SYLLABUS

Wireless Network

Sr. No.	Module	Detailed Content
0	Prerequisite	Modulation and Demodulation, Techniques, PSTN.
I	Fundamentals Wireless Communication	Fundamentals of Wireless Communication, Advantages, limitations and application, wireless media, Infrared Modulation Techniques, DSSS and FHSS, Frequency Spectrum : Radio and Infrared; Wireless generations : 1G : Cellular, 2G : Mobile Radio, 3G : UMTS- Security related Encryption Algorithm, 4G.
II	Evolution of Wireless Technologies	Multiple Access Technique : TDMA, FDMA, CSMA, CDMA Wireless Technologies : GSM, GPRS, EDGE, CDMA, LTE, UMTS.
III	Types of Wireless Networks	Ad-hoc : MANET and VANET, Application, Advantage and limitations; Wireless Sensor Network : Application, advantages and limitations.
IV	Emerging Wireless Technologies and standards	WLL, WLAN- 802.11 (Wi-Fi), WPAN- 802.15.1/3/4 (Bluetooth, Zigbee), WMAN-802.16a (Wimax), Wi-max and LTE /3GPP comparison, Mi-fi, Ly-fi.
V	Wireless Network Design Considerations	Wireless technology, Cisco Unified Wireless Network, Designing Wireless Networks with Lightweight Access Points and Wireless LAN Controllers.
VI	Wireless Network Security	The need, attacks, security serviced, WEP, Mobile IP, VPN (PPTP, LLTP, IPSec), Network Layer Security, Transport Layer Security, Email Security : PGP, S/ MIME, Internet Firewalls for Trusted System.

□□□

Scanned by CamScanner

Wireless Network

Chapter 1 : Fundamentals of Wireless Communication

Q. 1 How call is initiated in cellular system ? **Dec. 12**

Ans. :

Call initiated by telephone user

When a telephone user does a call to a mobile user the mobile switching centre (MSC) dispatches the request to all the base stations in the system. The subscriber's telephone number i.e. **mobile identification number** (MIN) is broadcast as a paging message on all the forward control channels of the cellular system.

Then the mobile receives the paging message sent by the base station that it observes and responds by identifying itself over the reverse control channel. The base station receives the acknowledgement sent by mobile and inform the MSC about the handshake. Then the MSC instructs the base station to move the call on to an unused voice channel within the cell.

The base station signals the frequencies to modify to unused forward and reverse voice channels. Also a **alert** (data message) is sent on the forward voice channel to tell the mobile telephone to ring and the other user to answer the ring. All these events occur very fast and are not noticeable by the subscriber.

When the call progresses the mobile switching center (MSC) adjusts the power transmitted (P_t) of the mobile unit and the base stations so as to maintain the call quality even though the mobile unit is non-stationary. The call in progress continues irrespective of the frequency changes from one base station to another base station. Such a call continued process without termination is called as **"hand-off"**.

As the mobile moves and the signal strength reduces when it is away from its base station of the cell, the next base station of the neighbouring cell where the mobile enters in will take charge of the call. A relay like process thus takes place within several base stations of the complete cellular system to maintain the call developed between two subscribers.

Call initiated by a mobile user

Whenever a mobile originates a call to a telephone user a request signal is sent on the reverse control channel. By seeing this request the mobile unit will transmit its, **Mobile Identification Number (MIN), Electronic Serial Number (ESN)** and the telephone number of the called party. The mobile unit also transmits a **SCM (Station Class Mark)** that indicates the maximum transmitter power level for a user.

The base station receives this information and sends it to the mobile switching center (MSC). Then the MSC will check the proper validity of the signals sent by the mobile and responds to its request by connecting the called subscriber through PSTN. It instructs the base station and mobile user to move to an unused forward and reverse voice channel pair to allow conversation to begin.

All cellular systems provide a facility called **Roaming**. It allows the users to operate in service areas other than that from which the service is subscribed. When a mobile enters other city or area it is registered as a **roamer** in that service area. The mobile communication establishes call, maintains it and terminates as the call is over. It enables communication even though the distance between the subscriber is large.

Q. 2 List the advantages of wireless technology. **Dec. 13**

Ans. :

Advantages of Wireless Communications

(i) **Mobility :** The primary advantage of wireless communication is to offer the user freedom to move about connected with the network. Wireless technology enables the industries to shift towards an increasing mobile workforce whether they are in meetings or working on a factory floor or conducting research.

(ii) **Increased reliability :** The most common source of network problems is failure or damage of network cables because of environmental conditions or erosion of metallic conductors using wireless technology not only eliminates these types of cable failures, but also increases the reliability of the network.

(iii) **Easy installation :** They can be easily installed without worrying about providing network connectivity through cables.

(iv) **Lower cost :** The need to install cables is eliminated using wireless communication and results in significant cost savings.

(v) **Rapid disaster recovery :** Accidents can happen because of earthquakes, fire, floods at any location and at any time. Any organization that is not prepared to recover from such natural disasters can find itself quickly out of business. As a computer network is a routine part of business, the network can be easily set up after disaster. However a documented disaster recovery is essential.

Scanned by CamScanner

Q. 3 List the disadvantages of wireless technology. **Dec. 16**

Ans. :

Disadvantages/Limitations of Wireless Communications

(i) **Radio signal interference :** Signals from other wireless devices can disrupt its radio transmission or a wireless device can itself be a source of interference for other wireless devices. e.g. Commonly used wireless devices like cordless phones, elevator motors, microwave ovens etc. transmit radio signals that can interface with wireless LAN operation. They can cause errors. Also Bluetooth and WLAN devices both operate in the same radio frequency, potentially resulting interference between these devices.

(ii) **Security :** A wireless communication device transmits radio signals over a wide open area, Hence, security is a major concern. It is possible for an intruder with a notebook computer and wireless N/C to intercept the signals from a nearby wireless network. Because of more of business, network traffic can contain sensitive information, it becomes a serious issue for many users.

Some wireless technologies can provide added levels of security with authorization features earlier to gaining access to the network. Network administrators can limit access for approved wireless devices only.

(iii) **Health hazards :** Biological damage can be produced as a result of High power levels of RF energy.

However, we do not know as to how much levels of RF energy can lead to adverse health effects. The continuous radiations at lower levels can be harmful to sensitive body organs. The RF energy is emitted by radio transmitters in the wireless communication systems. Typically these systems emit low levels of RF as they are used. Although research is carried to solve these problems there is no clear information about the biological effects of this type of radiations.

Q. 4 Write note on : Wireless applications. **Dec. 13**

Ans. :

Wireless Communication Applications

The wireless communication systems are used for following applications :

(1) Paging and messaging (2) Cordless Telephone Systems
(3) Wireless local loop (4) Wireless PAN
(5) Wireless LAN (6) Cellular phones
(7) Security systems (8) Television remote control
(9) Wi-Fi (10) Wireless keyboards
(11) Remote access to medical records.
(12) Bluetooth

Q. 5 With a neat diagram explain electromagnetic spectrum. **Dec. 16, Dec. 17**

Ans. :

EM Spectrum and Communication Applications

In the radio communication system the frequencies ranging from a few kilohertz to many gigahertz all are being used for various purposes. Let us see the applications of various frequency bands. The frequencies most commonly used in early days were from about 300 kHz to 3 MHz and were called as **medium frequencies (MF)**. The frequencies in the range 30 kHz to 300 kHz are known as the **low frequencies (LF)**.

The frequencies in the range 3 kHz to 30 kHz are called as **very low frequencies (VLF)**. On the higher frequency side **high frequencies (HF)** will cover the frequency range from 3 MHz to 30 MHz. Then **very high frequency (VHF)** from 30 MHz to 300 MHz and so on. Table 1.1 gives you the details of entire usable frequency spectrum and its applications.

Table 1.1 : The Radio Frequency Spectrum

Sr. No.	Frequency band	Wavelength	Applications
1.	30 Hz - 300 Hz. Extremely low frequencies ELF.	10^4 km to 10^3 km	Power transmission
2.	300 Hz - 3 kHz. Voice frequencies (VF)	10^3 km to 100 km	Audio applications
3.	3 kHz - 30 kHz. Very low frequencies (VLF)	100 km to 10 km	Submarine communications. Navy, Military communications
4.	30 kHz - 300 kHz. Low frequencies (LF)	10 km to 1 km. Long waves.	Aeronautical and marine, navigation, these frequencies act as sub carriers.
5.	300 kHz - 30 MHz Medium frequencies (MF)	1 km to 100 m. Medium waves.	AM radio broadcast, Marine and aeronautical communications.
6.	3 MHz - 30 MHz High frequencies (HF)	100 m to 10 m Short waves.	Shortwave transmission, Amateur and CB communication.

Scanned by CamScanner

Sr. No.	Frequency band	Wavelength	Applications
7.	30 MHz - 300 MHz Very high frequencies (VHF)	10 m to 1 m	TV broadcasting, FM broadcasting.
8.	300 MHz - 3 GHz Ultra high frequencies (UHF)	1 m to 10 cm. Microwaves.	UHF TV channels, Cellular phones, Military applications
9.	3 GHz - 30 GHz (SHF)	10^{-1} m to 10^{-2} m	Satellite communication and Radar
10.	30 - 300 GHz (EHF)	10^{-2} m to 10^{-3} m	Satellites and specialized radars.

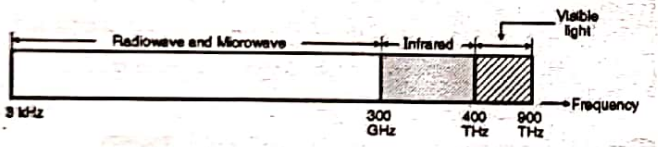
1. Infrared Signals

The EM signals having frequencies above 300 GHz are not referred as radio waves. The signal occupying the range between 0.1 mm and 700 nanometers (nm) are called infrared signals. These are used in various special kinds of communications as listed below.

1. In astronomy to detect stars and other heavenly bodies.
2. For guidance in weapon systems.
3. TV remote control.

2. Unguided Media : Wireless

The electromagnetic spectrum used for wireless communication is shown in Fig. 1.1.



(L-597)**Fig. 1.1 : Electromagnetic spectrum for the wireless communication**

Propagation methods

The unguided signals can travel from the transmitter to receiver in many different ways.

The three most important methods are :

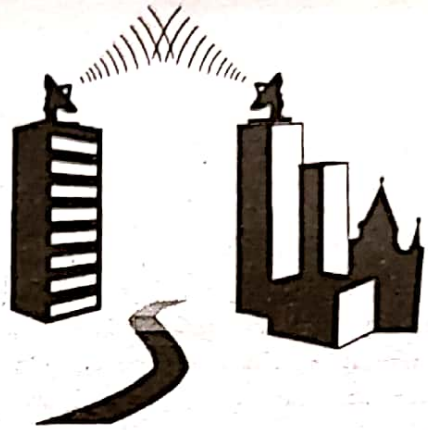
1. Ground wave propagation
2. Sky propagation.
3. Space propagation or line of sight propagation.

Q. 6 Explain terrestrial microwave systems and give its characteristics.

Ans. :

Terrestrial microwave systems

These systems use directional parabolic antennas to transmit and receive signals in the lower gigahertz range as shown in Fig. 1.2. The signals are highly focussed and the physical path must be line of sight. Relay towers are used to extend signals. Smaller terrestrial microwave systems can be used within a building. Microwave LANs operate at low power using small transmitters that communicate with omni-directional hubs. Hubs can then be connected to form an entire network.



(L-600)**Fig. 1.2 : Terrestrial microwave system**

Characteristics of Terrestrial Microwave Systems

1. The frequency range used is from 4-6 GHz and 21 to 23 GHz.
2. It supports a bandwidth from 1 to 10 mbps.
3. Attenuation is affected by frequency, signal strength, antenna size and atmospheric conditions.
4. The signals are affected by EMI effect, jamming and eavesdropping.
5. Line of sight requirements make installation difficult.
6. Short distance systems can be inexpensive but long distance systems are relatively expensive.

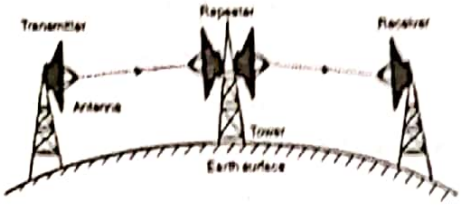
Q. 7 Explain RF Link (Microwave Link).

Ans. :

RF Link (Microwave Link)

Long form of RF link is radio frequency link. This is actually a type of point to point wireless communication. The radio frequencies used for RF links are in microwave range therefore, RF links are also called as microwave links. This is shown in Fig. 1.3.

Scanned by CamScanner



(L-601)Fig. 1.3 : Microwave link

Although many wire communication systems use copper wires or optical fiber, some just send the signal into the air. This happens when infrared, lasers, microwaves and radio are used for the transmission of data, as they do not need any physical medium.

For long distance communication, microwave radio transmission is widely used as an alternative to co-axial cable. The signal transmission takes place in the form of electromagnetic waves which have wavelengths of few centimetres. Parabolic antennas can be mounted on the towers to send a beam of waves to another antenna, tens of kilometres away.

The transmitting and receiving antennas are highly directional to enable a point to point communication. This system is widely used for both telephone and television transmission. The higher the tower which holds the antenna, the greater is the range. With a 100 metre high tower, the distances of 100 km can be easily covered.

Q. 8 Give advantages, disadvantages and applications of RF Link (Microwave Link).

Ans. :

Advantages of microwave link

1. Installation of towers and associated equipments is cheaper than laying down a cable of 100 km length.
2. Less maintenance as compared to cables.
3. Repeaters can be used. So effect of noise is reduced.
4. No adverse effects such as cable breakage etc.
5. Due to the use of highly directional antenna, these links do not make any interference with other communication systems.
6. Size of transmitter and receiver reduces due to the use of high frequency.

Disadvantages of microwave link

1. Signal strength at the receiving antenna reduces due to multipath reception.
2. The transmission will be affected by the thunderstorms, and other atmospheric phenomenons.

Applications of Microwave transmission

1. One-to-one communication
2. In cellular phones
3. In satellite networks
4. In the wireless LANs

Q. 9 Give comparison of Point to Point and Broadcast Infrared System.

Ans. :

Comparison of Point to Point and Broadcast Infrared System

Sr. No.	Factor	Point to Point	Broadcast
1.	Frequency range	100 GHz to 1000 terahertz	100 GHz to 1000 terahertz
2.	Bandwidth capacity	Data rates between 100 kbps to 16 mbps	Data rates less than 1 mbps
3.	Node capacity	2 (source to destination)	More than one
4.	Attenuation	Depends on quality of emitted light, its purity, atmospheric conditions and signal obstructions	Depends on quality of emitted light, its purity atmospheric conditions
5.	EMI	Affected by intense light	Affected by intense light
6.	Installation	Requires precise alignment	Fairly simple
7.	Cost	Moderately high if laser is used	High if laser is used.

Q. 10 Write note on concept of spread spectrum. **Dec.-10**

Ans. :

Spread Spectrum (DS/SS and FH/SS)

The increasing demand of wireless communications have faced problems because of limited spectrum capacity and multipath propagation. These problems can be minimized by spread spectrum communications.

Scanned by CamScanner

Features of Spread Spectrum Communication

Some of the features of spread spectrum communication are :

(i) Capability of Multiple access

(ii) Resistant to jamming

(iii) Higher channel capacity

(iv) It has the ability to resist multipath propagation

(v) Because of multipath propagation. It provides immunity to distortion

(vi) It cannot be intercepted by any unauthorized person.

Spread Spectrum Conditions

The conditions of spread spectrum communication are :

(i) It is a type of modulation where the modulated signal BW is larger than the baseband signal.

(ii) A pseudo noise (p–n) code is used for the spectrum spreading. The p–n code can also be used to despread the signal at the receiver.

Processing Gain

The processing gain is defined as the factor by which the bandwidth of the message signal is increased.

$$\text{Processing gain } N = \frac{B_{ss}}{B}$$

B : Message signal bandwidth

B_{ss} : Spread spectrum signal bandwidth

Spread Spectrum Model

Fig. 1.4 shows the general model of a spread spectrum digital communication system.

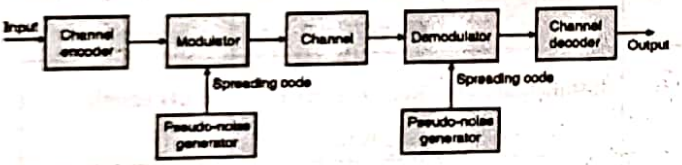


Fig. 1.4 : Spread Spectrum Model

The input is given to a channel encoder that produces the analog signal with narrow bandwidth at the centre frequency. Then the signal is modulated by a spreading code or sequence. The spreading code is generated by pseudo noise or pseudo random number generator. Modulation increases the bandwidth of the signal to be transmitted. At the receiver end the digit sequence is used to demodulate the spread spectrum signal. The signal is sent to the decoder to recover the data.

Advantages of Spread Spectrum Communication

(i) There is no interference with other signals.

(ii) Spread system can be operated at the same frequency at which the current narrow band systems are working.

(iii) As signal is spread over wide bandwidth, interception and jamming of signal will be difficult.

Q. 11 Explain DSSS with suitable example.

Dec. 11, May 12, Dec. 12, May 13, Dec. 13, Dec. 14, Dec. 15, May 16, Dec. 16

Ans. :

Direct Sequence Spread Spectrum (DS / SS)

The signal spreading code is called as pseudo noise (PN) sequence in the spread spectrum communication systems.

The DS/SS signal can be expressed as,

$$y(t) = m(t) \cdot c(t)$$

where, m(t) : Message signal

c(t) : Pseudo random binary sequence.

Fig. 1.5 shows the DS/SS signal generator

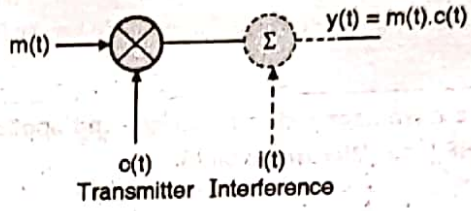


Fig. 1.5 : DS / SS generator

The bit rate of c(t) is higher than that of m(t). The pulse in c(t) is called as chip and bit rate of c(t) is called chip rate (R_C).

$$\text{Chip rate } R_C = \frac{1}{T_C}$$

where, T_C : Chip width

The auto correlation function ψ_c of c(t) is narrow. Fig. 1.6 shows SS generator signals.

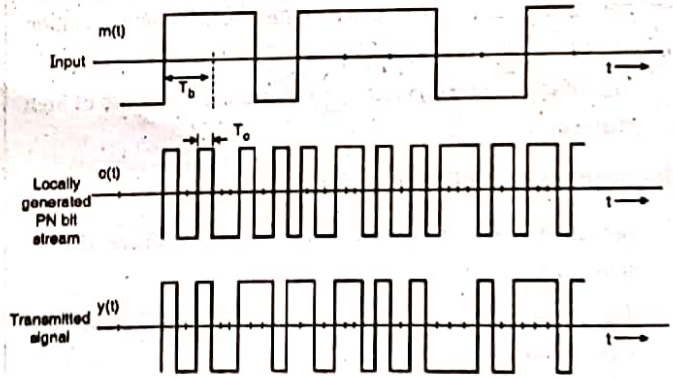


Fig. 1.6 : SS generator signals

For detection, a synchronous random sequence c(t) is used at the receiver end.

Scanned by CamScanner

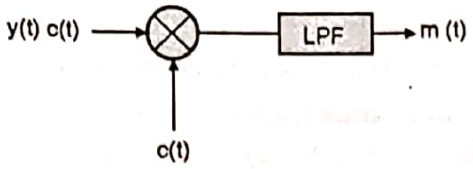


Fig. 1.7 : DSISS receiver

The received signal y(t) is multiplied by c(t) to recover the desired signal m(t).

$$y(t) \cdot c(t) = m(t) \cdot c^2(t)$$
$$= m(t) \quad \because c^2(t) = 1$$

As shown in Fig. 1.7 the LPF is an integrator. The receiver does the correlation of the incoming signal m(t) · c(t) and c(t) is generated.

The **Chip rate** = R_C bits/sec. and

Symbol rate = R_b bits/sec.

Processing gain $N = \frac{R_C}{R_b}$

Or $N = \frac{T_b}{T_c}$

T_c = **chip width**

The power spectral density (PSD) is :

$$S_m(\omega) = T_b \sin c^2\left(\frac{\omega T_b}{2}\right) \quad \text{for input signal A}$$

$$S_y(\omega) = T_c \sin c^2\left(\frac{\omega T_c}{2}\right) \quad \text{for output signal B}$$

Fig. 1.8 shows the power spectral density of input signal m(t) and output signal of DS/SS y(t). The bandwidth of PSD is directly proportional to the bit rate. Hence PSD of y(t) is N times wider than the PSD of m(t). The spreading process decreases the PSD of the signal by a factor N.

