS, and from the BTS to the BSC in the same way as a standard GSM call. However, at the output of the BSC, the traffic is separated; voice is sent to the Mobile Switching Center (MSC) per standard GSM, and data is sent to a new device called the SGSN via the PCU over a Frame Relay interface.

GPRS Support Nodes

Following two new components, called Gateway GPRS Support Nodes (GSNs) and, Serving GPRS Support Node (SGSN)are added:

Gateway GPRS Support Node (GGSN):

The Gateway GPRS Support Node acts as an interface and a router to external networks. It contains routing information for GPRS mobiles, which is used to tunnel packets through the IP based internal backbone to the correct Serving GPRS Support Node. The GGSN also collects charging information connected to the use of the external data networks and can act as a packet filter for incoming traffic.

Serving GPRS Support Node (SGSN):

The Serving GPRS Support Node is responsible for authentication of GPRS mobiles, registration of mobiles in the network, mobility management, and collecting information on charging for the use of the air interface.

Internal Backbone:

The internal backbone is an IP based network used to carry packets between different GSNs. Tunnelling is used between SGSNs and GGSNs, so the internal backbone does not need any information about domains outside the GPRS network. Signalling from a GSN to a MSC, HLR or EIR is done using SS7.

Routing Area:

GPRS introduces the concept of a Routing Area. This concept is similar to Location Area in GSM, except thatit generally contains fewer cells. Because routing areas are smaller than location areas, less radio resources are used While broadcasting a page message.

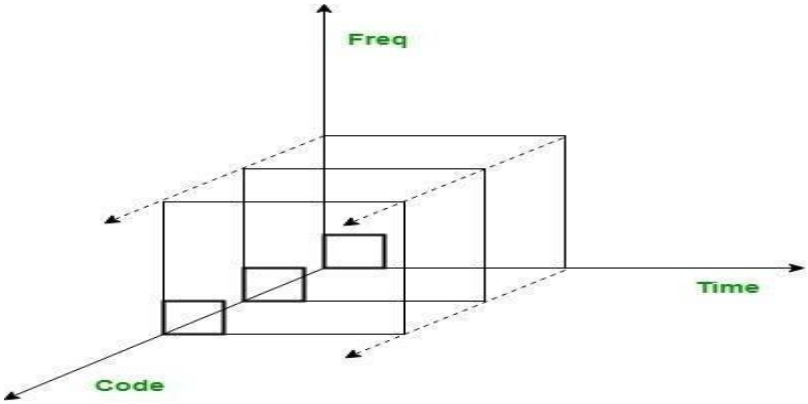
IS-95:

Interim Standard (IS) 95 Last Updated : 08 Aug, 2019

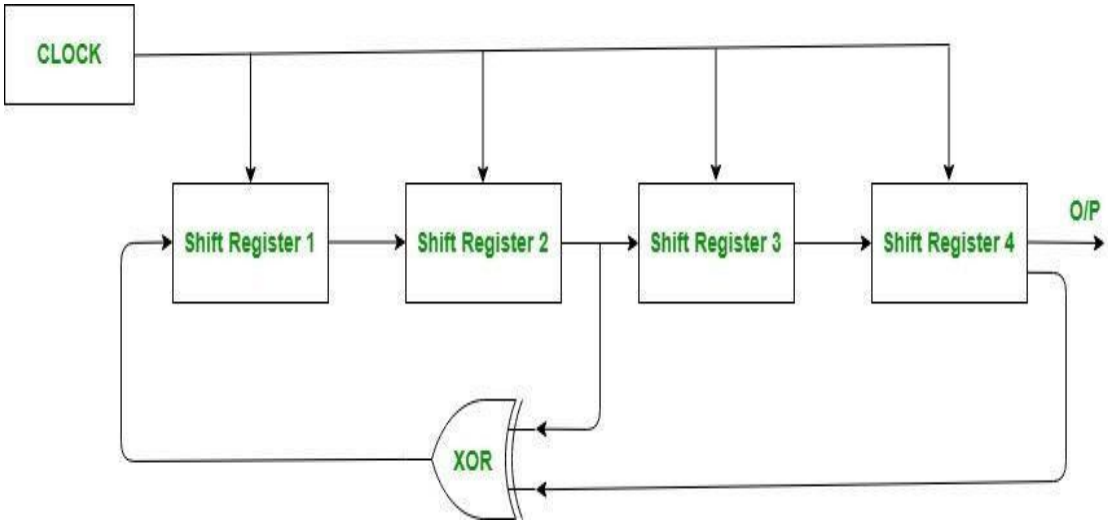
IS-95 stands for Interim Standard 95 and is also known as CDMAOne. It was the first ever CDMA-based digital cellular technology and was developed by Qualcomm. It is an 2G cellular system based on DS-CDMA. To understand IS-95 we need to understand DS and CDMA separately.

DSSS is Direct Sequence Spread Spectrum Technique which is a spread spectrum technique in which the data to be transmitted is encoded using spreading code and received and then decoded using the same code. It is used to avoid interference, spying and jamming. The spreading code used is known to transmitter and receiver only.