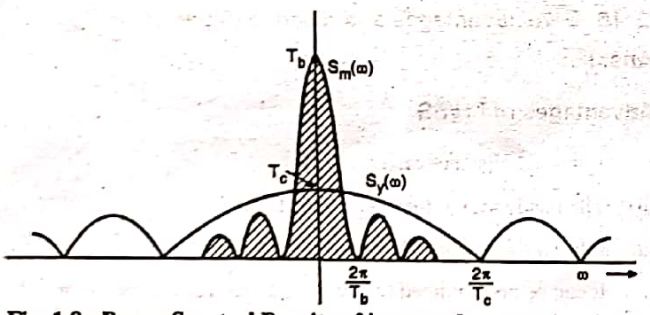
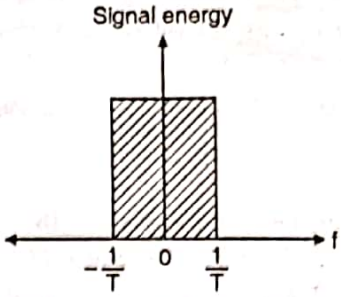


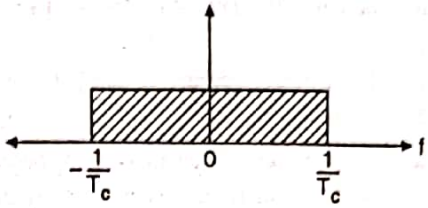
Fig. 1.8 : Power Spectral Density of input and output signals of DSISS system

DS/SS Signal Pattern

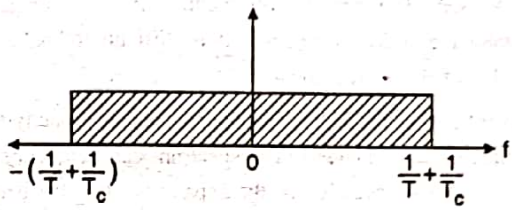
The width of the information signal is T. Hence, the data rate is $\frac{1}{T}$. The spectrum of the signal depends on the method of encoding and is around $\frac{1}{2T}$. Fig. 1.9 shows the spectrum of DS/SS. The spectrum of PN signal is $\frac{2}{T_c}$. The resulting spectrum spreading of DS/SS is shown in Fig. 1.9.



(a) Spectrum of the data signal



(b) Spectrum of pseudo-noise signal



(c) Spectrum of the combined signal

Fig. 1.9 : Spectrum of DSISS

Examples of DS/SS

(i) IEEE 802.11b standard for wireless LAN uses DS/SS over 2.4 GHz free spectrum.

(ii) IEEE 802.15.4 WPAN (Zigbee) uses DS/SS.

(iii) CDMA

(iv) Cordless phones operating in 900 MHz, 2.4 GHz and 5.8 GHz bands.

(v) Radio controlled model automotive vehicles.

(vi) Wifi.

Q. 12 What are the characteristics of DS/SS?

Ans. :

Characteristics of DS/SS

(i) **Secure communication :** If pseudo random code is used then the signal can be detected at the receiver end. It avoids unauthorized signal access.

Scanned by CamScanner

(ii) **Jamming resistance :** The DS/SS spectrum power is distributed over a wideband. Hence, these signals are difficult to jam. The PSD of jamming signal decrease by a factor N because of the spectrum spreading.

(iii) **Hiding of signal :** The DS/SS signal spectrum is spread over a wide band. The PSD is small. Hence, it is simple to hide the signal within the noise floor.

(iv) **Multiple access :** Many users can use the same band with a better
signal-to-noise ratio.

(v) **Resistance to multipath fading :** The signal received because of reflection is delayed version of DS/SS signal. The DS/SS has a low auto correlation with its delayed version. This minimizes the effect of multipath signals.

(vi) **Near-far problem :** The DS/SS is affected by the near-far problem.
Near-far problem occurs because of unequal power that is received by the user.

When an unwanted signal strength is more because of its proximity to its transmitter, the desired signal strength at the receiver is weak. In such cases the desired signal can be suppressed. The near far problem can be eliminated by making the codes orthogonal. It is difficult to make large number of codes orthogonal.

(vii) **Advantages of CDMA :** It supports a higher capacity of the communication channels. The spectrum can be occupied by many users irrespective of the separation distance between them. Each user has unique spreading codes. The unique spreading codes support code division multiple access (CDMA).

Q. 13 Give advantages, disadvantages of DS/SS.

Ans. :

Advantages of DS/SS

(i) It has best discrimination against multipath signals.

(ii) It has best noise and anti-jam performance.

(iii) The unidentified receivers find it difficult to detect the direct sequence signals.

Disadvantages of DS/SS

(i) DS/SS has a longer acquisition time.

(ii) It requires wideband channel with small phase distortion.

(iii) The pseudo noise generator must generate sequence at high rates.

Q. 14 Explain FHSS and DSSS with suitable example.

Dec. 11, May 12, Dec. 12, May 13, Dec. 13, Dec.14, Dec. 15, May 16, Dec. 16

Ans. :

Frequency Hopping Spread Spectrum (FH/SS)

Fig. 1.10 shows the FH/SS system. In this method an FSK signal is generated. Then the frequency of FSK signal is shifted by pseudo-noise (PN) sequence. The FSK output frequency is ω_l and synthesizer frequency is ω_h. The output of mixer contains $(\omega_h + \omega_l)$ and $(\omega_h - \omega_l)$. The BPF (band pass filter) passes $(\omega_h + \omega_l)$ frequency components.

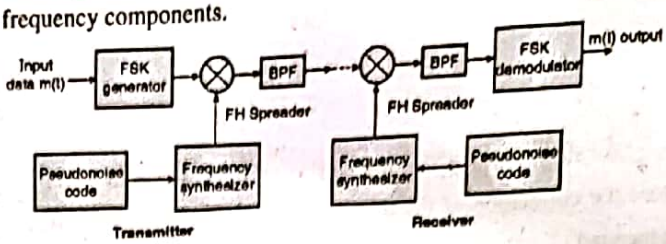


Fig. 1.10 : FH/SS system

The signal is transmitted by pulses whose frequencies hop over a wide range of frequencies according to the PN code. The bandwidth of the FH/SS signal is more than that of the FSK signal. The FH/SS receiver is identical to the PN code. The received signal shifts the frequencies back to original FSK frequencies. The frequencies can be demodulated.

There are two conditions depending on the frequency hopping rate R_h and symbol rate R_b.

(i) When $R_h \le R_b$ it is called **show frequency hopping (SFH).**

(ii) When $R_h > R_b$ it is called **fast frequency hopping (FFH).**

Examples of FH/SS

(i) Bluetooth uses FHSS over unlicensed ISM band at 2.4 – 2.4835 GHz

(ii) GSM

(iii) It is used in military

(iv) Walkie-talkies in 900 MHz unlicensed band.

Q. 15 Give advantages and disadvantages of FH/SS.

Ans. :

Advantages of FH/SS

(i) It has less distance effect.

(ii) The bandwidth of these system is large.

(iii) It has a short acquisition time.

(iv) It can be programmed to avoid some parts of the spectrum.

Disadvantages of FH/SS

(i) It needs error correction

(ii) It needs complex frequency synthesizers.

(iii) It is not useful for range and range rate measurement.

Scanned by CamScanner

Q. 16 Give advantages of FH/SS over DS/SS.

Ans. :

Advantages of FH/SS over DS/SS

(i) FH/SS is less susceptible to the near-far problems than DS/SS.

(ii) FH/SS can produce signals of wider bandwidth as compared to DS/SS.

(iii) The processing gain is higher than that of DS/SS.

(iv) In FH/SS the problems of relative power levels of co-channel signal are not critical as compared to DS/SS.

Q. 17 Compare frequency Hopping SS vs DSSS.

May 11

Ans. :

Comparison of DS/SS and FH/SS

Sr. No.	Parameter	DS/SS	FH/SS
1.	**Definition**	In DS/SS the pseudo noise sequence of large bandwidth is multiplied with narrow band data signal.	In FH/SS the data bits that are transmitted in the different frequency slots are changed by the PN sequence.
2.	**Signal spectrum**	Over the complete bandwidth of the spread spectrum signal the data sequence is spread.	In FH/SS the data sequence is spread over small frequency slots of the spread spectrum signal.
3.	**Modulation method**	BPSK	Mary FSK
4.	**Processing gain**	$PG = \frac{T_b}{T_c} = N$	$PG = 2^t$ where t = bits in the pseudo noise (PN) sequence.
5.	**Distance effect**	DS/SS is relative to distance.	FH/SS is less affected by distance change.
6.	**Acquisition time**	The acquisition time of DS/SS is long.	The acquisition time of FH/SS is short.
7.	**Cost**	High cost	Low cost
8.	**Power consumption**	High	Low
9.	**Data rates**	High data rates	Low data rates
10.	**Range**	More	Less
11.	**Capacity**	Low overall capacity	More overall capacity
12.	**Example**	IEEE 802.11 b	Bluetooth

Q. 18 Compare 1G, 2G, 2.5G, 3G, 4G and 5G.

Ans. :

Comparison Between 1G, 2G, 2.5G, 3G, 4G and 5G

Parameter	1G	2G	2.5G	3G	4G	5G
Year of introduction	1980s	1993	1997	2001	2009	2014
Location of first commercialization	USA	Finland	Finland	Japan	South Korea	To be implemented
Technology	AMPS, TACs, NMT, NIT, ETACS	IS – 95, GSM	GPRS, EDGE, HSCSD	IMT 2000, WCDMA, TD-SCDMA	LTE, WIMAX Wi-Fi	www unified IP seamless combination of LAN, PAN, MAN, WLAN

Scanned by CamScanner

Parameter	1G	2G	2.5G	3G	4G	5G
Type of switching	Circuit switching	Circuit switching for voice and packet switching for data	Packet switching/Circuit switching	Packet switching	Packet switching	Packet switching
Multiple Access	FDMA	TDMA, CDMA	TDMA, CDMA	CDMA	CDMA	CDMA
Data Rates	2.4 Kbps - 14..4 Kbps	14.4 Kbps	20 – 40 Kbps 171.2 Kbps (max) for GPRS	3.1 Mbps	100 Mbps	> 1 Gbps
Core Networks	PSTN	PSTN	PSTN	Internet	Internet	Internet
Supports	Voice only	Data and voice	Data and voice, SMS, MMS	Data and voice	Data and voice	Data and voice
Internet	No internet	Narrowband	Narrowband	Broadband	Ultra Broadband	Massive broadband
Operating frequencies	800 MHz	GSM 900 MHz 1800 MHz CDMA 800 MHz	GPRS	2100 MHz	850 MHz, 1800 MHz	LTE Frequency range 600MHz-6GHz and millimetre bands (24-86 GHz)
Band Narrowband	Narrowband	Narrowband	Narrowband	Wideband	Ultra wide band	Low power wide area technology (LPWA) for Internet of Things (IOT)
Carrier frequency	30 kHz	200 kHz	200 kHz	5 MHz	15 MHz	15GHz
Bandwidth	Analog	25 MHz	25 MHz	25 MHz	100 MHz	1Gbps
Handoff	Horizontal	Horizontal	Horizontal	Horizontal and Vertical	Horizontal and Vertical	Horizontal and Vertical
Advantages	Network Elements are simple	SIM and internet started	Supports SMS and MMS	High security international roaming	High speed, Bandwidth, Global mobility, MIMO technology	High resolution, bidirectional large bandwidth, More efficient and effective
Disadvantages	(i) Limited capacity (ii) Susceptible to noise (iii Frequent call drops (iv)Poor battery life (v) Poor handoff	(i) Slow data rates (ii) Low network range	(i) Low network range	(i) High power consumption (ii) High cost of spectrum license (iii) Low network coverage	(i) Difficult to implement and needs complex hardware	Security and privacy issues need to be resolved, Developing infrastructure will require more cost
Applications	Voice calls	Voice calls, SMS	Voice calls, SMS, MMS, VPN	Mobile TV, GPS, videoconferencing	Mobile TV, GPS, High speed Applications.	Mobile, TV, GPS, High speed applications

Scanned by CamScanner

Chapter 2 : Multiple Access Techniques

Q. 1 Explain the Wireless Multiple Access Techniques with suitable diagrams. **Dec. 16, Dec. 17**

Ans. :

Multiple Access

The transmission bandwidth in different frequency band varies in range. It is more than the bandwidth needed for a message to be transmitted. Hence, in order to utilize the frequency spectrum efficiency "**Multiple access**" methods are introduced.

Cellular systems consists of many users that will share the bandwidth. The ability of the system to carry many signals at the same time is called as "multiple access".

Through "multiple access" it is possible to share the communication capacity of the cellular system among a large number of base stations.

Fig. 2.1 shows the block diagram of a multiple access system.

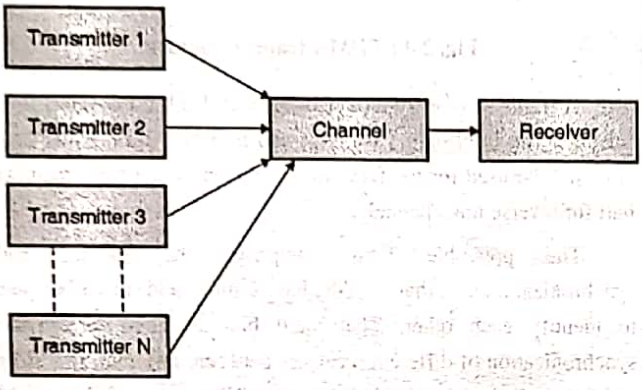


Fig. 2.1 : Block diagram of a multiple access system

Types of Multiple Access Techniques

The three main multiple access methods used to share the bandwidth in a wireless communication system are :

i) Frequency division multiple access (FDMA)

ii) Time division multiple access (TDMA)

iii) Code division multiple access (CDMA)

In **Frequency Division Multiple Access (FDMA)**, individual channels are assigned to individual users and each user is allocated a unique frequency band or channel.

The **Time Division Multiple Access (TDMA)** systems divide the radio spectrum into time slots and in one slot only one user is allowed to transmit or receive.

In **Code Division Multiple Access (CDMA)** systems, the narrowband message signal is multiplied by a large bandwidth called spreading signal. This spreading signal is actually a pseudo noise code sequence and it has a higher chip rate than the data rate of the message signal.

Q. 2 Explain in detail FDMA. **Dec. 12, Dec. 15**

Ans. :

Frequency Division Multiple Access (FDMA)

In wireless communication systems, the individual users are allocated individual channels. The channels or the frequency band is unique for each subscriber. The entire allowed radio spectrum is divided into many slices of the frequency bands and each band or channel is allocated to user. The channel allocation can be done on a demand basis to the users to request service.

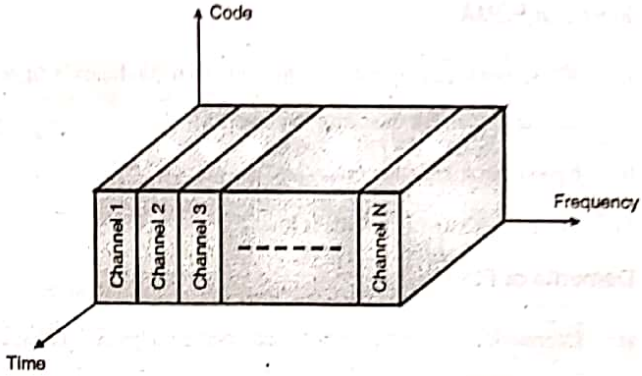


Fig. 2.2 : FDMA where different channels are assigned different frequency bands

When a call is processed, no other user can share the same channel. In FDMA/FDD systems the users are assigned a pair of frequencies, one for the forward channel and other for the reverse channel. Fig. 2.2 shows the principle of FDMA scheme where different channels are assigned different frequency bands.

Features of FDMA

The features of FDMA are :

i) If a FDMA channel is not in use, it will be idle and not used by any other user. Hence, there is a chance of resource wastage.

ii) The FDMA channel uses one phone circuit at any instant of time.

iii) If voice channel is assigned in FDMA, then the mobile unit and the base station start transmitting simultaneously.

iv) FDMA needs tight RF filtering to minimize the adjacent channel interference.

v) The FDMA mobile unit uses duplexers as both the transmitter and receiver operate simultaneously. It results an increase in the cost of subscriber units and base stations.

vi) The complexity of FDMA systems is less.

Scanned by CamScanner

vii) The FDMA systems have narrow bandwidth as each channel supports only one circuit per carrier.

viii) The symbol time is large in comparison to the delay spread. This indicates that the intersymbol interference is low and no equalization is required in FDMA narrowband systems.

ix) The cost of cell site is higher in comparison to the TDMA systems.

x) FDMA is a continuous transmission method. So few bits are required for overhead purposes (like synchronization and framing bits).

Merits of FDMA

i) All stations can operate continuously all 24 hours without having to wait for their turn to come.

ii) No synchronization is necessary.

iii) The complexity of systems is low.

Demerits of FDMA

i) Intermodulation frequencies can cause adjacent channel interference.

ii) As a result of non-linearities, intermodulation products are generated.

iii) It carries only one phone circuit at a time.

iv) The cell site cost of FDMA systems is high.

v) The bandwidth of FDMA channels is narrow.

Q. 3 Explain in detail TDMA. **Dec. 12, Dec. 15**

Ans. :

Time Division Multiple Access

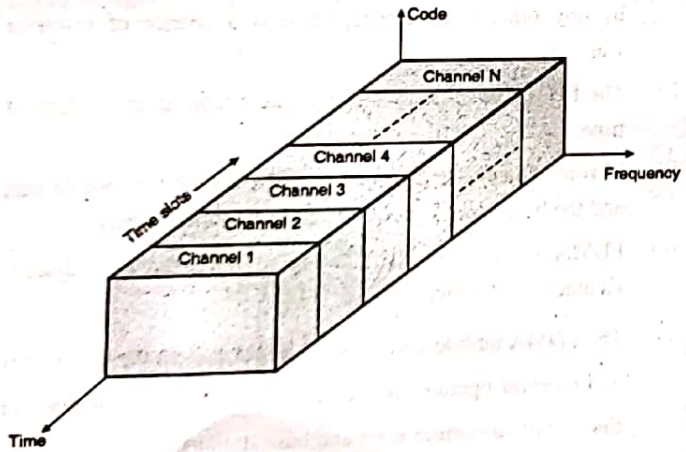


Fig. 2.3 : TDMA

It uses time instead of frequency. Different users share the same time slots of the complete time available. Each user to allocated a time slot in which the user can access the channel. In each slot only one user is allowed to transmit or receive.

As shown in Fig. 2.3 each user is assigned a time slot so that channel may be thought as a time slot that reoccurs every frame where N slots comprise a frame. The TDMA systems transmit data in **burst and buffer** method. The transmission from different users in interfaced into a repeating frame structure as shown in Fig. 2.4.

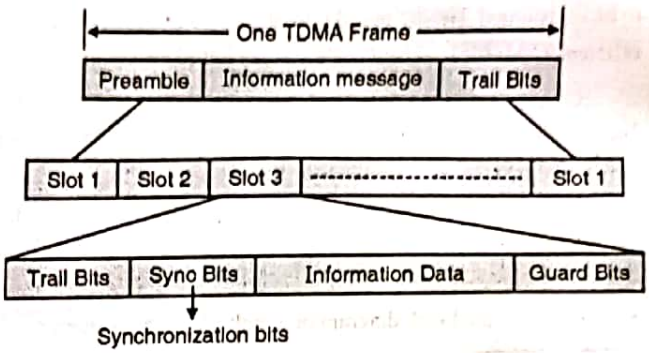


Fig. 2.4 : TDMA frame structure

A frame consists of a number of slots. Each frame consists of preamble, an information message and trail bits. Half of the time slots will be used for the forward link channels and the remaining half for reverse link channels.

The preamble field comprises the address and synchronization data that both the base stations and subscribers use to identify each other. The guard bits are used to provide synchronization of different receivers between, different time slots and frames. It is assumed that there are "N" number of slots for N users so that each user can access the channel in their allowed time slot.

The TDMA/FDD systems have identical frame structure that can be used for forward or reverse transmission, but the carrier frequencies will be different for both the links.

TDMA Features

i) TDMA uses different time slots for transmission and reception. Hence, duplexers are not required. If FDD is used then a switch is used to switch between transmitter and receiver.

ii) As the transmission rates are high adaptive equalization is necessary.

iii) TDMA shares a single carrier frequency with several users, where each user makes use of non-overlapping time slots. The number of time slots depend on parameters like bandwidth, modulation method etc.

Scanned by CamScanner

iv) Using TDMA we can allocate different number of time slots per frame to different users. Thus, bandwidth can be supplied on demand to different users by reassigning time slots depending on the priority.

v) Data transmission is done in bursts. It results in low battery consumption as the transmitter of the subscriber can be turned off when it is not in use.

vi) Guard time needs to be minimized. If the signal is transmitted at the edges of the time slot, it is suppressed to reduce the guard time. The transmitted spectrum will expand resulting in adjacent channel interference.

vii) In TDMA, the handoff process is simple. An enhanced link control like that provide by mobile assisted handoff (MAHO) can be carried by the subscriber by listening on an idle slot in the TDMA frame.

viii) Because of burst transmissions high synchronization overhead is needed in TDMA systems.

Q. 4 Explain in detail CDMA. **Dec. 12, Dec. 15**

Ans. :

Code Division Multiple Access

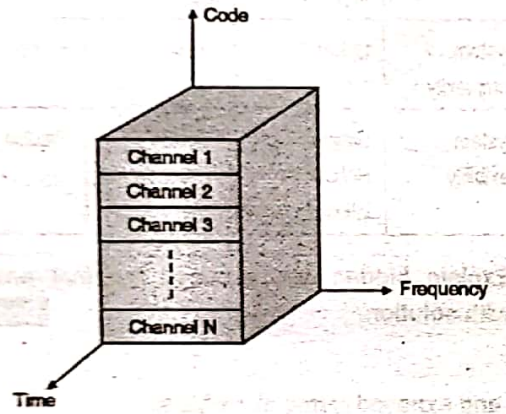


Fig. 2.5 : Code Division Multiple Access

In this multiple access scheme many users share the same carrier frequency (f_c). The narrowband message signal is also multiplexed with a spreading signal of larger bandwidth. This spreading signal is a pseudo noise code sequence and it has higher chip rate than the data rate of the message signal.

As the same channel is used by several users, there may be a problem of **near-far effect**. The near-far problem occurs if the power of each user within the cell is not controlled such that they appear equal at the base station.

The main advantage of CDMA when compared to other multiple access methods is reduced level of interference. As each user is allocated an individual pseudo random codeword that is orthogonal to the codewords of the other users at the receiver end the receiver tunes to receive the intended signal of the user.

To minimize the near-far problem power control is essential in CDMA systems. Power control is implemented at the base station by sampling the radio signal strength indicator (RSSI) levels of each mobile and then a power change command over the forward radio link.