CDMA stands for Code Division Multiple Access. It uses the same bandwidth for all the users. However, each user is assigned a separate code which differentiates the from each other.



Narrow bandwidth signals are multiplied with a very large bandwidth signals called Pseudo Noise Code Sequence (PN code). Each user has its own PN code which is orthogonal to each other. Auto-correlation is maximum and cross-correlation is zero of these PN codes. They repeats itself after a very large time period and hence, appears to be random. PN Sequence is generated by Linear Feedback Shift Register.



Power Control in IS-95:

It solves the Near-far problem in which transmitters at different distances transmits signal of same power then the power of the signal of Transmitter (nearer to the base station) will be greater than that of Transmitter (farther to the base station). So in power control technique transmitter nearer to the base station transmits less power signal that of the transmitter farther.

It is of two types:

Open loop power control:

Transmitter senses the power of the received signal at the base station and then adjusts its transmitting power accordingly in subsequent transmissions.

Closed loop power control:

Base station sends the received signal power information to the transmitter and tells to incrementor decrement the transmission power accordingly in subsequent transmissions.

CDMA-2000

CDMA2000 is a code division multiple access (CDMA) version of IMT-2000 specifications developed byInternational Telecommunication Union (ITU).

It includes a group of standards for voice and data services – Voice – CDMA2000 1xRTT, 1X Advanced

Data – CDMA2000 1xEV-DO (Evolution-Data Optimized)

Features

CDMA2000 is a family of technology for 3G mobile cellular communications for transmission of voice, data and signals.

It supports mobile communications at speeds between 144Kbps and 2Mbps.

It has packet core network (PCN) for high speed secured delivery of data packets.

It applies multicarrier modulation techniques to 3G networks. This gives higher data rate, greaterbandwidth and better voice quality. It is also backward compatible with older CDMA versions.

It has multi-mode, multi-band roaming features

W-CDMA

Wideband Code Division Multiple Access (WCDMA) is a third-generation (3G) standard that employs the direct-sequence code division multiple access (DS-CDMA) channel access method and the frequency-division duplexing (FDD) method to provide high-speed and high-capacity service. WCDMA is the most commonly used variant of the Universal Mobile Telecommunications System (UMTS). It was developed by Japan's NTT DoCoMo and formed the basis of its Freedom of Multimedia Access (FOMA) 3G Network.

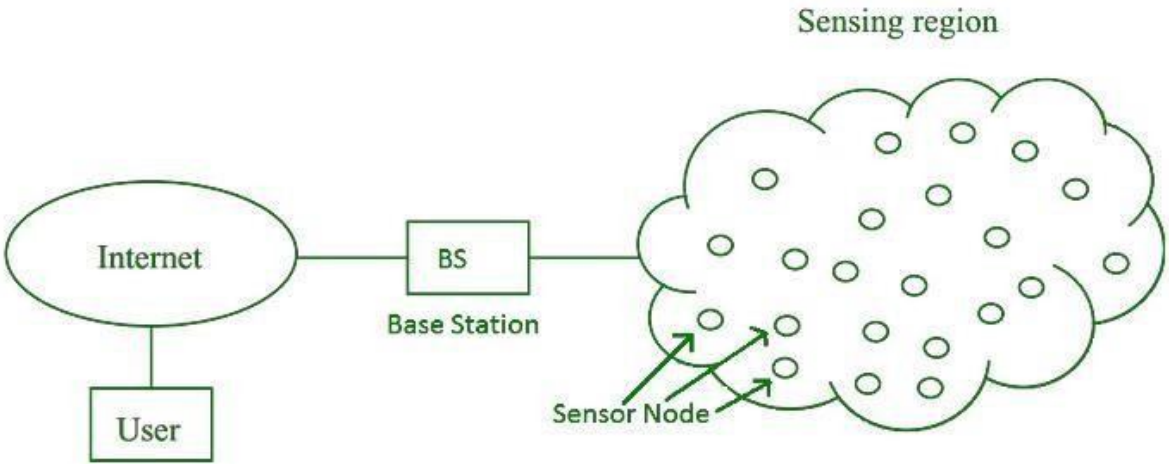
WIRELESS SENSOR NETWORK

Wireless Sensor Network (WSN)Difficulty Level : Basic

Last Updated : 03 Jun, 2021

Wireless Sensor Network (WSN) is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions.

Sensor nodes are used in WSN with the onboard processor that manages and monitors the environment in a particular area. They are connected to the Base Station which acts as a processing unit in the WSN System. Base Station in a WSN System is connected through the Internet to share data.



WSN can be used for processing, analysis, storage, and mining of the data.

Applications of WSN:Internet of Things (IOT)

Surveillance and Monitoring for security, threat detection Environmental temperature, humidity, and air pressure Noise Level of the surrounding
Medical applications like patient monitoringAgriculture
Landslide Detection

Challenges of WSN:

Quality of ServiceSecurity
Issue Energy Efficiency
Network Throughput
Performance
Ability to cope with node failure Cross layer optimisation
Scalability to large scale of deployment

Components of WSN:

Sensors:

Sensors in WSN are used to capture the environmental variables and which is used for data acquisition. Sensor signalsare converted into electrical signals.

Radio Nodes:

It is used to receive the data produced by the Sensors and sends it to the WLAN access point. It consists ofa microcontroller, transceiver, external memory, and power source.

WLAN Access Point:

It receives the data which is sent by the Radio nodes wirelessly, generally through the internet.

Evaluation Software:

The data received by the WLAN Access Point is processed by a software called as Evaluation Software for presenting the report to the users for further processing of the data which can be used for processing, analysis, storage, and mining of the data.

****

CHAPTER-10

MESSAGING SERVICES

SHORT MESSAGE SERVICES

Stands for "Short Message Service." SMS is used to send text messages to mobile phones. The messages can typically be up to 160 characters in length, though some services use 5-bit mode, which supports 224 characters. SMS was originally created for phones that use GSM (Global System for Mobile) communication, but now all the major cell phone systems support it.

While SMS is most commonly used for text messaging between friends or co-workers, it has several other uses as well. For example, subscription SMS services can transmit weather, news, sports updates, and stock quotes to users' phones. SMS can also notify employees of sales inquiries, service stops, and other information pertinent to their business. Doctors can receive SMS messages regarding patient emergencies.

Fortunately, text messages sent via SMS do not require the recipient's phone to be on in order for the message to be successfully transmitted. The SMS service will hold the message until the recipient turns on his or her phone, at which point the message will be be sent to the recipient's phone. Most cell phone companies allow you to send a certain number of text messages every month for no charge. Though it would be a good idea to find out what that number is before you go text message crazy.

MULTIMEDIA MESSAGE SERVICES

- MMS stands for Multimedia Messaging Service. It is the standard way to send messages from one deviceto another through a network.
  As the name Multimedia, we can suggest from here that it is not only for sending text messages, we canalso send multimedia like images, audio clips and video clips, and many more things.
- It is the extension used for SMS(Short Message Service) where we send and receive text messages onlywith the limitation of only 160 characters in one SMS.
  Most of the smartphones support MMS messaging nowadays. Basically it is the advanced version of thetext messaging with the additional feature of multimedia.

Modes of sending MMS

There are basically six modes which are as follows:

- Sending messages to an MMS mobile phone via an MMS mobile phone.
  It can be sent in the same way as we send SMS messages, except that MMS messages include multimediacontents.
- Sending messages to a non-MMS mobile phone via an MMS mobile phone.
  Since the non-MMS mobile phones can't receive a multimedia message, the MMS system automatically forwards the messages to the receiver's corresponding email box and then sends a notification to his mobile phone.
- Sending messages to email boxes via an MMS mobile phone Multimedia messages can be sent via an MMS mobile phone to an email box, and the receiver logs on the email box to read the messages. However, mostemail boxes don't support multimedia messages yet.
- Sending messages to an MMS mobile phone via an email box.
  A user logs on to his email box, selects multimedia messages to sent, inputs a receiver's MMS mobile phone number, and send the messages as an attachment.
- Downloading multimedia messages from the internet to an MMS mobile phone.
  A user can customize and order multimedia messages on websites that provide MMSs and then send MMSto an MMS mobile phone.
- Sending messages from an MMS mobile phone to personal e-albums.
  A user can send MMS messages to his personal e-album via an MMS mobile phone. User writes MMS messages in mobile phones, inputs the album website number, and then sends the messages.

Advantages

- We can easily send and deliver MMS messages.
- The MMS messages which we received, we can store them (save them) and also we can forward messages.
- Users are using these services as they are user-friendly.

These services are interactive.

Image, video, and other media-rich content allows for better branding.Disadvantages

MMS service is not available on all mobile phones. So, we cannot use this service in all the phones.

Some multimedia content has some resolution issues due to the varied display sizes of different phones.

As it a service provided to us but there are also extra charges associated with it. If we have to use this service we have to pay extra charges for this service.

Users who have opted in to an MMS database don't necessarily have an MMS enabled phone. Sending bulk MMS messages is often only available through a dedicated messaging platform rather than a network.

MULTIMEDIA TRANSMISSION OVER NETWORK

Multimedia transmission over wireless networks highlighting general challenges driving the research on wireless technologies and networking techniques for mobile multimedia support. After an overview of wireless networks and multimedia transmission characteristics, a layered analysis is provided ranging from the application to physical protocol layers. This discussion is extended with a cross-layer perspective focusing on cross-layer design. The chapter also introduces a number of emerging wireless/mobile networking concepts including Cognitive Radio Networks (CRNs), ad hoc and multihop networks, and mobile content delivery with a discussion of key issues from multimedia networking perspective. These approaches are envisaged to increase wireless link rates while also improving system capacity, energy efficiency and spectral efficiency dramatically. Finally, we present and discuss major challenges for modeling and simulation of wireless multimedia networking in this diverse and dynamic environment.

****