Features of CDMA

The features of CDMA are :

i) In CDMA the channel data rates are very high. Hence, the symbol duration is short and less than the channel delay spread. As PN sequences have low auto correlation, multipath that is delayed by more than a chip will appear as noise. A Rake receiver can be used to improve the reception by collecting time delayed versions of the required signal.

ii) If an undesired user has a high power compared to other user then near far problem arises at the CDMA receiver end.

iii) CDMA uses cochannel cells. Spatial diversity can be used to provide soft handoff. Soft handoff is done by the MSC that can monitor a specific user from two or more base stations. Without switching the frequencies, MSC can decide the best version.

iv) The CDMA system users share the same frequency. TDD or FDD can be used.

v) CDMA has a soft capacity limit. If the number of users increases, the noise increases and system performance decreases.

vi) Multipath fading can be reduced as the signal is spread over a large spectrum. If the spread spectrum bandwidth is greater than the coherence bandwidth of the channel, the frequency diversity will mitigate the effects of small-scale fading.

vii) In CDMA systems self jamming is a problem. The spreading sequences of different users are not exactly orthogonal. This leads to self jamming.

Q. 5 Compare FDMA, TDMA and CDMA technologies. **Dec. 12**

Ans. :

Comparison of FDMA, TDMA and CDMA technologies

Sr. No.	Parameter	FDMA	TDMA	CDMA
1.	Method	Overall band width is shared among many stations.	Time sharing of satellite transponder takes place.	Sharing of bandwidth and time both takes place.
2.	Interference effect	Due to nonlinearity of	Due to incorrect synchronizati	Both type of interferences will be

Scanned by CamScanner

Sr. No.	Parameter	FDMA	TDMA	CDMA
		transponder amplifiers, inter modulation products are generated due to interference between adjacent channels.	on there can be an interference between the adjacent time slots.	present.
3.	Synchronization	Synchronization is not necessary.	Synchronization is essential.	Synchronization is not necessary.
4.	Code word	Code word is not required.	Code word is not required.	Code words are required.
5.	Guard times and bands	Guard bands between adjacent channels are necessary.	Guard times between adjacent time slots are necessary.	Guard bands and Guard times both are necessary.
6.	Hand-over	Hard handover	Soft handover	Soft handover
7.	Allocated bandwidth	12.5 MHz	12.5 MHz	12.5 MHz
8.	Frequency reuse	7	7	1
9.	Required channel bandwidth	0.03 MHz	0.03 MHz	1.25 MHz
10.	Number of RF channels	$\frac{12.5}{0.03} = 416$	$\frac{12.5}{0.03} = 416$	$\frac{12.5}{1.25} = 10$
11.	Control channels / cell	2	2	2
12.	Usable channel / cell	57	57	8
13.	Voice channels cell	$57 \times 1 = 57$	$57 \times 4 = 228$	$8 \times 4 = 320$
14.	Sectors per cell	3	3	3
15.	Voice calls/sector	$\frac{57}{3} = 19$	$\frac{228}{3} = 76$	$\frac{320}{3} = 106$
16.	Key resources	FDMA assigns individual channels to individual users.	TDMA systems divide the radio spectrum into time slots.	CDMA systems use the same carrier frequency and can simultaneously transmit.
17.	Sharing of resources.	Each user is allocated a unique channel. No other user can share that channel when a call is in progress.	Each user makes use of non-overlapping time slots. The data transmission occurs in bursts.	Each user has its own pseudorandom codeword that is orthogonal to other keywords.
18.	System complexity	Lower	Higher	Higher
19.	System flexibility	Simple and Robust, inflexible	Flexible	Flexible

Q. 6 Explain hidden and exposed terminal problem with solution. **Dec. 16**

Ans. :

Hidden and exposed terminal problem

The basic access method is CSMA/CA carrier sense multiple Access with collision avoidance mechanism. CSMA/CD is most popularly used protocol. (CD stands for Collision Detection.) In a wired environment every station connected the wire can sense the signal in the wire. In a wired LAN of there is no activity or collision of messages, every station connected to the LAN will be able to sense the collection instantly. CSMA/CA protocol is used as it is not possible to detect collision of data packets in midair.

Fig. 2.6 shows three mobile nodes.

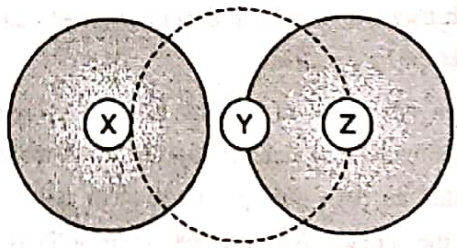


Fig. 2.6 : Hidden terminal

Scanned by CamScanner

The transmission of X reaches Y, but not Z. The transmission of Z reaches Y, but not X. However the radio signal of Y reaches both X and Z making X and Z both in the range of Y. The net effect is X cannot detect Z and Z cannot detect X. X starts sending to Y, Z does not receive this transmission. Z also wants to send to Y and senses the medium. To Z the medium appears to be free. Thus, Z starts sending causing collision at Y. But now X cannot detect the collision and continues with its transmission. X is **"hidden terminal"** for Z and vice-versa.

Consider Fig. 2.7. The radio transmission of signal of X reaches Z and Y. The radio signal of Z reaches both X and W. X wants to communicate to Y, X starts sending signals to Y. Z wants to communicate to W, Z senses the carrier and finds what X is talking to Y. Z has to wait till the time X finishes with Y. However W is outside the range of A. Hence waiting is not essential. X, Y, Z and W can communicate in parallel without any collision, but according to the protocol it is not possible. The terminals X and Z are called **"exposed-terminals"**.

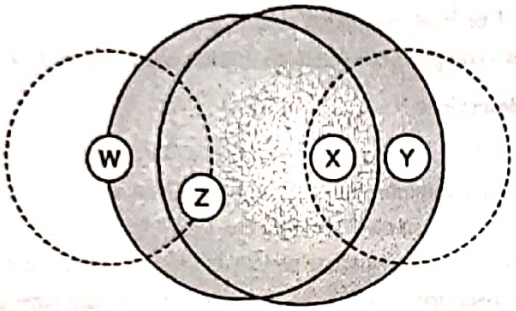


Fig. 2.7 : Exposed terminal

Q. 7 Write note on : OFDM.

May 11. Dec. 11. Dec. 15. May 16

Ans. :

OFDM (Orthogonal Frequency Division Multiplexing)

Orthogonal frequency division multiplexing (OFDM) is a multicarrier transmission technology. Its function is to obtain a higher data rate in the multipath fading environment of mobile communication.

In mobile communication the selection of digital modulation is dependent on three parameters. They are :

i) Narrower bandwidth

ii) Efficient power utilization

iii) Elimination of intermodulation products.

Fig. 2.8 shows a multicarrier OFDM method. Orthogonal means "unrelated or independent of each other". The subcarriers for each radio channel are orthogonal to one another. As shown in Fig. 2.8 the subcarriers are spaced close to each other without guard bands.

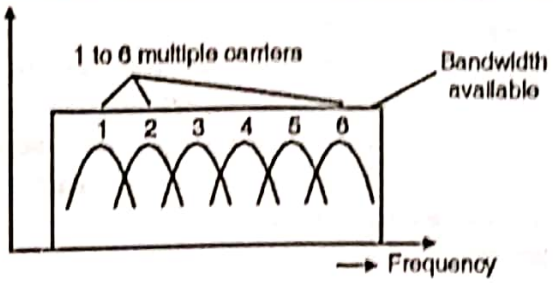


Fig. 2.8 : OFDM method

The principle of orthogonality can be obtained by dividing the carrier signal with an integer multiple that is capable of making the inverse of symbol duration of the parallel bit streams. OFDM uses data bursts to reduce the intersymbol interference many symbols are sent in parallel. Hence, the symbol rate decreases.

When the symbol duration increases, the intersymbol interference effects that were produced by Rayleigh fading are reduced. The OFDM method is applied to reduce the frequency selective fading and burst errors generated by wideband fading signals in wireless communication. The OFDM method is robust in the narrowband interference environment.

The advantage of OFDM is it's efficiency to handle suppressing multipath effects. Figs. 2.9 and 2.10 shows an OFDM transmitter and receiver. At the transmitter side error correction coding, interleaving process is done over the data stream. The data stream that is sent is in the form of symbols that have undergone quadrature amplitude modulation. Then the symbol stream is passed through serial to parallel process. Each symbol is assigned to one of the subcarriers with assigned symbol. Every subcarrier will operate at a particular frequency.

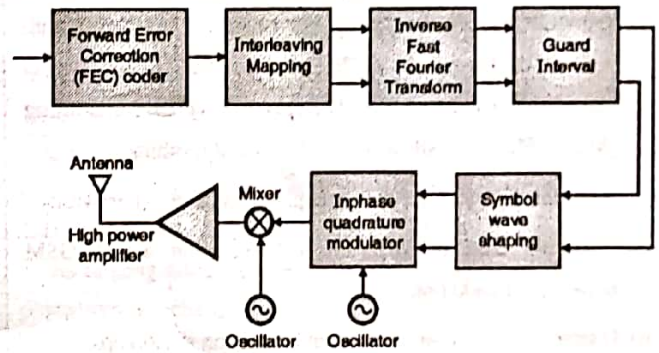


Fig. 2.9 : OFDM transmitter

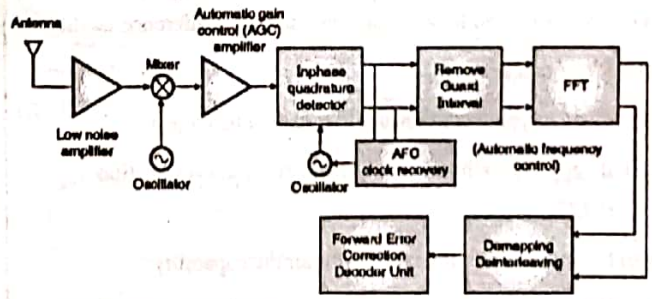


Fig. 2.10 : OFDM receiver

Scanned by CamScanner

In frequency domain the symbol frame is formed with the group of symbols from all subcarriers. Then every symbol frame is transformed into time frame with the help of N point "Inverse Fast Fourier Transformation (IFFT)". The digital data stream is generated by these time frames. Finally the signal is amplified and transmitted to the antenna. Convolutional coding method with CRC error detection is use to provide high data security.

OFDM is sensitive to phase and frequency noise. To minimize it correct pulse shape needs to be selected. In OFDM receiver the symbol frames received is detected. It has to adjust automatic gain control to the desired level. A robust algorithm is to be used to withstand phase noise and frequency offset of the receive unit that will interface with the synchronization process.

Chapter 3 : Wireless Technologies

Q. 1 What are the features of GSM ?

Ans. :

Features of GSM

(i) It supports more subscriber capacity in the given spectrum.

(ii) The short messaging service (SMS) allows the GSM subscribers to transmit and receive character text messages.

(iii) It has a subscriber identity module (SIM). The SIM is a memory device that stores information like subscriber's identification number. Each subscriber uses a four digit personal ID number inorder to activate service from any GSM phone. The SIMs are smart cards or plug-in modules. The subscribers can insert their SIM into a mobile phone, a personal phone and then receive GSM calls to the number irrespective of the location.

(iv) On-the-air privacy is provided by the GSM system. Privacy is done by encrypting the digital bit stream sent by the GSM transmitter, according to a secret cryptographic key that is known to the cellular carrier. For each user key is different. Before deploying a GSM system, the GSM system manufacturer must sign a **Memorandum of Understanding** (MoU). The MoU allows cryptographic algorithms.

(v) It has the ability to use the same phone in different networks.

(vi) It allows data transmission and reception across GSM networks at 9600 bps.

(vii) It supports FAX transmission and reception at 9.6 kbps.

(viii) It supports smaller handsets.

(ix) It supports call forwarding, call on hold, conference facility.

(x) Rapid call setup.

(xi) The encrypted conversions that cannot be tapped.

(xii) It supports Calling Number Identification Presentation (CLIP).

(xiii) It supports fully international roaming capability.

(xiv) It has compatibility with ISDN for supplementary services.

Q. 2 Explain GSM services. **Dec. 12**

Ans. :

GSM Services

All the GSM services follow ISDN guidelines.

The GSM services can be divided into three categories. They are :

The teleservices comprise mobile telephony and mobile originated or base originated traffic. The data services comprise computer - computer communication and packet switched traffic.

(i) Teleservices

A telephone is the most basic teleservice supported by GSM. Like all other communication systems, in GSM speech is digitally encoded and transmitted through the GSM network as a digital stream. An emergency calling service is present, where the nearest emergency-service provider can be notified by dialing three digits. It also includes facsimile. GSM supports videotext and Teletext transmission.

(ii) Bearer services or data services

The bearer or data services are limited to the first 3 layers of OSI model. The data can be transmitted using either a transparent mode or nontransparent mode.

The data services provided by GSM are :

(a) The users can transmit and receive data from 300 bps to 9.6 Kbps.

(b) Access to users on POTS (Plain Old Telephone Service), ISDN, Packet Switched Public Data Networks and Circuit Switched Networks using a variety of access methods and protocols like X.25 and X.32.

(c) It supports Group 3 facsimile (FAX) service.

(d) It supports bidirectional SMS service, the messages are transported in a store-and-forward manner. The SMS can be sent on point-to-point and cell broadcast mode.

(iii) Supplementary ISDN services

These services are provided apart from teleservices or bearer services.

Scanned by CamScanner

They include :

(a) Call diversion (b) Number identification services

(c) Closed user groups (d) Call forwarding services

(e) Call completion services (f) Multiparty services

(g) Call restriction services (h) Short messaging service

The GSM system also provides General Packet Radio Service. It provides possibility to access public packet switched networks through a dedicated traffic channel. The SMS can be used for safety and advisory applications like weather information to all GSM subscribers in range.

Q. 3 Explain GSM network architecture.

May 11, Dec. 11, May 12, Dec. 12, Dec. 14, Dec. 15, May 16

Ans. :

GSM System Architecture

BTS : Base Transceiver Station

BSC : Base Station Controller

HLR : Home Location Register

VLR : Visitor Location Register

MSC : Mobile Switching Centre

EIR : Equipment Identity Register

AUC : Authentication Center

OMC : Operation Maintenance Center

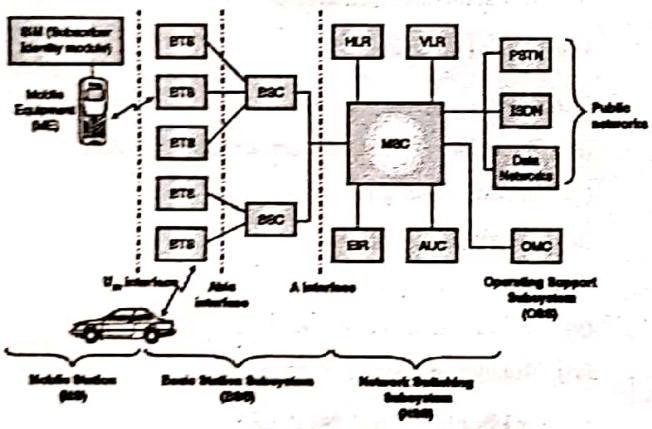


Fig. 3.1 : GSM architecture

A GSM network consists of various functional entities, whose functions and interfaces are specified. Fig. 3.1 shows the generic architecture of a GSM network. A GSM architecture consists of three major subsystems that interact between themselves with the users through some network interfaces.

The subsystems are :

(i) Base Station Subsystem (BSS)

(ii) Network and Switching subsystem (NSS)

(iii) Operation Support Subsystem (OSS)

The Mobile Station (MS) is also a subsystem, but it is consider to be part of BSS for architecture purposes. Fig. 3.1 shows the GSM architecture. The mobile stations (MS) communicate with the base station subsystems over the radio interface (U_m). The BSS called as the radio subsystem, provides and manages the radio transmission path between the mobile stations and the Mobile Switching Centre (MSC). It also manages radio interface between mobile stations and other subsystems of GSM.

Each BSS comprises many Base Station Controllers (BSCs) that connect the mobile station to the network and switching subsystem (NSS) through the mobile switching center. The NSS controls the switching functions of the GSM system. It allows the mobile switching center to communicate with networks like PSTN, ISDN, CSPDN, PSPDN and other data networks.

The Operation Supports Subsystem (OSS) allows the operation and maintenance of the GSM system. It allows the system engineers to diagnose, troubleshoot and observe the parameters of the GSM system. The OSS subsystem interacts with the other subsystems and is provided for the GSM operating company staff that provides service facilities for the network.

1. Mobile Station

The Mobile Station (MS) comprises of **Mobile Equipment** (ME) and a smart card called **SIM (Subscriber Identity Module).** SIM provides personal mobility to have access to subscribed services irrespective of the mobile equipment. After inserting the SIM card into a GSM handset, the user can receive calls, make calls and enjoy other subscribed services.

The mobile equipment (handset) is uniquely identified by the **International Mobile Equipment Identity (IMEI)** number. The SIM card has the **International Mobile Subscriber Identity** (IMSI) used to identify the subscriber to the system. It is a separate secret key provided for authentication. Both the IMEI and IMSI are impendent. They allow personal mobility. The SIM card can be protected against unauthorized use by a password or **Personal Identity Number (PIN).** The GSM mobile stations support power levels ranging from 0.8 – 8W. Inorder to extend the battery life, power saving techniques are used.

2. Base Station Subsystem (BSS)

The base station subsystem comprises of two parts :

The BSS consists many BSCs that connect to a single MSC. Each BSC controls upto several hundred Base Transceiver Stations (BTSs). Some of the BTSs can be colocated at the BSC and the others can be remotely distributed. They are connected to the BSCs by dedicated leased lines or microwave links. The interface that connects BTS to BSC is called as the **Abis interface.** It carries the traffic and maintenance data.

Scanned by CamScanner

a. Base Transceiver Station (BTS)

The BTS has radio transceivers that define a cell and are capable of handling the radio-link protocols with the Mobile Station (MS).

The **functions** of BTS are :

(i) Handling radio link protocols.

(ii) Providing full duplex communication to the Mobile Station (MS).

(iii) Interleaving and deinterleaving.

The BTS comprises the **Transcoder Rate Adapter Unit (TRAU)**. In this unit, the GSM specific speech encoding and decoding is done. Also the rate adaption function of data is done.

b. Base Station Controller (BSC)

The Base Station controller manages the radio resources for one or more BTSs. It controls upto several hundred BTSs. They are connected to a single MSC.

The **functions** of the base station controller are :

(i) To control BTSs

(ii) Radio resource management.

(iii) Handoff management and control.

Mobile handoffs between two BTSs that **are controlled by a BSC are handled by the same BSC**. This reduces the burden of the Mobile Switching Center (MSC). BSC also handles radio-channel set up and frequency hopping. The BSCs are physically connected through leased lines or microwave links to the MSC. The interface between the BSC and MSC is called as **A interface**.

3. Network and Switching Subsystem (NSS)

It handles the switching of GSM calls between the external networks and the BSCs in the radio subsystem. The NSS is responsible for managing and providing external access to various customer databases. The central component of this subsystem is the MSC (mobile switching center). It controls all the traffic among all the BSCs. The function of MSC is to handle mobile subscribers registration, authentication, localization, handovers, call routing etc.

The network and switching subsystem includes three different databases for mobility management. They are :

(i) Home Location Register (HLR)

(ii) Visitor Location Register (VLR)

(iii) Authentication Center (AUC)

a. Mobile Switching Center (MSC)

The MSC connects to fixed networks like ISDN, PSTN etc. It provides additional capabilities to support mobility management functions like terminal registration location, updating and handoff.

The **functions** of MSC are :

(i) Call setup, supervision and release.

(ii) Digit collection and translation.

(iii) Collection of billing information.

(iv) Mobility management- registration, location updation and call handoff between BSC and MSC.

(v) Call handling / routing.

(vi) Cancellation of echo.

(vii) Management of signaling protocol.

(viii) Radio resource management during call.

(ix) Interrogation of appropriate registers (VLR / HLR).

b. Home Location Register (HLR)

The call roaming and call routing capabilities of GSM are handled by the Home Location Register (HLR). It comprises all the administrative information of every subscriber that is registered in that corresponding GSM network . Also the current location of the mobile station (MS) is available in the HLR. A unique International Mobile Subscriber Identify (IMSI) of each subscriber is maintained in the HLR database. Each home number can be identified by this number.

There is logically one HLR per GSM network, although it may be implemented as a distributed database.

The HLR database can be grouped into two types.

1. Dynamic database

(i) It contains the location information for each subscriber.

2. Permanent database

It includes :

(i) International Mobile Subscriber Identity (IMSI)

(ii) Service subscription information.

(iii) Supplementary services.

(iv) Service restriction.

(v) Mobile terminal characteristics.

(vi) Billing / accounting information.

c. Visitor Location Register (VLR)

The Visitor Location Register (VLR) contains selected administrative information from HLR essential for call control and provision of subscribed services. The VLR is a temporary database. It stores the IMSI number and customer information for each roaming customer visiting the coverage area of a specific MSC. It consists the information of every user visiting in that area. When a mobile that is roaming, is logged in the VLR the MSC sends the essential information to the subscribers HLR so that calls to the roaming mobile can be routed over the PSTN by users HLR.

Scanned by CamScanner

The VLR also contains information about the locally activated features like call forward on busy.

The temporary subscriber information in VLR includes :

(i) Currently activated features.

(ii) International Mobile Subscriber Identity (IMSI).

(iii) Current location information about Mobile Station (MS).

(iv) Directory number to route calls to the roaming station.

(v) Copy of subscriber data from HLR.

(vi) Temporary mobile station identity (TMSI).

(vii) Location where the mobile is registered.

(viii) HLR address.

(ix) Mobile station ISDN number.

d. Authentication Center (AUC)

The Authentication Center is a protected database. It stores a copy of the secret key stored in each subscriber's SIM card that is used for authentication and encryption over the radio channel. The authentication center maintains authentication keys and algorithms. It provides security triplets (RAND, SRES and K_C) to the VLR. The AUC handles authentication and encryption keys for each subscriber in the HLR and VLR.

The Authentication center contains a register called as **Equipment Identity Register (EIR)**. It identifies stolen or fraudently altered phones that transmit the identity data that does not match with the data in HLR or VLR.

The EIR is a database that contains a list of valid mobile equipment on the network where each mobile station is identified by its International Mobile Equipment Identity (IMEI) number. The IMEI is marked invalid if it is reported stolen or not type approved. The data in EIR is in the form of **white, grey and black lists that** the network consults when it wishes to confirm the authenticity of terminal requesting service.

The different lists and their contents are given below :

Type	IMEI Number	Contents
White List	Valid IMEI number.	List of valid mobile equipments.
Black List	Prohibited IMEI number.	List of mobile for which service is barred.
Grey List	IMEI under scanner	List of suspected mobile under observation.

4. Operation Support Subsystem (OSS)

The OSS supports one or many Operation Maintenance Centers (OMC) that are used to monitor and maintain the performance of different subsystems within a GSM system.

The three functions of OSS are :

(i) To manage subscription management i.e. charging and billing procedures.

(ii) To manage all mobile equipment in the system.

(iii) To maintain all telecommunications hardware and network operations within a market.

An OMC is allotted to each task. It has capability of adjusting all the base station parameters and billing procedures. It allows the system operators to determine the performance of the GSM system. If there is an emergency at the base station, the OSS can determine where the BTS is located, what type of failure occurred and what equipment the site engineer will need to repair the failure.

Q. 4 List and explain the types of channels of GSM. **Dec. 17**

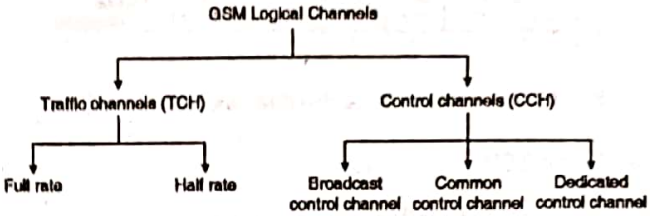
Ans. :

GSM Channel Types

There are two types of GSM logical channels. They are :

(i) Traffic channels (TCH)

(ii) Control channels (CCH)



The traffic channels (TCH) are used to carry digitally encoded user speech or user data in the forward or reverse links. For full rate the data rate is 22.8 KB/s and for half rate the data rate is 11.4 KB/s. The control channels (CCH) carry the synchronizing and signaling commands between the base station and the mobile station. They are responsible for mobility management. Fig. 3.2 shows the GSM channel structure.

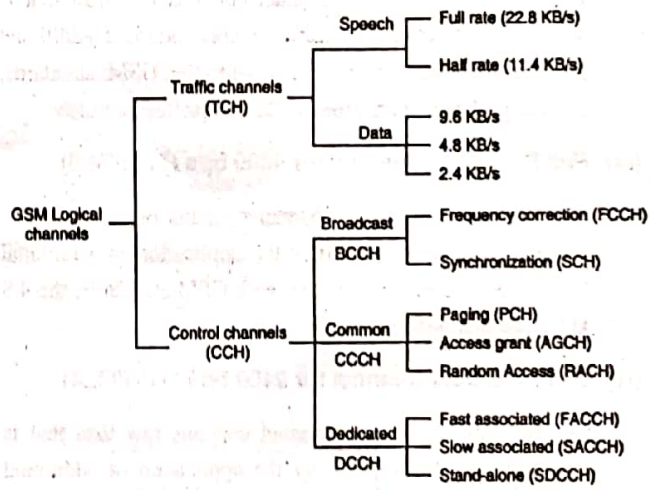


Fig. 3.2 : GSM Channel Structure

Scanned by CamScanner

(I) Traffic Channel (TCH)

Traffic channels carry digitally encoded user data or user speech on the forward and reverse links. A TCH is a group of 26 consecutive TDMA frames, called a **multiframe** of the 26 TDMA frames, 24 are used as TCH frames, one frame (13th) is for SACCH and 26th is unused or idle frame.

TCH supports two types of information rates. They are :

(i) Full rate (TCH/F)

(ii) Half rate (TCH/H)

When transmitted as full rate, the user data is occupied within TS per frame. When transmitted as half rate, the user data is occupied into the same time slot but sent in alternate frames. The 26th frame contains idle bits if full rate TCHs are used and contains SACCH data if half rate TCHs are used.

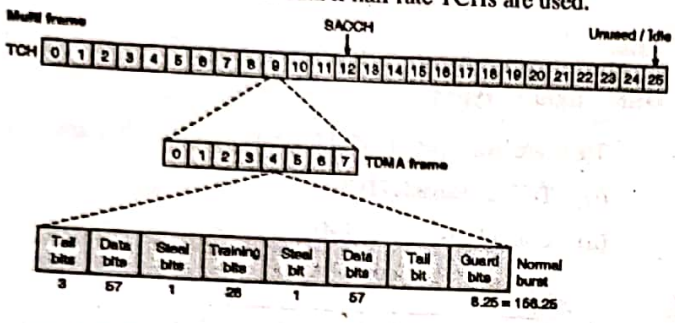


Fig. 3.3 : TCH data transmitted in 26 consecutive frames

Full Rate TCH

Different full rate TCH for data and speech channels are :

(I) Full-Rate Speech Channel (TCH/FS)

At 13 Kbps the full rate speech channel is digitized. The full rate speech channel carries 22.8 kbps after adding the GSM channel coding to the digitized speech.

(ii) Full-Rate Data Channel for 9600 bps (TCH/F9.6)

The full rate traffic data channel contains raw data that is transmitted at 9.6 kbps. After the application of additional forward error correction coding with the GSM standards, 9600 kbps data is transferred at 22.8 kbps.

(iii) Full Rate Data Channel for 4800 bps (TCH/F4.8)

The full rate traffic data channel contains raw data that is transmitted at 4.8 kbps. After the application of additional forward error correction coding with GSM standards, the 4.8 kbps data is transferred at 22.8 kbps.

(iv) Full Rate Data Channel for 2400 bps (TCH/F2.4)

The full rate traffic data channel contains raw data that is transmitted at 2.4 kbps. After the application of additional forward error correction coding with GSM standards, the 2.4 kbps data is transferred at 22.8 kbps.

Half Rate TCH

Different half rate TCH for speech and data channels are given below :

(I) Half Rate Speech Channel (TCH/HS)

The half rate speech channel can carry digitized speech that is sampled at a rate half that of full rate channel. GSM anticipates the availability of speech coders. It can digitize speech at about 6.5 kbps. After adding GSM channel coding to the digitized speech, the half rate speech channel will carry 11.4 kbps.

(ii) Half Rate Data Channel for 4800 bps (TCH/H4.8)

The half rate traffic data channel carries raw user data that is sent at 4800 bps. After the application of forward error correction using GSM standards, 4800 bps data is sent at 11.4 kbps.

(iii) Half Rate Data Channel for 2400 bps (TCH/H2.4)

The half rate traffic data channel carries raw user data that is sent at 2400 bps. After application of additional forward error correction using GSM standards, 2400 bps data is sent at 11.4 kbps.

(ii) Control Channels (CCH)

The control channels carry the signaling and synchronizing commands between the base station and the mobile station. They are used when the mobile is in the idle or dedicated mode.

There are three main control channels. They are :

Each control channel consists of several logical channels that are distributed to provide necessary control functions.

Broadcast Control Channel (BCCH)

The BCCH is a forward control channel. It is a unidirectional base to mobile channel that provides information about the network, the cell in which the mobile is currently located and adjacent cells.

It broadcasts a list of channels that are currently in use within the cell.

The BCCH includes two channels. They are :

(I) Frequency Correction Channel (FCCH)

It is a base to mobile channel that provides information for carrier synchronization. It is a special data burst that occupies TS0 slot for the first GSM frame. It is repeated every ten frames within a control channel multiframe. The FCCH allows the mobile subscriber to synchronize its internal frequency standard with the frequency of the base station (BS). In the first burst of FCCH, all zero bits are sent to indicate the unmodulated carrier.

Scanned by CamScanner

Fig. 3.4 shows the frequency correction burst.

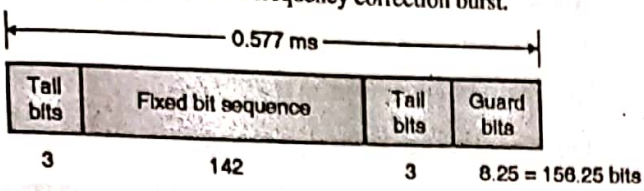


Fig. 3.4 : Frequency correction burst (FCCH) structure

(ii) Synchronization Channel (SCH)

This channel acts as a base to mobile channel. The mobile channel carries the information for identification and frame synchronization of the base station (BS) transceiver. It also comprises the frame number in relation to the hyper frame and the BSIC (Base Station Identity Code). In the frame that after the FCCH, in time slot TS0 BTS transmits with SCH. The SCH has a unique burst structure. It comprises of a 64 bit binary sequence that is common throughout the GSM networks.

The BSIC is assigned to each BTS in the GSM system. The SCH is transmitted once every ten frames within the control channel multiframe.

Fig. 3.5 shows the synchronization burst structure.

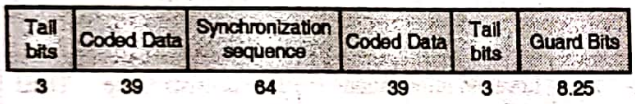


Fig. 3.5 : Synchronization burst structure

Common Control Channels (CCCH)

There are three different channels :

(i) Paging Channel (PCH)

The paging channel (PCH) provides paging signals from the base station to all the mobile in the cell. It registers an incoming call that originates from the PSTN. Paging is done by transmitting IMSI of the target subscriber along with request for acknowledgement from the mobile unit on the RACH. The PCH can be used to provide cell broadcast ASCII text messages to all the subscribers.

(ii) Random Access Channel (RACH)

It is a reverse link channel. With the help of RACH, the mobile station (MS) originates a call, sends signaling messages when not on call, acknowledges message. It uses slotted ALOHA access method i.e. all the mobiles must access or respond to a PCH alert within TS0 of a GSM frame. At the BTS each frame will accept the RACH transmissions from the mobiles during TS0. The base station responds to the RACH transmission by allocating a channel and a Stand-alone Dedicated Control Channel (SDCCH) for signaling in the presence of a call. The connection is confirmed by the base station over the Access Grant Channel (AGCH).

The RACH burst has longer guard period to protect for burst transmission from Mobile station that does not know the timing advance when it first accesses the system. The additional guard time allows a distance upto 35 km between base station to mobile station. Fig. 3.6 shows the Random access burst.

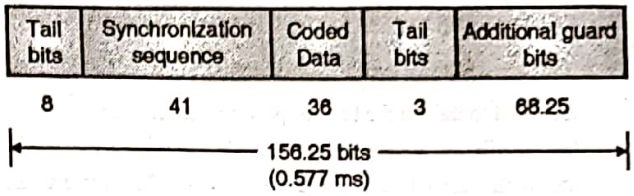


Fig. 3.6 : Random access burst

(iii) Access Grant Channel (AGCH)

The AGCH is used by the base station to provide forward link communication to the mobile. It carries data that instructs the mobile to operate in a specific channel with a particular dedicated control channel. It is the message sent by the base station before a subscriber is moved off the control channel. The AGCH is used by the base station to respond to RACH sent by the mobile station in the earlier CCCH frame.

Dedicated Control Channels (DCCHs)

The dedicated control channels (DCCHs) come into picture after a call is established. The dedicated control channels are bidirectional. They have same formats and functions in the forward and the reverse links.

There are three different dedicated control channels. They are :

(i) Stand-alone Dedicated Control Channels (SDCCH)

The Stand-alone Dedicated Control Channel (SDCCH) is allocated for every mobile station. It contains the signaling data that follows the connection of the mobile with the Base Station (BS), prior to the allocation of TCH by the Base Station (BS) to the MS. It guarantees that the Mobile Station (MS) and base station (BS) will remain connected. The Base Station and Mobile Switching Center will verify subscriber unit and assign the needed resources to the mobile. This channel that accepts the newly completed call from the BCH. It holds the traffic while waiting for the base station to assign a TCH channel.

The SDCCH is also used to transmit authentication and alert messages as the mobile synchronizes itself with the frame structure and waits for TCH. SDCCHs can be assigned their own physical channel. Also they can occupy the TS0 slot of the BCH if there is low demand for BCH or CCCH traffic.

Scanned by CamScanner

(ii) Slow Associated Control Channel (SACCH)

It is related to traffic channel or SDCCH.

On the forward link it is used to send regularly changing information like :

(i) transmit power level.

(ii) specific timing advance instructions for each user.

(iii) broadcast messages.

On the reverse link it carries information about

(i) received signal strength.

(ii) quality of TCH and BCH

(iii) measurement results from neighboring cells.

It is used to inform the base of power measurements mode by the mobile of signal strength in the adjacent cells. It is transmitted during the 13th frame (and on the 26th frame when half rate traffic is used) of every dedicated control channel multi frame. SACCH exchanges control information between base station and mobile station during a call or call set up.

(iii) Fast Associated Control Channels (FACCHs)

FACCH carries important messages. It is used for exchange of time critical information between the mobile and the base station during the progress of the call. The FACCH is assigned whenever SDCCH is not dedicated to a user and there is an urgent message like hand-off request.

The FACCH transmits control information by stealing capacity from the associated traffic channel. It is done by setting two special bits called stealing bits. In the TCH forward channel burst. If a stealing bit is set, the time slot contains FACCH data for that frame.

Q. 5 Explain in detail GSM Privacy and Authentication with neat diagram. **May 17**

Ans. :

Authentication and Security in GSM

GSM is a system that operates on radio frequencies. The information on the air interface needs to be protected inorder to provide data to the user confidentially (in SIM). Also subscriber privacy needs to be ensured. In GSM, the mobile station consists of two parts : one the hardware and the software specific to the radio interface. The user specific data is referred as **Subscriber Identity Module (SIM).**

SIM has various functions and limited programs. Most of the information present in the SIM is protected against modification. Because of security functions duplication of SIM is difficult as it provides a high degree of protection against fraudulent access to the network.

The security aspects supported by the GSM SIM are :

(i) Authentication algorithm (A_3)

(ii) Subscriber authentication key (K_i)

(iii) Cipher key generation algorithm (A_8)

(iv) Control of access to SIM stored data and functions performed in the SIM.

(v) Cipher key (K_C).

The SIM storage capability includes data given in Table 3.1.

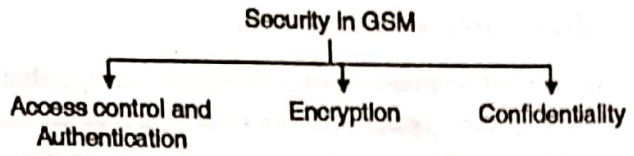
Table 3.1

Sr. No.	Parameter	Description
1.	Administrative information	It indicates the mode of operation of SIM.
2.	SIM service table	It indicates the optional services that are provided by SIM.
3.	International Mobile Subscriber Identity (IMSI)	It identifies the subscriber unambiguously.
4.	IC card identification	This number uniquely identifies the SIM and card issues.
5.	Location information	It consists the TMSI (Temporary Mobile Subscriber Identity) and Location Area Information (LAI).
6.	Broadcast control channel information	It lists the carrier frequencies to be used for call selection.
7.	Cipher key and cipher key sequence number	It is a sequence of symbols needed to encrypt or decrypt the information.
8.	Language preference	It shows the Man-machine Interface (MMI) languages preferred by the subscriber.
9.	Forbidden PLMNs.	They are used by SIM to avoid unnecessary registration attempts.

The degree of security in GSM is higher. The basic security mechanisms are :

1. **Access control and authentication :** To prevent access by unregistered users.
2. **Encryption :** To prevent unauthorized listening.
3. **Confidentiality :** To prevent subscriber location disclosure.

Scanned by CamScanner



(i) Confidentiality

Encryption and decryption methods are used to maintain confidentiality. The information about the user is encrypted. Only an authorized person can decrypt it.

(ii) Encryption

All the user related information is encrypted. It ensures privacy from the subscriber point of view. After the authentication the Base Transceiver Station (BTS) can work with proper encryption with the help of cipher key (K_C). The SIM, MS and the network calculate the key 'K_C' based on a particular random value. The key itself is not transmitted.

The cipher key 'K_C' is not generated by using subscriber authentication key (K_i) but generated using some random value with a particular algorithm. The base transceiver station (BTS) and mobile station (MS) can encrypt at one end and decrypt at the other end using a cipher key of 64 bits.

(iii) Authentication

To prevent fraudulent use of the mobile identities and the subscriber, the GSM uses two techniques. They are :

(i) GSM uses a 4 digit PIN (Personal Identity Number) stored in the SIM. A user that wishes to make a call enters the PIN that is checked by the SIM.

(ii) GSM interrogates with the units. It is controlled from the MSC/VLR. Authentication can be done at call setup, localization, handover etc.

Once a mobile user has done an access and service request, the network checks the identity of the user by sending a random number (RAND) of 128 bits to the mobile. The mobile uses the RAND, K_i and A_3 algorithm to produce a 32 bit signed response (SRES) that is checked against the response from the mobile. Access continues only if the two responses match. Fig. 3.7 shows the authentication. Inorder to maintain desired security level, A_3 is devised so that computation of signed response (SRES) from RAND and K_i is simple. The computation of K_i from RAND and SRES is complex.

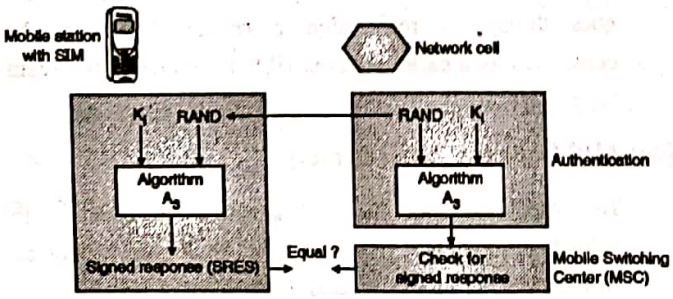


Fig. 3.7 : GSM authentication

The RAND and SRES and secret key "K_C" are sent to the Home Location Register (HLR). The Visitor Location Register (VLR) sends random number RAND to the SIM where the subscriber and network does the same type of functions. When both match, the VLR will accept the subscriber or will reject it. Hence, higher user authentication is made possible in the GSM users. Also, authentication of GSM mobile users can be carried out on mobile originated call and mobile terminated call setup and on activation of supplementary services.

Q. 6 With a neat diagram explain CDMA one architecture. **Dec. 10, Dec. 14, Dec. 15, May 17**

Ans. :

Architecture of IS-95 CDMA System

The CDMA on standard protocol architecture is shown in Fig. 3.8. The lower two layers and the corresponding layers of the OSI model are shown.

The functions of layer 1 are :

(i) Frequency use

(ii) Radio transmission

The functions of layer 1 are related to the voice and data packets. In layer 2 the Medium Access Control (MAC) sublayer is responsible for the channel management. It follows a finite state machine of two states.

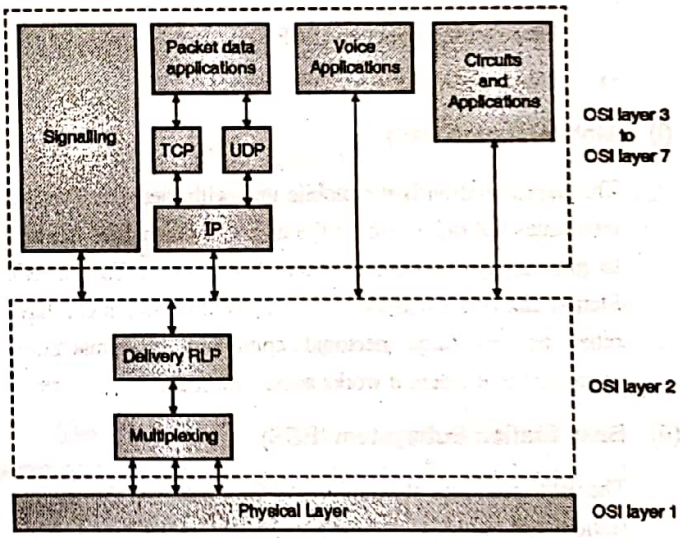


Fig. 3.8 : Protocol architecture of IS-95 (CDMA one standard)

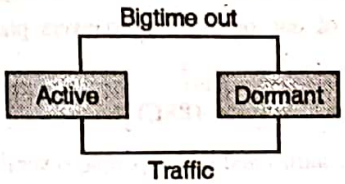


Fig. 3.9 : MAC states in IS-95 standard

Scanned by CamScanner

The status of packet data in transmissions is shown as a finite state machine of two cycles. Whenever a Mobile Station (MS) is idle it is considered as big time period. In the active state the channels are assigned to the mobile and in the dormant state the mobile units do not maintain any sequence of channels. As they do not maintain any sequence there is no mechanisms for transmitting user data when it is in dormant mode.

After the idle period the mobile channels go to the dormant state. Thus, the data from various sources are multiplexed initially and then handled. Fig. 3.10 shows the CDMA Architecture. CDMA one or IS-95 uses radio or last mile communication. Other than the radio interface, the remaining network is similar to GSM.

The main elements of the architecture are :

(i) Mobile Station (MS)

(ii) Base Station Subsystem (BSS)

(a) Base Transceiver Station (BTS)

(b) Base Station Controller (BSC)

(iii) Mobile Switching Center (MSC)

(iv) Home Location Register (HLR)

(v) Data Message Handler (DMH)

(vi) Visitor Location Register (VLR)

(vii) AUC (Authentication Center)

(viii) Equipment Identity Register (EIR)

(ix) (OMC) Operation Maintenance Centers

(x) Interworking Function (IWF)

(xi) Public Networks

(i) Mobile Station (MS)

The mobile station is the mobile unit with the user. The MS terminates the radio path on the user side. It enables the user to gain access to services from the network. The Mobile Station can be a stand-alone device. Mobile station can have other devices (e.g., personal computers, fax machines) connected to it where it works as pass through.

(ii) Base Station Subsystem (BSS)

The BSS manages the radio interface between the mobile stations and the MSC. It consists of BTS and BSC.

(a) Base Transceiver Station (BTS)

It consists of one or more transceivers placed at a single location.

(b) Base Station Controller (BSC)

Each BSC controls and manages upto several hundred BTSs. The BSC exchanges messages with the BTS and MSC. Some of the signaling messages can pass through the BSC transparently.

(iii) Mobile Switching Center (MSC)

The mobile switching center is the central unit equivalent to the telephone exchange in a fixed network. It is an automatic system that interfaces the user traffic from the wireless network with the wireline network or other wireless networks.

The functions of MSC are :

(a) **Anhor MSC :** It provides radio contact to a call.

(b) **Border MSC :** An MSC that is controlling BTSs adjacent to the location of the mobile station.

(c) **Originate MSC :** Direct the MSC to an incoming call towards the mobile station.

(d) **Candidate MSC :** MSC can accept the call or a handoff.

(e) **Remote MSC :** The MSC at the other end of the intersystem trunk.

(f) **Service MSC :** Provide service to a current call.

(g) **Tandem MSC :** MSC providing only trunk connections for call where handoff has occurred.

(h) **Target MSC :** Select MSC for handoff.

(i) **Visited MSC :** MSC providing service to the mobile station.

(iv) Home Location Register (HLR)

The Home location register maintains all subscriber related information and is responsible for managing the mobile subscribers. This register can be collocated with the MSC as an integral part of the MSC or it can be independent of the MSC. Multiple MSCs are served by an HLR. They can be distributed over multiple locations.

(v) Data Message Handler (DMH)

It is responsible for collecting the billing data.

(vi) Visitor Location Register (VLR)

It is linked to one or more MSCs. It is a functional unit that dynamically stores the subscriber information obtained from the subscriber's HLR data. When a roaming MS enters a new service area covered by the MSC, the MSC informs the associated VLR about the MS by querying the HLR after MS goes through a registration procedure. VLR can be considered as a cache whereas HLR is similar to persistent storage.

(vii) AUC (Authentication Center)

The AUC manages the authentication associated with individual subscriber. The AUC can be located within an HLR or MSC or may be located independent of both.

Scanned by CamScanner

(viii) Equipment Identity Register (EIR)

EIR provides information about the mobile device for record purposes. EIR can be located with the MSC or located independent of it.

(ix) Operation Maintenance Centers (OMC)

They are response for the overall management of the wireless network.

(x) Interworking Function (IWF)

It enables the MSC to communicate with other networks.

(xi) Public Networks

These are communication networks. They can be Public Switched Telephone Network (PSTN), an Integrated Service Digital Network (ISDN), a Public Land Mobile Network (PLMN) or a Public Switched Packet Data Network (PSPDN).

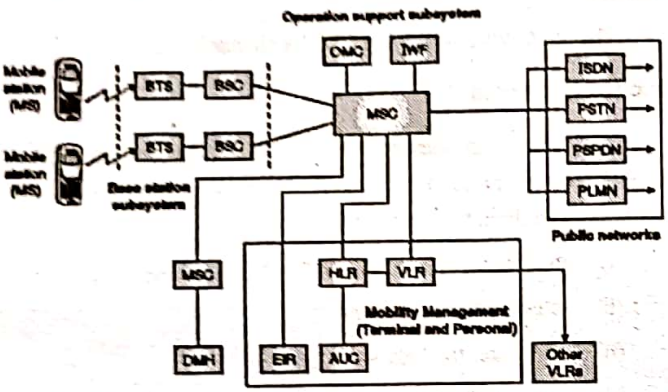


Fig. 3.10 : CDMA Architecture

BTS :	Base Transceiver Station
BSC :	Base Station Controller
MSC :	Mobile Switching Center
DMH :	Data Message Handler
OMC :	Operation Maintenance Center
IWF :	Interworking Function
HLR :	Home Location Register
VLR :	Visitor Location Register
AUC :	Authentication Center
EIR :	Equipment Identity Register

Q. 7 Explain the IS-95 CDMA forward and reverse channel in detail. **Dec. 12**

Ans. :

IS - 95 Channel Structure

IS-95 uses Frequency Division Duplexing (FDD) with 25 MHz in each direction.

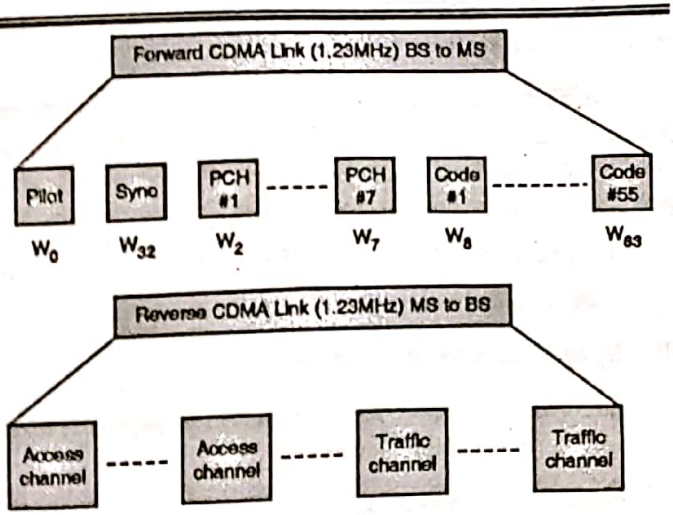


Fig. 3.11 : IS - 95 Forward and Reverse Link channel structure

Fig. 3.11 shows the IS - 95 forward and reverse link channel structures. By using direct - sequence spread spectrum DS/SS, an RF channel at the base station supports 64 orthogonal CDMA channels. Both the forward and the reverse channels are different. Let us study them one by one.

1. Forward CDMA Channels

The forward channels are called as **downlink channels.** They carry the data traffic from the base stations to the mobile stations effectively. They consist of 64 channels. The respective logical channels are differentiated from each other by various CDMA spreading codes called as orthogonal codes or Walsh function (W_0 to W_{63}). Some of the dedicated and common control traffic channels are as follows :

Pilot Channel

The pilot CDMA signal transmitted by a base station provides a reference for all mobile stations. It is assigned Walsh code W_0. The pilot signal level for all base stations is kept 4 to 6 dB higher than the traffic channel with a constant signal power. This is because the mobile station at the cell boundaries must be able to receive the pilot signal from the other cells to decide when to perform handoff.

The pilot signals from all the base stations use same PN sequences, but each station is identified by a unique time offset. The offsets are in increments of 64 chips to provide 512 unique offsets. The data rate is 19.2 kb/sec. The channel is a stream of 0's without discontinuity.

Sync Channel

It is an optional channel used to send synchronization information to the mobile stations. It is assigned Walsh code 32 (W_{32}). W_{32} has a pattern of 32 consecutive 0s and 32 consecutive 1s, that is ideal for synchronization. The sync channel message parameters are System Identification (SID), Network Identification (NID), pilot short PN sequence offset index. Long code state, system time, offset of local time, daylight saving time indicator and paging channel data rate (4.8 kbps or 9.6 kbps).

Scanned by CamScanner

Paging Channel (PCH # 1 – PCH # 7)

Paging channel is an optional channel. There are upto seven paging channels that transmit the control information to the terminals that do not have calls in progress. They operate at one of data rates namely 2400, 4800 or 9600 bits/sec.

The paging channels are assigned Walsh functions W_1 to W_7.

Some of the messages carried by paging channel include :

(i) System parameter message

Like base station identifier, the number of paging channels and the page channel number.

(ii) Neighbor list message

Data regarding the neighbouring base station parameters like PN offset.

(iii) Access parameters message

Parameters needed by the mobile to transmit on an access channel.

(iv) Paging message

It provides a page to the Mobile Station (MS).

(v) Channel assignment message

It informs the mobile station to tune to a new carrier frequency.

(vi) Data burst message

It is sent by the base station to the mobile.

(vii) Authentication

Authentication allows the base station to validate the mobile identify.

Forward Traffic Channels

The channels that are not used for paging or sync can be used for traffic. Thus, the total number of traffic channels is 63 minus the number of paging and sync channels in operation of the base station. The information on the forward traffic channel includes primary traffic (voice or data), secondary traffic (data) and signaling.

When forward link is used some of the messages will be,

(i) **Order message.**

(ii) **Authentication message :** It is used to prove the identity of the mobile when the base station suspects its validity.

(iii) **Alert with information message :** This message allows the base station to validate the mobile identity.

(iv) **Handoff direction message :** It provides the mobile with data required to initiate the handoff mechanism.

(v) **Analog handoff direction message :** It informs the mobile to switch to the analog mode and initiate the handoff.

(vi) **In-traffic system parameters message :** It updates some of the parameters set by the system parameter message in the paging channel.

(vii) **Neighbor list update message :** It updates the neighbor base station parameters set by Neighbor list message in the paging channel.

(viii) **Data burst message :** It is the data message sent by the base station to the mobile.

(ix) **Mobile registration message :** It informs the mobile that it is registered and supplies the necessary system parameters.

(x) **Extended handoff direction message :** It is one of the handoff message sent by the base station.

2. Reverse CDMA Channels

The reverse CDMA channels are also called as the **uplink channel.**

The main types of reverse CDMA channels are :

Access Channels

A terminal that does not have a call in progress can use the Access channel to send messages to the base station for three functions. The three functions are :

(i) to respond to a paging message

(ii) to originate the call and

(iii) to register the location

Up to 32 access channels can be operated by each base station. They operate at a rate of 4.8 kbps. The messages carried by the access channel include :

(i) **Order message :** It transmits information like base station challenge, mobile station acknowledgement, local control response and mobile station reject.

(ii) **Data burst message :** It is a user generated data message sent by the mobile station to the base station.

(iii) **Origination message :** It allows the mobile station to place a call sending dialed in digits.

(iv) **Registration message :** It sends to the base station data needed to page the mobile like status, location and identification.

(v) **Authentication response message :** It comprises data essential to validate the mobile stations identity.

Reverse Traffic Channel

It can multiplex primary (voice) and secondary (data) or signaling traffic.

The typical messages that the reverse traffic channel carries are :

Scanned by CamScanner

(i) Order messages

They include base station channel, parameter update confirmation, mobile station acknowledgement, service option request and response, release, connect, DTMF etc.

(ii) Authentication challenge response message

It consists data to validate the mobile station.

(iii) Pilot strength measurement message

It contains information about the strength of other pilot signals that are not associated with the serving base station.

(iv) Data burst message

It is a user generated data message sent by the mobile to a base station.

(v) Handoff completion message

It is a mobile response to a handoff direction message.

(vi) Parameter response message

It is a mobile response to the base station to retrieve parameters message.

Q. 8 Compare GSM with CDMA. **Dec. 17**

Ans. :

Difference between CDMA and GSM

Sr. No.	Parameter	GSM	IS-95/CDMA
1.	Frequency	900 MHz, 1800 MHz (PCS180), 1900 MHz (PCS 1900).	800 MHz, 1900 MHz.
2.	Channel bandwidth	Total 25 MHz bandwidth with 200 KHz per channels, 8 time slots per channel with frequency hopping.	Total 12 MHz with 1.25 MHz for the spread spectrum.
3.	Full-rate digitally code speech	13 kbps.	8 kbps or 13 kbps.
4.	Data bit rate	9.6 kbps and expandable.	9.6 kbps.
5.	SIM card	Yes.	No.
6.	Short message service	160 characters of text support.	120 characters
7.	Carrier (channel) spacing	200 KHz	1.25 MHz
8.	Time slots (TS) is a frame full rate	8 TS	64 TS
9.	Time slots (TS) is a frame half rate	16 TS	128 TS
10.	Downlink frequency (Base station to mobile subscriber)	935-960 MHz	869-894 MHz
11.	Uplink frequency (Mobile subscriber to base station)	890-915 MHZ	824-849 MHz
12.	Frequency separation	45 MHz	45 MHz
13.	Radio interface	TDMA	CDMA
14.	Handoff	Hard handover	Soft handoff
15.	Modulation method	GMSK	QPSK / BPSK
16.	Multipath characteristics	Causes interference and destruction to service	Is used as an advantage.
17.	System capacity	Fixed and limited	Flexible and higher than GSM.
18.	Economy	Expensive	Due to many technological advantages, dimension of investment per subscriber is expected to be lower than GSM.

Q. 9 Explain GPRS architecture. **Dec. 16, May 17**

Ans. :

GPRS System Architecture

GPRS provides many services without restricting data rates of transmission. The service precedence namely high, low, normal, reliability, class, throughput and delay are determined by QoS profile. For voice calls the GPRS systems uses the GSM architecture. However, for packet data transmission GPRS includes a new set of network nodes called as GPRS Support Nodes (GSN). The main **function** of the GSN is to route and deliver the data packets between the Packet Data Network (PDN) and the mobile stations. GPRS supports two support nodes.

They are :

(i) SGSN (Serving GSN)

(ii) GCSN (Gateway GSN)

Scanned by CamScanner

Fig. 3.12 shows the GPRS system architecture.

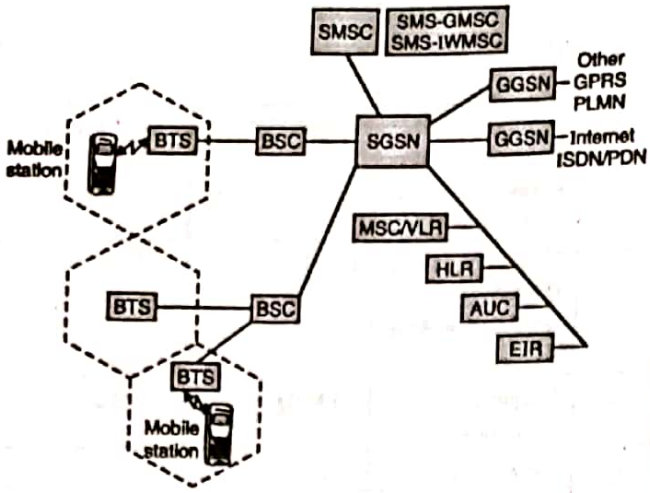


Fig. 3.12 : GPRS System architecture

AUC:	Authentication Center
BTS :	Base Transceiver Station
HLR :	Home Location Register
GGSN :	Gateway GPRS support Node
MSC :	Mobile Switching Center
PLMN :	Public Land Mobile Network
SMS - GMSC :	SMS Gateway MSC
SGSN :	Serving GPRS Support node
BSC :	Base Station Controller
EIR :	Equipment Identity Register
VLR :	Visitor Location Register
ISDN :	Integrated System Digital Network
PDN :	Packet Data Network
SMSC :	Short Message Service Center
SMS – IWMSC :	SMS interworking MSC

In addition to the new GPRS components (SGSN and GGSN), some of the existing GSM elements must be enhanced to support packet data. They are :

(I) Base Station Subsystem (BSS)

In order recognize and send packet data, the base station subsystem requires new functionalities that upgrade the BTS such that it supports transmitting the user data to the SGSN and between BTS and MS over radio network.

(II) Home Location Register (HLR)

For registering the GPRS user profiles and providing response to the GPRS queries originating from GSNs in regards to the user profiles the HLR also needs to be upgraded or enhanced.

(III) Mobile Station (MS)

The mobile station or the mobile phone for GPRS is different from that of GSM.

(Iv) SMS Nodes

SGSN support SMS transmission. The SMS-GMSCs and SMS-IWMSCs are enhanced. For efficient co-ordination of GPRS and non-GPRS services the MSC/VLR also needs to be upgraded.

(v) Serving GPRS Support Node (SGSN)

It functions similar to the GSM-MSC. The functions that GSM-MSC supports for voice are supported by the SGSN for packet data.

They comprise functions like

(a) Packet switching, (b) Data transfer

(c) Routing (d) Mobility management

(e) Logical link management

(f) authentication and security

(g) Billing /charging functions.

(h) Registration of new mobile subscribers and track of their location for a given service area.

The SGSN location register is responsible for storing the location information and user profiles of all GPRS users that are registered with SGSN. For acquiring the profile data of the subscribers it sends queries to the Home Location Register (HLR). SGSN is connected to the base station with frame Relay.

(vi) Gateway GPRS Support Node (GGSN)

A gateway GPRS support node (GGSN) acts as an interface between the external packet data networks and the GPRS backbone network.

The functions of the GGSN are identical to that of router in a LAN.

GGSN functions are

(a) To maintain the information related to routing for tunnelling the Protocol Data Units (PDUs) to the SGSNs service specific mobile stations.

(b) To convert the GPRS packets into correct packet data protocol (PDP) format for data networks like IP or X.25.

(c) Perform authentication

(d) Perform billing / charging

PDP sends these packets to the **PDN (packet data network)**. The packets received from PDN are converted to the GSM addresses of the destination user. The readdressed packets are sent to the SGSN in-charge of it. The GGSN needs to store the address of current SGSN and also the user address along with his/her location in the location register.

Scanned by CamScanner

Q. 10 Compare CDMA 2000 & W-CDMA.

Dec. 15, May 17

Ans. :

Comparison of CDMA 2000 and WCDMA

Parameter	CDMA 2000	WCDMA
Chip rate	1.2288 Mcps for 1 × RTT 3 × 1.2288 = 3.68 Mcps for 3 × RTT	3.84 Mcps
Frame duration	20 ms	10 ms
Carrier spacing	3.75 MHz	5 MHz
Frequency reuse factor	1	1
Power control frequency	800 Hz	1500 Hz
Frequency diversity	Multipath diversity with RAKE receiver.	Multipath diversity with Rake Receiver.
Packet data	Packet scheduling	Load based packet scheduling
Data modulation	QPSK	BPSK
Spreading factor	Higher	Lower
Base station synchronization	Synchronous	Asynchronous
Multiple Access	FDD MC CDMA	FDD – DS CDMA TDD DS CDMA
Duplexing	FDD and TDD	FDD and TDD
Backward compatibility	Backward Compatibility with IS – 95A and IS – 95B	Backward compatibility with GSM

Chapter 4 : Types of Wireless Networks

Q. 1 Write short note on wireless sensor networks.

Dec. 16, May 17

Ans. :

Wireless Sensor Networks

A **sensor network** is a network that translates the physical parameters like humidity, temperature, pressure direction etc. to a form that can be easily measured, analyzed and processed further.

Sensor networks are integrated into various different devices as well as machines. Hence, they provide many advantages. With the advances in wireless networking, Very Large Scale Integration (VLSI), Micro Electro-Mechanical Systems (MEMS) and embedded microprocessors; a new generation of **wireless sensor networks** is being developed. These networks are suitable for different applications like air traffic control, home automation, building automation, military applications, environmental applications, health care, process control, weather sensing, national border monitoring, video surveillance etc.

What is a Wireless Sensor Network ?

A **wireless sensor network** is a group of sensors that are used for monitoring as well as recording the environmental physical conditions like humidity, pressure, temperature, sound pollution, wind speed etc. and organizing the data gathered at some central location.

A wireless sensor network provides a bridge between the physical world and the virtual world.

The elements of a sensor network include :

1. A group of localized or distributed sensor.
2. A communication network.
3. A central location for clustering the data collected.
4. A group of computing resources at the central location.

A wireless sensor network is a network consisting of small sensor nodes that communicate amongst themselves with the help of radio signals and are deployed for sensing, understanding and monitoring the physical world. The wireless sensor networks demand in-network processing as data gathered is large in quantity. The wireless sensor networks have several applications ranging from smart homes, artificial intelligence, surveillance, vehicular and supply chain management applications.

Examples of previously used sensor networks are radar networks used for nationwide stations, air traffic control. However, these systems employ specialized computers as well as communication protocols and are expensive. This led the researchers to find less expensive and secure WSNs that need automation and are based on intelligent sensing. The WSNs that are developed nowadays are well planned.

Scanned by CamScanner

Sensor networking is a versatile area that combines artificial intelligence, database management, signal processing, networking, power management strategies etc. Various applications and protocols for these systems are being developed. Depending on the parameter to be monitored, different sensors are selected according to the applications eg. Passive infrared sensors are used for measuring infrared light that radiated by objects in vicinity.

The different sensors used as resistive sensors, electric sensors, magnetic sensors, piezoelectric sensors, acoustic sensors, optical sensors, ultrasound sensors, pressure sensors, humidity sensors, infrared sensors, radio frequency sensors etc. Nowadays the sensors are termed as **smart sensors**. This is because they are cheap, include multiple on board sensing elements that are linked to a central location. The sensor nodes also called as **motes**.

The different sensors communicate with each other through multihop short distance low power wireless links. Many network applications need many sensors that are deployed in inaccessible and remote areas. Hence, a wireless sensor network comprises thousands of sensor nodes that support sensing, on board processing, embedded computing communication and storage capabilities.

The key elements in the development of wireless sensor networks are :

(i) Limited battery power

(ii) Memory limitation

(iii) Limited computational capability

(iv) Cost

(v) Physical size of the sensor node.

The physical size of sensors ranges from several nanometers to millimetres i.e. their diameters can be in the order of 1-100 nm, 100-10,000 nm, 10-10000 μm or in millimetre-meter range. Today miniaturized sensors are used that are embedded on board. These sensors are called as **microsensors.** These microsensors with onboard processing and wireless communication interface can be used for studying and observing different parameters. The sensor nodes are single point elements. They also can be multipoint detection arrays.

Embedded network sensing includes many application specific sensors and onboard signal processing ability for manipulating data. e.g. Building, battlefield. Wireless sensor networks have low data range and small ranges. It uses a **low power low data rate technology.** The maximum data rate is 20-250 Kbps. The wireless networks are able to detect the structural faults in buildings, ships, homes, aircrafts. They can detect tsunami alert on coastlines. They are used for battle field surveillance, detecting the state of atmosphere etc.

Wireless sensor networks are in developing phase. Extensive research is done in this field by different equipment manufacturers, companies. In the next few years a majority of devices will support sensing, processing and communicating i.e. supporting wireless sensor applications. As an example consider a basic wireless sensor network that comprises of many sensors those are distributed in a region or area. The sensors sense the physical parameter, digitize it, process it and with a transmitter they transmit the data.

This data is passed to the node 2, and from node 2 to node 3 and so on till it reaches to the **gateway of the network.** The area is also called patch network. This data is sent from the gateway to the user through any communication medium like satellite, wireless, cables or through internet. The area covering all these sensor nodes is called as **patch network** as shown in Fig. 4.1.

The sensor nodes can be similar or dissimilar. The sensor have specifications so that they can be used for different applications. The sensor node can have different processing powers, different roles. The sensor is node is a low power device. So the power transmitted is also low. The sensor nodes are scattered in a region so they must be of small size and also they must be cheap.

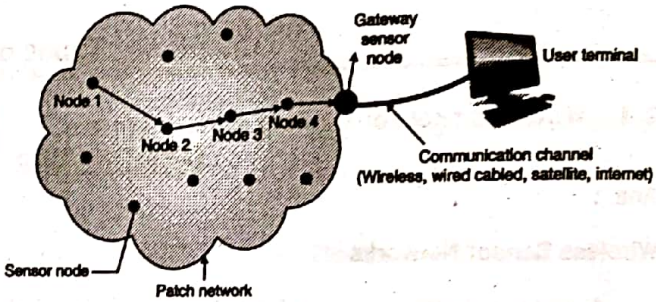


Fig. 4.1 : Basic wireless network

WSNs are analogous to a single thread. It is weak and can easily break. But when many threads are all put together cooperating with each other to stick together it becomes a strong rope. This is the basic concept i.e. nodes of wireless sensor networks. They have a large number of very small resource devices that cooperate, collaborate, with each other to perform a single task for which the network is designed.

In wireless sensors networks, there are many sensors (senders) that are sending data to the gateway. This is in contrast to a computer network where there is one sender and one or many destinations or recipients. Thus, wireless networks are special kind of networks where there are **many sensor nodes** (sensors). **Special routing protocols** need to be developed for wireless sensor networks than computer network protocols used.

Scanned by CamScanner

WSN requires new innovative approaches and poses very big challenge to the network designers. Currently more stress is on developing wireless sensor networks with low power communication, low cost on node processing, self routing protocols. For the development of such WSNs the radio architecture should be correctly selected. Research is carried on how energy or power must be efficiently utilized i.e. enhancement of the energy efficiency.

Maximation of network and node lifetime, is the main objective of the design of the wireless sensor network. These objectives are achieved using three methods. They are :

(i) Processing the data locally or network in order to decrease the data volume.

(ii) Operating at low duty cycles.

(iii) Using multihop communication networks. In multihop network data is transmitted in hops. Every sensor node behaves like a repeater. This reduces the power required for transmission and also the range to be covered.

Wireless Sensor Network comes under W-PAN. It has low data rate and its range is also small i.e. wireless sensor networks use low power low data rate technology. The network designers ruled out Wi-Fi standard as more bandwidth than that needed for sensors. Bluetooth (IEEE 802.15.1) technology was also ruled out as it is complex and expensive.

ZigBee Standard (IEEE 802.15.4) is designed for such low power low data rate applications. ZigBee standard in used in contrast to Bluetooth, Wi-Fi and Utra Wide Band (UWB) for wireless sensor networks. ZigBee (IEEE 802.15.4) has small data rates from 20-250 kbps at ranges 30 to 200 ft. The signals from different sensors do not have high frequency component, so we don't need high bandwidth and high data technology for these signals. Hence, ZigBee standard is designed for such low data rate WSN applications that allow sensors to transfer the data in a standardized fashion.

Wireless sensor network is a group of specialized transducers or sensors that have a communications infrastructure and are intended to monitor and record the conditions at diverse locations. The commonly monitored parameters are pressure, temperature, humidity, wind direction, vibration intensity, sound pollution etc.

Q. 2 What are the advantages and disadvantages of Wireless Sensor Networks ?

Ans. :

Advantages of Wireless Sensor Networks

1. The wireless sensor networks work efficiently under harsh conditions.
2. The wireless sensor networks can be deployed on a large scale.
3. The wireless sensor networks are applications oriented i.e. they are developed according to the application.
4. The wireless sensor networks support embedded processing and onboard storage.
5. The wireless sensor networks can be accessed through a centralized monitoring system.
6. The WSNs can be easily implemented. Its implementation cost is less than that of wired networks.
7. They avoid a lot of wiring.
8. The wireless sensor networks are suitable for monitoring unreachable areas like rivers, mountains, rural areas etc.
9. The wireless sensor networks are robust and scalable.
10. The wireless sensor nodes have ability to compensate for node failures.
11. The wireless sensor networks have a communication infrastructure.
12. A wireless sensor network can accommodate multiple nodes at a time.

Disadvantages/Limitations of Wireless Sensor Networks

1. They are low communication speeds as compared to wired networks.
2. It is less secure hackers can easily hack the network.
3. Because of limited resources, limited size, limited memory it is difficult to design a routing method for WSN.
4. WSN is affected by the surrounding elements.

Q. 3 Give the applications of Wireless Sensor Network.

Ans. :

Applications of Wireless Sensor Network

Wireless Sensor Network (WSN) supports a wide variety of applications. Some of the applications that use WSN are :

1. Home automation
2. Environment monitoring system
3. Inventory management
4. Healthcare systems
5. Military systems
6. Air traffic control
7. Building automation
8. Industrial monitoring and control
9. Tsunami monitoring
10. Forest fire detection
11. National security applications

Scanned by CamScanner

12. Consumer electronics (TV, CD/DVD, LCD, VCR)
13. Military surveillance
14. Metropolitan applications (traffic, automatic tolls, fire)
15. Earthquake detection
16. Detecting structural faults in ships, buildings, aircraft
17. Electricity load management
18. Habitat monitoring
19. Lighting control
20. Battlefield management
21. Supermarket management
22. Volcanic eruptions
23. Vehicle tracking systems
24. Nuclear threat detection systems
25. Robots

Chapter 5 : Wireless Local Loop (WLL)

Q. 1 What is WLL ? Explain wireless local loop technology.

Dec. 10, May 12, Dec. 12, May 13, Dec. 14

Ans. :

Wireless Local Loop (WLL)

With the fast growth of internet the demand for broadband internet and computer access from homes, offices and businesses throughout the world has increased. Specifically, in the developing nations there is need for reliable, inexpensive, usable broadband connectivity. A single broadband connection can provide all the necessary telecommunication services like telephone, radio, fax and internet. For deploying a broadband connection fixed wireless access systems are well suited. Modern fixed wireless systems are generally designed at microwave or millimetre frequencies in the 28 GHz band and higher.

At these frequencies, the wavelengths are very small. In Fixed Wireless Access Systems (FWA), the Wireless Local Loops (WLL) are popular. WLL is also called as fixed wireless loop. The **function** of the WLL systems is to make primary access to the telephone networks. It supports subscribers of fixed and known locations. The WLL system enables connectivity with the Public Switched Telephone Network (PSTN). It uses radio connectivity instead of wired cable. It can be for full system or partially between subscriber and switch set up alone. Pure radio or hybrid of radio and wired cabling is used for establishing the connection. The microwave wireless links can be used to generate a Wireless Local Loop (WLL). It is a milestone in telecommunication era and exists between the central office (CO) and the individual residences near the CO. Fig. 5.1 shows a simple configuration of wireless local loop.

In the developed countries, the copper or fiber optic cables are installed at homes, offices and businesses in buildings. However, in the developing countries it is difficult to install cables. The wireless links can be deployed in a couple of hours. In the WLL systems there are two concepts namely NWLL and BWLL.

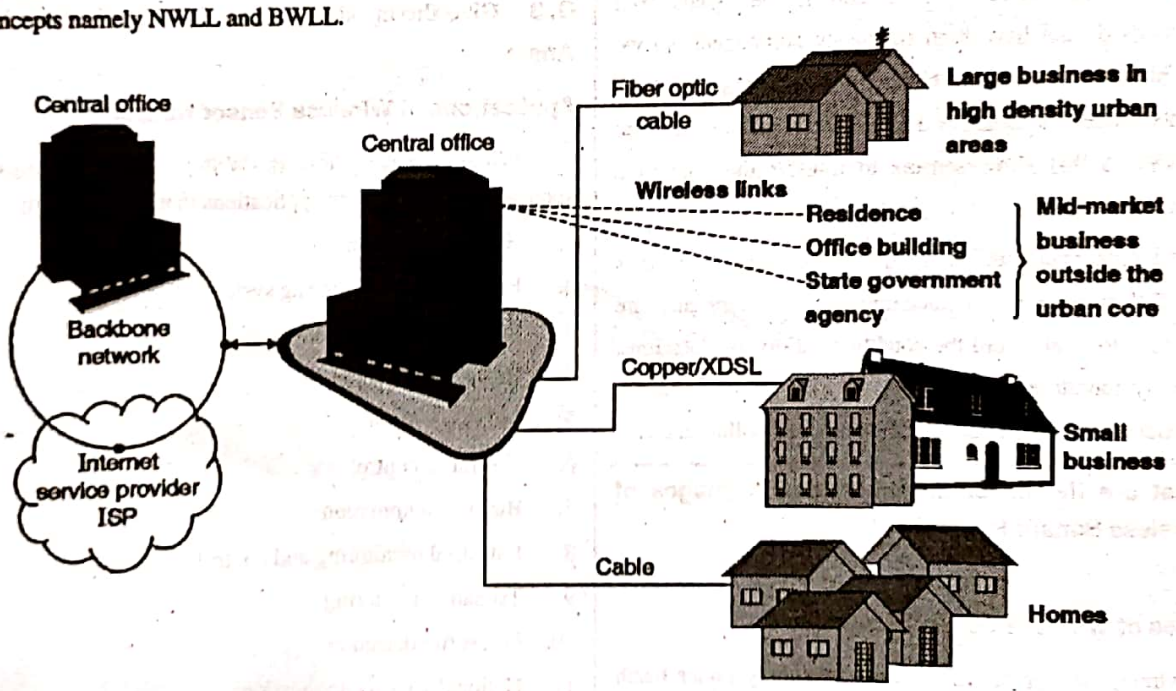


Fig. 5.1 : Simple configuration of Wireless Local Loop (WLL)

Scanned by CamScanner

NWLL (Narrowband WLL) is used to replace conventional telephone systems and BWLL (Broadband WLL) is used to produce higher speed data and voice services. Thus, WLL is the best system to handle high data traffic in the local loop systems.

The advantages of the WLL are :

i) The cost of wireless equipment is less, once paid no additional costs are required whereas the fibre optic and copper cables need to be leased from the service provider on monthly basis.

ii) Wireless equipments can be installed in a couple of hours.

iii) They have good scale of installation.

The WLL systems are based on the Personal Communication Systems (PCS) like mobile technologies like W-CDMA, GSM, PDC etc. WLL alongwith these technologies produces the above advantages. The capacity requirement of WLL is different from that of the capacity need of fixed WLL system. In a fixed system the capacity is provided to meet subscribers of known numbers but it is no so in mobile wireless as it has to meet the traffic in worst cases.

WLL system must have features like :

i) They should provide better Quality of Service (QoS).

ii) They should be compatible with other cellular technologies.

iii) They should have complete scalability to meet the traffic requirements.

For fixed subscriber considerations the terminal under WLL has to be oriented for greater signal in their installation. The fixed WLL needs comparatively less transmission power and it uses directional antennas for its functionality.

Q. 2 Draw and explain the main components of Wireless Local Loop (WLL) Architecture.

May 16, Dec. 16, May 17, Dec. 17

Ans. :

WLL System Architecture

The WLL architecture comprises three units.

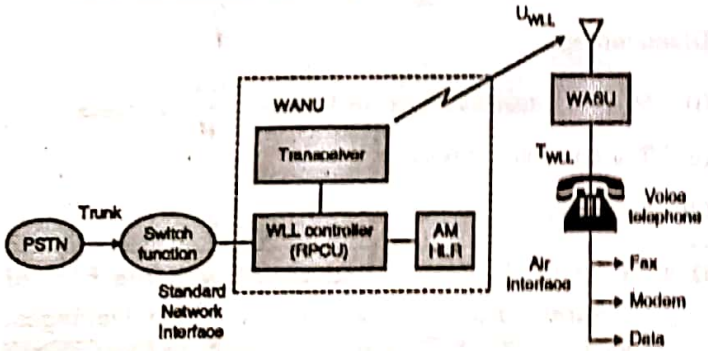


Fig. 5.2 : WLL system architecture

1. Wireless Access Network Unit (WANU)

It comprises of many radio ports (RP) or base station transceivers, a radio port control unit (RPCU), home location register (HLR) and access manager (AM). The WANU must be able to provide radio resource management for authentication and air interface privacy, operation and maintenance, switching functions, billing etc. WANU also provides wide area roaming.

The functions of WANU are :

(i) It provides radio resource management.

(ii) It provides authentication and air interface privacy.

(iii) It consists of a protocol that does conversion and transcoding of data as well as voice.

(iv) It does registration of the subscriber units over the air.

(v) An internetworking function is present that supports facsimile and voice band data.

(vi) To provide billing, maintenance and routing.

2. Wireless Access Subscriber Unit (WASU)

The wireless access subscriber unit (WASU) is responsible for providing an air interface to the network. This interface provides facilities like :

(i) Voice and data support.

(ii) Authentication check

(iii) Operation and maintenance

(iv) Transcoding and protocol conversion

(v) Information about fax and computer data

(vi) System power supply back up

The U_{WLL} interface uses standard air interfaces for GSM.

The T_{WLL} interface is RJ = 11, RJ = 45 etc.

3. Switching Function

The switching function (SF) in WLL is a digital switch. This switch can be with or without advanced intelligent network (AIN) capability. The newer WLL systems support advanced intelligent network capability. It can comprise ISDN (integrated services digital network) algorithms or a mobile switching centre (MSC). A_{WLL} is the interface between the switching function and wireless access network unit. The data transmission between the switching function and wireless access network unit can be done using cable, microwave link, leased line or optical links.

Q. 3 Describe four major technologies for WLL systems. What are the advantages and disadvantages of these approaches.

Dec. 11, May 16

Ans. :

WLL Technologies

The WLL system can be based on following technologies.

Scanned by CamScanner

1. Cellular Based System

The cellular based WLL systems are used for expanding the telephony services in the frequency ranges 450 MHz, 800 – 900 MHz, 1.5 GHz, 1.8 – 1.9 GHz.

The cellular based systems provide features like :

(i) Medium circuit quality

(ii) Medium subscriber density

(iii) High operating power

(iv) Wide range

It provides fixed wireless access, mobility and can be easily deployed. They are designed with Rayleigh fading channel with 5-10 ms delay spread. The IS-136, IS-95 (CDMA), GSM, TR-95 are being considered for WLL. HNS E-TDMA was the first cellular based system deployed for WLL.

Advantages

(i) They provide fixed wireless access and mobility.

(ii) They can be rapidly deployed in rural and urban areas.

(iii) They provide large power.

(iv) They provide large operating range.

(v) They provide medium circuit quality and medium subscriber density.

Disadvantages

(i) They are not recommended for deployment indoors and in picocells.

(ii) Air interface is complex e.g. GSM uses FEC (forward error correction), burst interleaving and equalization inorder to correct the fade rates.

(iii) The user bandwidth is limited.

2. Satellite Based System

The satellite based WLL systems are used for providing telephony services in the rural area, islands and other different isolated areas. They can be designed for WLL applications or mobile satellite systems.

They provide features like,

(i) Low bit rate for voice and data

(ii) Low cost mobile terminals.

(iii) It provides quality and grade of service for WLL applications.

Satellite based systems are designed with Rician fading channel with K > 9 dB. HNS telephony earth station (TES) technology is developed as satellite based technology for WLL. The mobile satellite system comprise Globalstar, Iridium, Odyssey, American mobile satellite corporation (AMSC), Inmarsat, International circular orbit (ICO system), Thuraya.

Advantages

1. They provide telephony to remote areas of the world, where landlines are not cost effective or emergency backup is required.
2. They provide low cost mobile terminals.
3. They provide low bit rate for data and voice applications.

Disadvantages

1. The number of satellites and propagation delay put restrictions on the system design.
2. Handover capability is needed e.g. LEO, MEO (Low and medium earth orbit) satellites are in motion relative to the earth's surface, so they need handover capability for all fixed and cellular applications.

3. Fixed Wireless Access System (FWA)

The fixed wireless access WLL systems are particularly for fixed wireless applications. In different zones they cover the telephone area from the PSTN switches. In rural areas the connections are provided at remote ends of rural link to the clients.

Advantages

(i) Less expensive

(ii) It can be easily installed.

(iii) The installation time need is less.

Disadvantage

(i) Limitation on toll-quality voice and signaling transparency.

4. Low-tier PCS or Microcellular Based Systems

The microcellular based WLL systems work at frequencies 800 MHz, 1.5 GHz, 1.8 GHz and 1.9 GHz. They use Rayleigh fading with delay spread upto 500 ns.

Advantages

(i) High subscriber density

(ii) Low power

(iii) High circuit quality

Disadvantages

(i) More base stations are required to cover an service area.

(ii) Transmission cost is more.

(iii) Small range.

Q. 4 Explain the MMDS and LMDS with the help of diagram. State its advantages and disadvantages.
Dec. 10, May 12, Dec. 14, Dec. 15, May 16, Dec. 16, May 17

Scanned by CamScanner

Ans. :

1. Local Multipoint Distribution Service (LMDS)

It is a broadband method used for delivering data, voice, internet including video services in 25 GHz frequency and frequencies greater than that. The propagation characteristics are well defined in the spectrum.

The LMDS system has network configuration similar to the cellular networks. In US a frequency of 1.3 MHz bandwidth is allocated for LMDS for delivering broadband services. The propagation characteristics of the signals reduces the potential coverage area at one cell site.

The range of LMDS transmitter can be upto 8 km incase of metropolitan regions. In LMDS the signals are transmitted by point to multipoint or broadcast methods. The services offered by LMDS method is dependent on the operators choice. Also, the return path from subscribers to base station is of point-to-point transmission method. The frequency bands allotted by US FCC for fixed wireless communication are shown in Fig. 5.3.

Frequency in GHz
2.150 – 2.162
2.400 – 2.4835
2.596 – 2.644
2.650 – 2.656
2.6620 – 2.6680
2.6740 – 2.6800
⋮
27.5 – 28.35
29.1 – 29.25
31.075 – 31.225
31.225 – 31.300
38.600 – 40.000

Fig. 5.3 : Frequency bands of wireless communication

An application for LMDS is in a local exchange carrier (LEC) network. Fig. 5.4 shows a typical network configuration in which the LEC has a wide bandwidth Asynchronous Transfer Mode (ATM) or Synchronous Optical Network (SONET) backbone switch that is capable of connecting hundreds of megabits per second of traffic with the internet, the PSTN or its own private network.

As long as a line-of-sight path is present, LMDS will allow the local exchange carrier to install wireless equipment on the customer premises for broadband connectivity. The factors like rain, snow, hail can affect the channel gain between the transmitter and receiver.

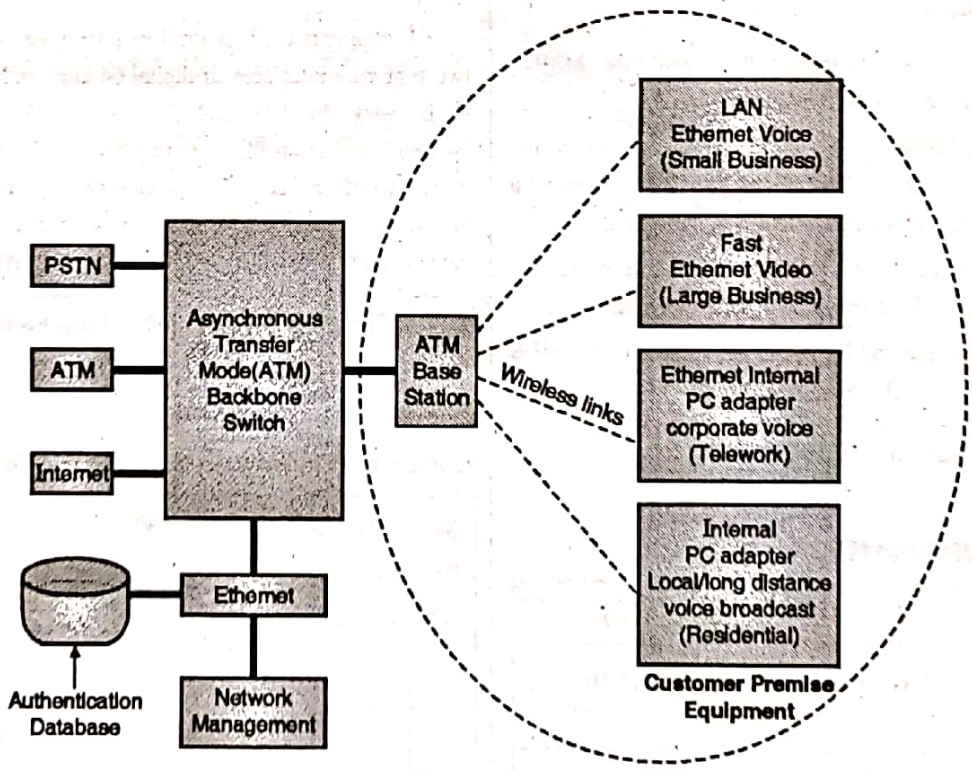


Fig. 5.4 : Wireless Local Exchange Carrier (LEC) using ATM distribution

Scanned by CamScanner

Advantages of LMDS system

i) LMDS systems can be easily deployed.

ii) The systems are cost effective. Network management, maintenance and operation is possible.

iii) The system data rate is very high.

iv) According to customer demands, the architecture is scalable.

Disadvantages of LMDS system

(1) The **drawback** of LMDS is that it needs a large number of base stations because of its short range of operation from the base stations.

(2) The LMDS services include voice, video, data signal as different combinations.

2. Multichannel Multipoint Distributed Service (MMDS)

The FCC has assigned five bands of frequency in U.S. in the range from 2.15 GHz to 2.68 GHz for fixed wireless access that uses multichannel multipoint distributed service (MMDS). In 1970's two licensed frequency bands were allocated for television broadcasting. They are called Multipoint Distribution Service (MDS). Then the FCC enhanced the frequency band allocations as allowed Multichannel MDS (MMDS) services.

However, there is a constraint regarding the service area in km and transmitted power as the FCC did not allow the power transmitted of the base station (BS) serving and area that is more than 50 km. It is a drawback of the MMDS. The MMDS has several advantages when compared with LMDS.

Advantages of MMDS

i) Because of larger wavelength of the signal, the MMDS signals are susceptible to the rain absorption.

ii) Compared to LMDS signals, the wavelengths (λ) of the MMDS signals are larger. This allows the signals to travel a long distance any without power losses in the signal.

iii) Base station cost needed for MMDS is lower as it consists equipments that can be operated at low frequencies.

Thus, the MMDS method has more advantages than LMDS in Wireless Local Loop (WLL) technology.

Q. 5 Compare LMDS and MMDS.

Ans. :

Comparison of LMDS and MMDS

Parameter	LMDS	MMDS
Frequency band	27.5 – 31.3 GHz	2.15-2.68 GHz
Bandwidth	High	Low
Coverage radius	1 – 4 km	4-6 km
Subscriber data rate	1 Mbps	300 Kbps
Cost	High	Low
Atmospheric losses	High	Low
Use	Commercial applications	Domestic applications
Wavelengths	Less	More

Q. 6 How interfaces are done between WLL to the PSTN ? **May 13, Dec. 13**

Ans. :

WLL Interface to the PSTN

We know that the WLL subscribers are linked to the system through radio to the network of base stations. A WLL system can be connected to the PSTN through direct connection to the local exchange or with a switch. The WLL system can depend on PSTN to do all the switch functions. An analog or digital interface is required for connecting PSTN switches directly to the WLL system.

If copper is used for local loop then the switches can provide two-four wire interfaces. If digital 64 kbps PCM interface is used it is easy to use and low cost. The ETSI (European Telecommunication Standard Institute) has standardised V5.2 as a digital interface between a private branch exchange and WLL system. For matching switches with digital interface different vendors have developed digital interfaces for WLL systems.

Q. 7 Compare wireless local loop Vs wired Access. **May 11**

Ans. :

Comparison between WLL and Wired Networks

Sr. No.	Parameter	WLL	Wired network
1.	Connection	WLL systems connects users to PSTN using radio signals.	In wired system users are connected to PSTN through copper wires between the users and switches.

Scanned by CamScanner

Sr. No.	Parameter	WLL	Wired network
2.	Cost	Less expensive	More expensive
3.	Deployment	Deployment is easy and can be quickly done	Difficult as many cables need to installed.
4.	Selective installation	Radio units can be installed only for users who need service at a given time.	In wired system, cable laid for every subscriber in the area.
5.	Maintenance	Less as compared to wired systems.	More
6.	Reliable	Less reliable	More reliable
7.	Speed and bandwidth	Low	High
8.	Security	Weak	Good
9.	Mobility	Outstanding	Limited
10.	Fading	Less	More
11.	Interference	Less	More
12.	Installation time	Less	More

Chapter 6 : Wireless Local Area Networks

Q. 1 Explain working of wireless LAN.

Dec. 12, May 17

Ans. :

WLAN

There is need for developing new networking methods for the personal communication systems. The networking methods must include mobile, data and the voice users who roam in the buildings or throughout the cities. The FCC assigned a 300 MHz of unlicensed spectrum in 1987, for the ranges 5.150 – 5.350 GHz and 5.725 – 5.825 GHz for Industrial Scientific and Medical (ISM) bands. The spectrum was allocated for supporting low power license free spread spectrum data communication. The allocation is referred to as **Unlicensed National Information Infrastructure (UNII) band.**

With the provision of license free spectrum allocation, the FCC hoped to encourage the development of spread spectrum knowledge, spread spectrum equipment and the ownership of individual WLANs and other short range low power devices that can support computer communications in the workplace.

In 1987, the IEEE 802.11 Wireless LAN working group was developed. It was developed for the standardization of spread spectrum WLANs for use in ISM bands. In the late 1990s, the WLAN gained popularity because of its ability to handle a number of applications like inventory control. These applications find advantage of mobility associated with the wireless LANs.

In 1997 the IEEE 802.11 WLAN was standardized. It specifies the physical and MAC layers for operation of wireless LAN and addresses the **Direct Sequence Spread Spectrum (DSSS)** and **Frequency Hopping Spread Spectrum (FHSS)** access methods for the radio propagation. It supports 2 Mbps user data rates. It specifies support for synchronous as well as asynchronous data transfers.

In 1999, the 802.11b standard was approved. This standard provides user data rate capabilities of 11 Mbps, 5 Mbps in addition to earlier 1 Mbps and 2 Mbps data rates of IEEE 802.11. Fig. 6.1 shows that both FHSS and DSSS methods were used in IEEE 802.11 standard. The FHSS proponents of the IEEE 802.11 have formed the home RF standard that supports the frequency hopping equipment. An FH-SS standard called Home RF 2.0 was developed in 2001. It supports data rate of 10 Mbps.

The IEEE 802.11a standard provides a data rate upto 54 Mbps in 5 GHz band. The DSSS IEEE 802.11b standard is called **Wi-Fi (Wireless Fidelity)** by Wireless Ethernet Compatibility Alliance (WECA). IEEE 802.11g is developing complimentary code keying orthogonal frequency division multiplexing (CCK-OFDM) standards in 2.4 GHz (802.11b) and 5 GHz (802.11a) bands. It will support roaming and the use of dual bands for the WLAN networks. Also, it will be compatible with 802.11b.

The FHSS and DSSS types of WLANs need to operate in the same unlicensed bands that contain cordless phones, baby monitors, Bluetooth devices and other WLAN users. The IEEE 802.11 is the first WLAN standard and so far the only one that has a secured market. Compared with wired LANs, wireless LANs operate in a difficult medium for communication and they need to support mobility and security.

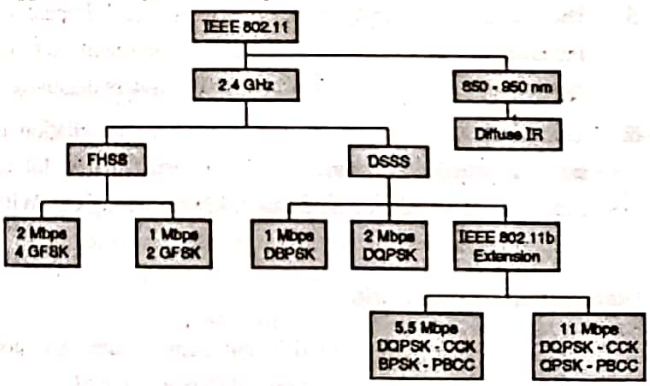


Fig. 6.1 : IEEE 802.11 WLAN standard

Scanned by CamScanner

Table 6.1 lists the channel allocations for DSSS and FHSS WLANs in the 2.4 GHz band.

Table 6.1 : IEEE 802.11b channels for DSSS and FHSS WLAN standards

Country	Frequency Range GHz	DSSS Channels Available	FHSS channels Available
United states	2.4 – 2.4835	1 through 11	2 through 80
Canada	2.4 – 2.4835	1 through 11	2 through 80
Japan	2.4 – 2.497	1 through 14	2 through 95
France	2.4465 – 2.4835	10 through 13	48 through 82
Spain	2.445 – 2.4835	10 through 11	47 through 73
Remainder of Europe	2.4 – 2.4835	1 through 13	2 through 80

All the WLANs are manufactured to operate on a particular channel. They are assigned a channel by the network operator when the system is initially installed. Channelization method is used by the network installer so as to avoid interference and degraded performance.

Q. 2 What are the advantages, disadvantages and applications of WLAN.

Ans. :

Advantages of WLAN

1. **Quicker deployment :** It is easier to add or move subscribers or workstations.
2. **Easy access :** The WLANs installation is fast and easy. It reduces the need of LAN wiring through ceiling and walls.
3. **LAN extension :** They provide connectivity in areas where it is difficult to install cables.
4. **WLAN mobility :** The subscribers can access the network from anywhere within the range of access point.
5. **Increased productivity :** They have a direct impact on increase in productivity because of minimum set up requirements and centralised access to the system database.
6. **Cost effective :** The initial cost needed for installation is same as wired LAN. However, after installation a lot of expenses are saved on maintenance, labour, wiring etc. With modem techniques, the WLAN installation cost is reduced.

Disadvantages of WLANs

1. The WLAN devices from different manufactures are not compatible as every network uses a different standard.
2. Because of limited bandwidth and data rates, WLAN cannot download large data files speedily. Also they cannot support real time applications or video conferencing.
3. The wireless medium is insecure leading to jamming and vulnerable attacks.
4. There can be interference in the wireless link because of traffic, errors, rains make data transmitted unreliable.
5. It is slow, inefficient and unreliable in comparison with the wired networks.

Applications of WLAN

1. It can be used to extend the range of existing LAN network to cover a particular area.
2. It can be used as an alternative to wired LAN.
3. It supports more number of users.
4. It can wirelessly connect in organizations, nearby buildings by establishing a link between them.

Q. 3 Write note on wireless LAN Topologies. **Dec. 10, Dec. 13**

Ans. :

WLAN Topologies

WLAN can be constructed with the following topologies :

1. Peer-to-peer topology (adhoc technology)
2. AP based technology
3. Point-to multipoint bridge topology.

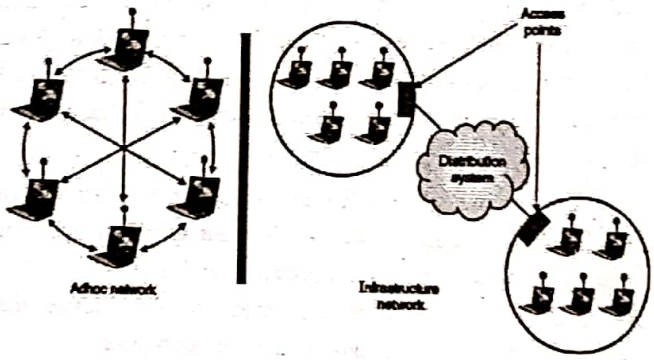


Fig. 6.2 : Peer-to-peer topology (Adhoc network)

In the peer to peer topology as shown in Fig. 6.2 subscribers or users in a cell can directly communicate with each other. Fig. 6.3 shows the AP based technology. It employs APs (access points) for routing traffic. The access points allows the users to communicate with other devices on the network.

The devices can be wired or wireless. WLAN extends the connectivity of wired LAN systems by providing connectivity to new mobile devices. In point to multipoint bridge topology, the wireless bridges from one location connect to other location that are nearby or far apart.

Scanned by CamScanner

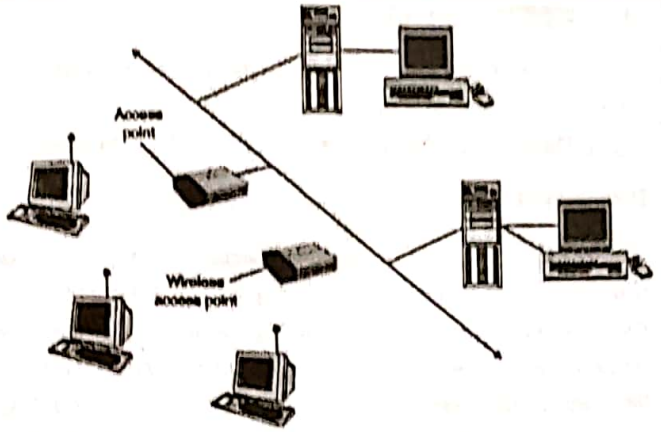


Fig. 6.3 : Access point based topology

Q. 4 With a neat diagram explain the IEEE802.11 system architecture.

Dec. 10, May 13, Dec. 14, Dec. 15, May 16, Dec. 17

Ans. :

IEEE 802.11 Architecture

IEEE 802.11 is the prominent standard for WLANs. It has been adopted by many manufactures. Later developments of this standard is 802.11b commonly called as Wi-Fi (Wireless Fidelity).

The **advantages** of IEEE 802.11 architecture are as follows :

1. It is flexible and support small as well as large networks.
2. It provides power saving and long battery life of the equipments without loss of network connection.
3. Robust model for industries.
4. It provides user mobility.

Under the IEEE 802.11, the two network architectures defined are as follows :

1. **Infrastructure network :** It is a network architecture that supports communication between the wired devices and wireless customers. An access point (AP) is needed for sending data from wireless medium to wired medium.
2. **Point-to-point (Adhoc) Network :** It does not require an access point. It connects all the devices in the network wirelessly. It does not allow access to a wired network.

IEEE 802.11 supports three types of topologies.

(a) Independent Basic Service Set

It is the basic building block of wireless LAN. It is an independent network called as standalone network or adhoc network. It does not have an access point (AP). As shown in Fig. 6.4 no node behaves as a server. The stations communicate with each other wirelessly or in adhoc manner. The IBSS covers a small range. It is created for few stations and some specific application.

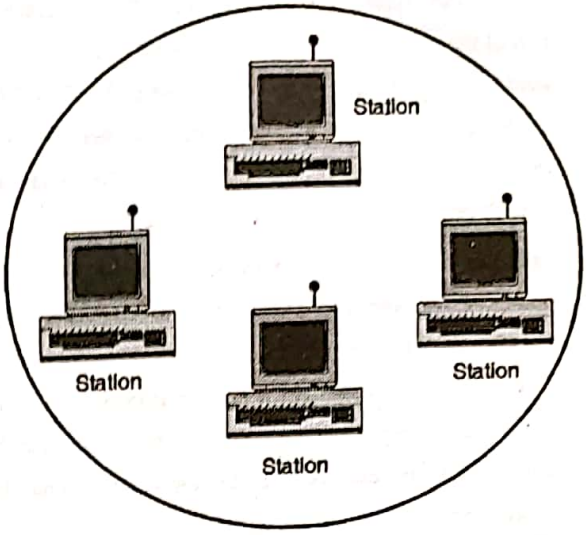


Fig. 6.4 : IBSS configuration

(b) Basic Service Set

It uses an access point. It is made of stationary or moving wireless stations and a central base station called **access point (AP).**

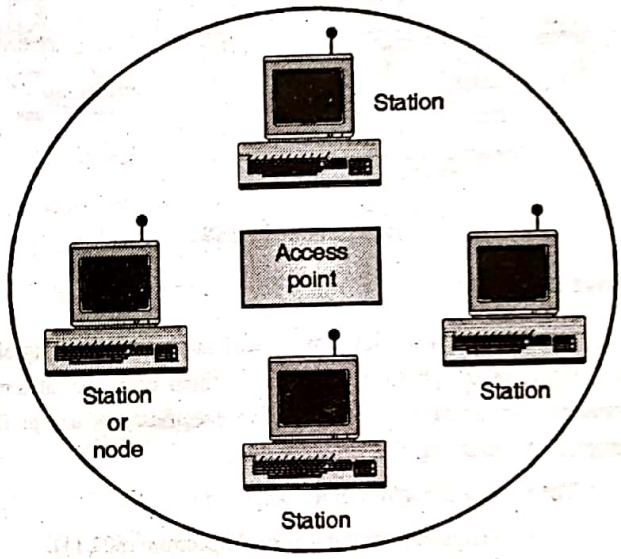


Fig. 6.5 : BSS configuration

The access point connects multiple WLAN devices.

(c) Extended Service Set

An Extended Service Set (ESS) consists of two or more BSSs with APs. The BSSs in this system are connected to each other via a **distribution system** which is generally a wired LAN as shown in Fig. 6.6. The distribution system connects the APs to each other. The distribution system can be any type of LAN such as Ethernet.

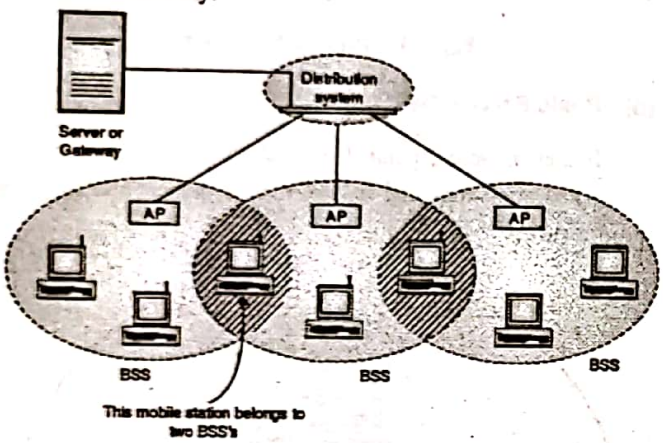
Thus ESS contains two types of stations :

1. Mobile stations
2. Stationary of non-moving stations.

Scanned by CamScanner

Out of these, the non-moving stations are the APs which are a part of the wired LAN. Whereas the mobile stations are those contained in the BSS. Fig. 6.6 shows an ESS. The BSSs are connected to each other to form a network called **infrastructure network**. In such networks the stations close to each other can communicate without taking help of AP.

But if two stations located in two different BSS wish to communicate with each other, than they have to do so through APs. This type of communication is very similar to that in the cellular communication. The BSS acts as a cell and AP as base station. As shown in Fig. 6.6 it is possible that a mobile station can belong to more than one BSSs simultaneously.



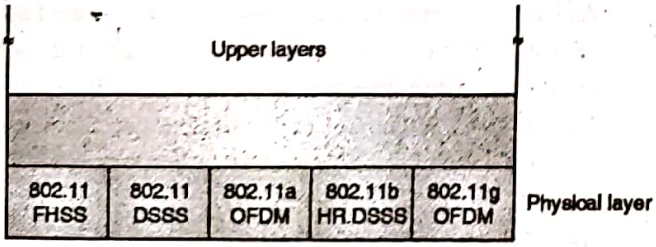
(G-381)**Fig. 6.6 : ESS**

Physical Layer

IEEE 802.11 has defined the specification for converting bits to a signal in the physical layer one of them is in the infra-red frequency spectrum and the other five specifications are in RF range as shown in Fig. 6.7.

The five specifications in RF range are :

1. FHSS - Frequency Hopping Spread Spectrum (802.11).
2. DSSS - Direct Sequence Spread Spectrum (802.11)
3. OFDM - Orthogonal Frequency Division (802.11 a)
4. HR-DSS-High Rate-DSSS (802.11 b).
5. OFDM (802.11 g)



(G-382)**Fig. 6.7**

(A) IEEE 802.11 FHSS

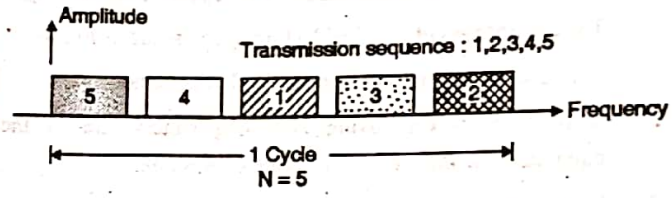
The IEEE 802.11 describes a method called FHSS i.e. Frequency Hopping Spread Spectrum for conversion of bits into a signal. The frequency band used for this is 2.4 GHz ISM band.

Principle of FHSS

In FHSS, the sender sends one frequency for a short period of time. Then hope to another carrier frequency and transmits it for the same amount of time. Then it hops again to a new carrier frequency and transmits it for the same duration and so on. In all there are N-such hoppings in one cycles as shown in Fig. 6.8. The cycle repeats itself after N-hoppings. The bandwidth of FHSS signal is equal to NB Hz where B is the bandwidth of the original signal that is being converted to FHSS signal.

The techniques of spreading used in FHSS makes it difficult for an unauthorised person to understand the transmitted data. The frequency of allocated bands in FHSS is decided with mutual agreement between the sender and the receiver. The frequency band by FHSS is 2.4 GHz ISM (industrial, scientific and medical). This band is divided in 79 equal subbands of 1 MHz each.

The hopping frequency is selected by a pseudorandom number generator.



(G-383)**Fig. 6.8 : Principle of FHSS**

The modulation techniques used is FSK (Frequency Shift Keying) at 1 M baud /sec. And the data rate is 1 or 2 Mbps.

(B) IEEE 802.11 DSSS

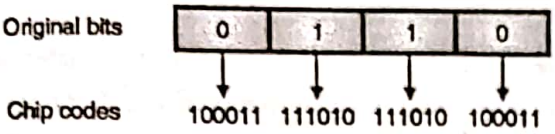
IEEE 802.11 has defined the DSSS i.e. direct sequence spread spectrum technique in order to convert the bits into signal. The DSSS also uses the same frequency band as that of the FHSS i.e. 2.4 GHz. ISM band.

Principle of DSSS

In DHSS, each bit being sent by the sender is first converted into a group of bits called as the **chip code**. The time required to send each chip code should be equal to the time period of the original bit in order to avoid the buffering. Let N represent the number of bits in each chip code. Then the data rate of DSSS would be equal to N times the data rate of the original signal. Fig. 6.9 demonstrates the principle of DSSS. DSSS even though similar to CDMA is not a multiple access method. The bit sequence used in DSSS uses the entire frequency band of 2.4 GHz (ISM band). DSSS uses the PSK (Phase Shift Keying) as its modulation technique at 1 M baud /s and the data rate is 1 or 2 Mbps.

Scanned by CamScanner

Bit	Chip code
0	100011
1	111010



(G-384)Fig. 6.9 : Principle of DSSS

(C) IEEE 802.111 a OFDM

OFDM stands for orthogonal frequency division multiplexing. It is used by IEEE 802.11 a as the signal conversion technique.

Principle of OFDM

The basic principle of OFDM is same as that of FDM. But the major difference is that all the frequency subbands are used by one source at a given time. OFDM uses the 5 GHz ISM band for its operation. This band is subdivided into 52 subbands. Out of these 52 subbands, 48 subbands are used for sending 48 groups of bits at a time and the remaining 4 subbands are used for sending the control information.

These subbands can be used randomly in order to increase the security of transmitted data. The type of modulation used by OFDM is PSK (Phase Shift Keying) and QAM (Quadrature Amplitude Modulation). The data rates are 18 Mbps (PSK) and 54 Mbps (QAM).

(D) IEEE 802.11 b HR- DSSS

HR-DSSS is the short form for high speed direct sequence spread spectrum. IEEE 802.11 b uses HR-DSSS method for signal generation. It uses the frequency band of 2.4 GHz (ISM band). HR-DSSS is conceptually very similar to that of a DSSS techniques. The only difference is the encoding method used. HR-DSSS uses a method called Complementary Code Keying (CCK) which encodes 4 or 8 bits of original data into one CCK symbol.

The HR-DSSS needs to backward compatible with DSSS. Hence HR-DSSS defines four data rates : 1,2,5.5 and 11 Mbps. The 1 and 2 Mbps data rates are allocated for the same type of modulation as used for DSSS. The modulation used for 5.5 Mbps is BPSK and the transmission rate is 1.375 Mbaud / sec with a 4 bit CCK encoding. The 11 Mbps data rate is assigned for QPSK type modulation and the corresponding transmission rate is 1.375 Mbaud/s. It uses 8 bit CCK encoding.

(E) IEEE 802.11g OFDM

It is a new specification using OFDM. The frequency band used is 2.4 GHz ISM with a complex modulation technique used, it is possible to achieve data rate of upto 54 Mbps.

Data Link Layer

The data link layer comprises of two layers Logical Link Control (LLC) and Media Access Control (MAC). The LLC is layer above MAC. It is responsible for framing. The frame has source address, destination address and error handling bits. It uses 48 bit addressing. The MAC is responsible for supporting multiple customers on a shared basis such that the sender senses the medium prior to accessing it. Due to near-far problem collision detection is not possible in 802.11 WLAN.

Q. 5 Explain in detail the IEEE 802.11 MAC Layer.

Dec. 15

Ans. :

MAC Layer : In this section, we will describe the MAC layer as specified by the IEEE 802.11 standard. The function of MAC layer is to artibrate and statistically multiplex the transmission requests of various wireless stations operating in that area. Wireless transmissions are broadcast in nature and therefore it is necessary to resolve any contentions to access the shared channel. This is necessary to avoid collisions or at least minimize the number of collisions.

Some other auxiliary functionalities supported by the MAC layer are as follows :

1. To offer support to roaming.
2. Support authentication.
3. To take care of power conservation.

MAC layer supports the following basic services :

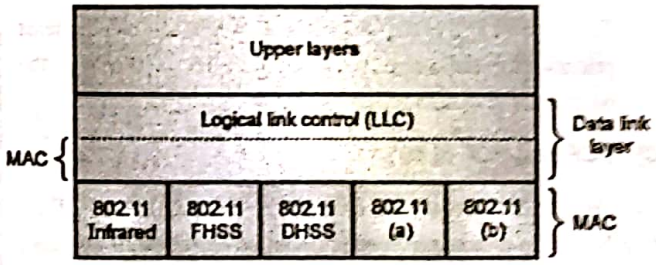
1. The mandatory asynchronous data service.
2. The optional real time service.

The asynchronous data service is for communication with the unicast packets as well as the multicast packets, whereas the real time service is supported only in the infrastructure based wireless networks.

(A) Distributed Foundation Wireless Medium Access Control (DFWMAC)

The primary access method of IEEE 802.11 is by means of Distributed Co-ordinate Function (DCF). There is a second method called the Point Co-ordinate Function (PCF) which is used to provide the real time service.

Fig. 6.10 shows a part of 802.11 protocol stack.



(G-386) Fig. 6.10 : Part of the 802.11 protocol stack

Scanned by CamScanner

There are five possible transmission techniques make it possible to send a MAC frame from one station to another. They differ in the technology used and speeds available. The 802.11 faces the hidden station problem and the exposed station problem. Hence it does not use the CSMA/CD as the MAC protocol.

To deal with this problem, the 802.11 supports two modes of operation :

1. DCF (Distributed Co-ordination Function)
2. PCF (Point Co-ordination Function)

The DCF does not use any kind of central control and PCF uses the base station to control all the activity in its cell. All implementations must support DCF but PCF is optional. When DCF is employed, 802.11 uses a protocol called CSMA/CA (CSMA with collision Avoidance). The other mode of CSMA/CA operation is based on MACAW and uses virtual channel sensing.

(B) Inter-Frame Spacing (IFS)

IFS is defined as the time interval between the transmission of two successive frames by any station.

The four types of IFS are as follows :

1. SIFS 2. PIFS 3. DIFS 4. EIFS

These are in the order of shortest to longest. (SIFS is the shortest and EIFS is the longest). They have different priority levels to access the medium. SIFS has the highest priority and EIFS has the lowest.

The four types of IFS are defined as follows :

1. Short Interframe Spacing (SIFS)

SIFS is the shortest type of all IFS. It has the highest priority. It is defined for the short control messages such as acknowledgements for data packets and polling responses. If the channel is sensed to be idle for a minimum time period of SIFS only then the sender and transmit his packet.

2. PCF Interframe Spacing (PIFS)

It is used for the real time service and defined as the waiting time whose value lies between SIFS and DIFS.

3. DCF Interframe Spacing (DIFS)

DIFS is used by the stations operating under DCF mode for transmitting their packets.

4. Extended Interframe Spacing (EIFS)

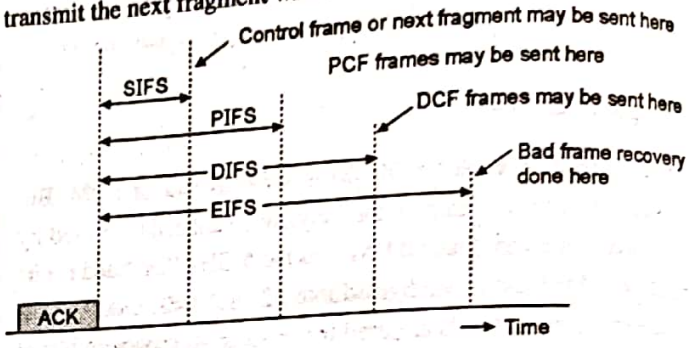
This type of IFS is the longest type of IFS and has the least priority, for accessing the medium. EIFS is used for the purpose of re-synchronization.

(C) DCF and PCF In 802.11

The PCF (Point Co-ordination Function) and DCF (distributed Co-ordination Function) can co-exist within one cell, which might seem impossible at the same time.

But 802.11 provides a way to achieve this goal. It works by carefully defining the interframe time interval. After sending a frame a certain amount of dead time is required before any station may send a frame. Four different intervals are defined as shown in Fig. 6.11 each for a special purpose.

The shortest interval of all is SIFS (Short Interframe Spacing). It is used to allow the parties in a single dialog the chance to go first. During this period the receiver sends a CTS to respond to an RTS letting the receiver to send an ACK for a fragment or full data frame, and lets the sender of a fragment burst transmit the next fragment without having to send an RTS again.



(G-387) **Fig. 6.11 : Interframe spacing in 802.11**

Only one station is allowed to respond after a SIFS interval. If it is not able to make use of this chance, and a time PIFS (PCF Inter Frame Spacing) elapses, then the base station may send a beacon frame or poll frame. This mechanism allows a station sending a data frame or fragment sequence to finish its frame without anyone else interrupting, but gives the base station a chance to grab the channel when the previous sender is done without having to compete with eager users.

If the base station has nothing to say and the time interval DIFS (DCF Inter Frame Spacing) elapses, any station may attempt to acquire the channel to send a new frame. The usual contention rule is to be applied and the binary exponential backoff may be required to be used in the event of a collision. The fourth time interval EIFS (Extended InterFrame Spacing) is used only by a station which has just received a bad or unknown frame to report the bad frame. This event has been given the lowest priority.

(D) CSMA/CA Mechanism

The 802.11 WLANs use the CSMA/CA MAC layer mechanism. It is not possible to use CSMA/CD for WLANs because of the higher error rates existing in WLANs and also due to the fact that detecting collisions is not always possible for the wireless medium. Hence the technique of Collision Avoidance (CA) is adopted for WLANs.

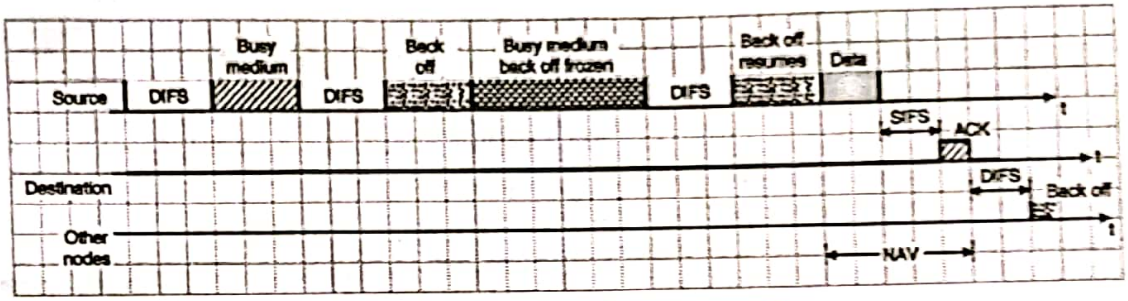
Scanned by CamScanner

Q. 6 Explain media Access mechanism in detail. **Dec. 11, May 12, Dec. 14**

Ans. :

Medium Access Mechanism

Fig. 6.12 shows the basic channel access mechanism of IEEE 802.11. If the medium is found idle during the DIFS then the node accesses the medium for transmission. If the medium is busy, the node will back off. In this situation the station defers channel access by a random amount chosen within a **Contention Window (CW)**. The value of CW will vary between two extreme values CW_{min} and CW_{max}. As soon as the back-off counter expires (reaches zero), the station can access medium. During the back off time itself if a node detects that the channel is busy then it freezes the back off counter and the process will restart only after the channel becomes idle for a period of DIFS.



(G-1525) **Fig. 6.12 : IEEE 802.11 DCF mechanism**

Acknowledgements

Acknowledgements (ACKs) should be sent for data packets so as to ensure their correct delivery. If the packets are unicast then the receiver receives data, waits for SIFS and sends an ACK signal as shown in Fig. 6.12. Other stations will have to wait for DIFS plus their back-off time as shown in Fig. 6.12. ACK ensures that correct data is received by using the CRC (Cyclic redundancy checksum) technique. If ACK is not received, the sender will retransmit the data.

However the number of retransmissions is limited and after a pre-decided number of retransmissions, the sender will report failure to the higher layers.

Q. 7 Explain hidden and exposed terminal problem. **Dec. 12, May 16**

Ans. :

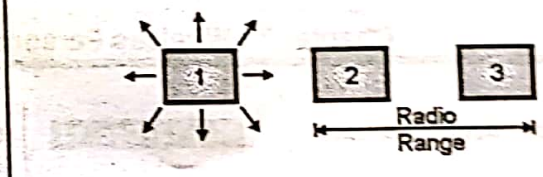
Problems in Wireless LAN

If we try to use CSMA for the wireless LAN, then it uses the principle of simply listening to other transmission and only transmit if no one else is transmitting. But there are two problems in using CSMA. They are hidden station problem and exposed station problem.

Hidden station problem

Refer Fig. 6.13 where station-1 is transmitting to station 2. Now if station-3 senses the medium to see if anyone is transmitting, it will not hear station 1 because it is out of range.

So station-3 will come to a wrong conclusion that no one is transmitting and so it can transmit to station-2. If station-3 starts transmitting, it will create an interference at station-2 and will wipe out the frames from station-1. This problem in which a station is not able to detect a potential competitor which is too far away is called as the **hidden station problem.**

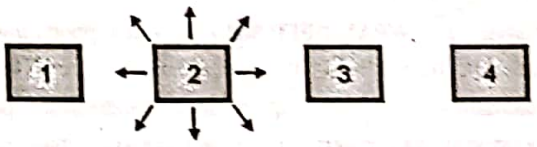


(G-377) **Fig. 6.13 : Hidden station problem**

Exposed station problem

Now consider Fig. 6.14 in which station-2 is transmitting to station-1. If station-3 senses the medium, then since station-2 comes in range with station-3. So station-3 will sense the transmission going on. So it will falsely decide that it should not transmit to station-4. Note that the transmission from 3 to 4 is OK, even when 2 is transmitting.

This problem is called as the **exposed station problem.**



(G-378) **Fig. 6.14 : Exposed station problem**

Scanned by CamScanner

Q. 8 Explain 802.11 MAC management functions. Explain in detail power management function with a neat diagram. **Dec. 16**

Ans. :

802.11 MAC Functions

MAC management plays a vital role in IEEE 802.11. It controls the functions that are related to system integration, synchronization etc. The 802.11 MAC management functions are :.

(i) **Roaming :** It comprises functions for joining (associating a network), changing of the access points, scanning the access points.

(ii) **Synchronization :** It comprises functions for determining a wireless LAN network, synchronizing the internal clocks and generating beacon signals.

(iii) **Management Information Base :** It comprises parameters that represent the current state of the wireless network that can be accessed through Simple Network Management Protocol (SNMP).

(iv) **Power management :** It comprises functions to control the transmitter activity for conserving the power e.g. buffering, periodic sleep without missing a frame.

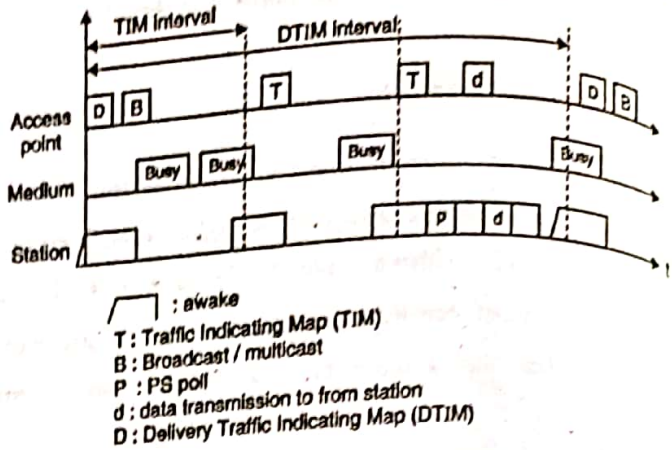


Fig. 6.15 : Power management example

The main motive behind power management is to switch off transceiver when it is not required. Receiver can periodically wake-up transceiver.

For a station there are two states :

(i) Sleep and awake

(ii) Buffering of senders data

The transmitter/sender can communicate with the power saving station if it wants to buffer data. If the station observes that it is a destination for buffered packet, then the station has to remain awake till the packet is sent. For the beacon sent by the access point (AP), a traffic indicating map (TIM) is transmitted. A DTIM (delivery traffic indicating map) informs the transmitter/sender that the data is buffered on the AP.

Chapter 7 : Wireless Personal Area Networks (WPAN)

Q. 1 Describe PAN applications. **May 12, Dec. 14**

Ans. :

PAN applications

The different WPAN technologies and applications are :

(1) Bluetooth (IEEE 802.15.1) – It has a throughput of 1 Mbps. It is used for applications like microphones, speakers, Personal Digital Assistants (PDAs), handheld PCs, headphones, laptops, modems, cell phones.

(2) UWB HR-WPAN (IEEE 802.15.3) It supports high data rates (> 20 Mbps). It is used in digital imaging and multimedia applications.

(3) Zigbee LR – WPAN (IEEE 802.15.4) – It supports **low data rates** (< 0.25 Mbps). It is used in commercial building automation, telecom applications, industrial process monitoring and control, home automation, smart energy, agriculture, vehicle monitoring.

Q. 2 Write note on Bluetooth specifications. **May 12, May 13**

Ans. :

Bluetooth specifications

Bluetooth is an open standard that provides an adhoc way for connecting devices in the 10 m range. In 2002 it was considered by IEEE Wireless Personal Area Network (WPAN) committee as 802.15 standard. Bluetooth is a short range, low cost and power efficient radio frequency based wireless technology that supports both point-to-point and point-to-multipoint connections.

Bluetooth operates in the 2.4 GHz band and uses a frequency hopping TDD method for each radio channel. It connects one hand-held device to other Bluetooth enabled device within a 10 m (30 foot) radius like mobile phones, printers, laptops and other accessories. Bluetooth operates in unlicensed ISM band with locational variations. The Bluetooth enabled devices can automatically locate each other, but user action is essential to make connections with other devices and to form networks.

Scanned by CamScanner

Bluetooth Features (Specifications)

Table 7.1 : Bluetooth feature

Characteristics	Description
Physical layer	FHSS
Frequency band	2.4 – 2.4835 GHz
Hop frequency	1,600 hops/s
Data Rate	1 Mbps
Data and Network Security	Provides three levels of security, two levels of device trust and three levels of service security.
Operating range	10 m
Throughput	Around 720 kbps

Q. 3 Define piconet. **Dec. 10, Dec. 17**

Ans. :

PICONET

Bluetooth is an WPAN (Wireless Personal Area Network) open standard that provides an ad hoc way of connecting devices in the 10m range. It is a short range, low cost and power efficient radio technology that supports point to point and point-to-multipoint connections. It connects handheld devices like printers, laptops, mobile phones and other accessories in the 10m radius. It operates in the ISM band.

Bluetooth operates in the 2.4 GHz band and uses a frequency hopping TDD method for each radio channel. The Bluetooth enabled devices can locate each other, but user action is essential in order to make connections with other devices and form networks. Up to Eight devices can be connected in a Bluetooth network called, **PICONET**. One of them acts as a master and remaining act as slaves. Hence a maximum of 7 slaves can be supported inside a piconet.

Fig. 7.1 shows a Bluetooth PICONET. Whenever two or more devices detect each other and communicate through Bluetooth, a PICONET is formed. One device acts as a master and the remaining devices are slaves. The master device is responsible for initiating the data transmission. The slave devices cannot directly send data to each other.

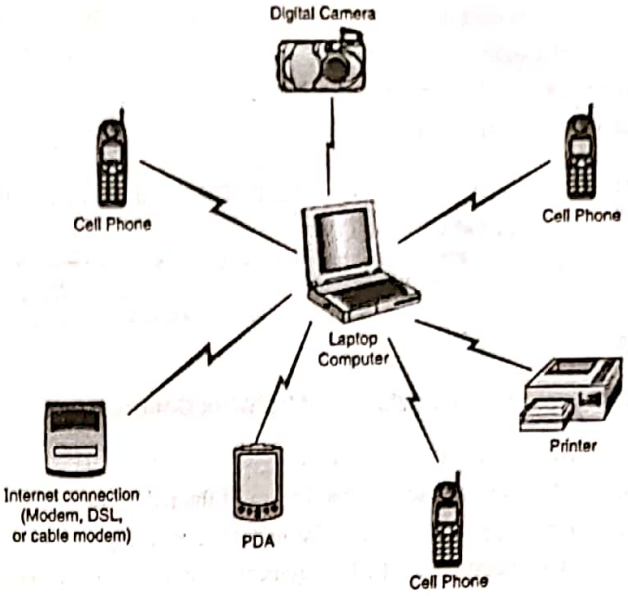


Fig. 7.1 : Bluetooth PICONET

All the PICONET devices use a frequency hopping sequence. As simple examples consider a laptop and a tablet where laptop is the master and the tablet is the slave device. The tablet downloads data from the laptop when both the devices are connected in range.

Q. 4 Define scatternet. **Dec. 17**

Ans. :

Scatternet

Eight devices can be connected in a Bluetooth network called **piconet**. One of them acts as master and the others act as slaves. A **scatternet** is formed when two or more piconets connect through a bridge node as shown in Fig. 7.2.

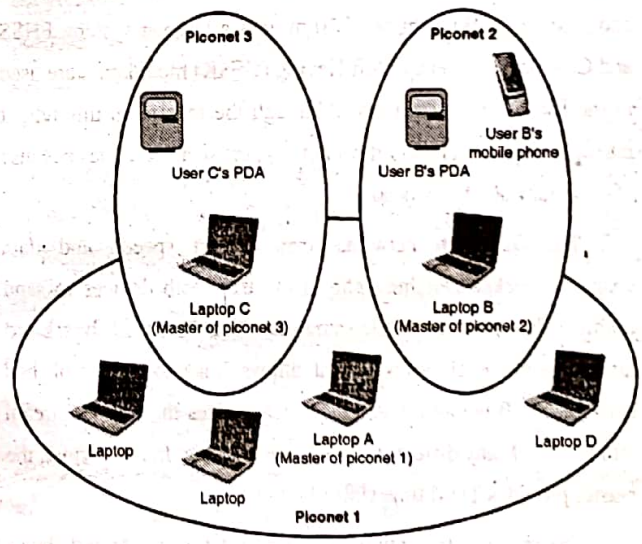


Fig. 7.2 : Bluetooth scatternet

In addition to the seven active slaves, there can be upto 255 parked nodes in the net that can only respond to a beacon signal from the master. The slaves are dumb devices that do the task that the master tells them to do.

Scanned by CamScanner

The piconet is a TDM system with the master controlling the clock and determining which slave gets to communicate in which time slot. All the communication is between the master and slave and not between the slaves.

Q. 5 Explain in detail Bluetooth Protocol architecture with neat diagram.

May 11, Dec. 11, Dec. 12, Dec. 14, Dec. 15, May 16, Dec. 17, May 17

Ans. :

Bluetooth Protocol Stack and Network Connection

The Bluetooth protocol stack defines the software layers that are used for communication on the top of the radio link. The top layer is the application layer. The middle layer comprises of the industry standard protocols. The protocols were used for Bluetooth so that the applications could be easily ported to the Bluetooth.

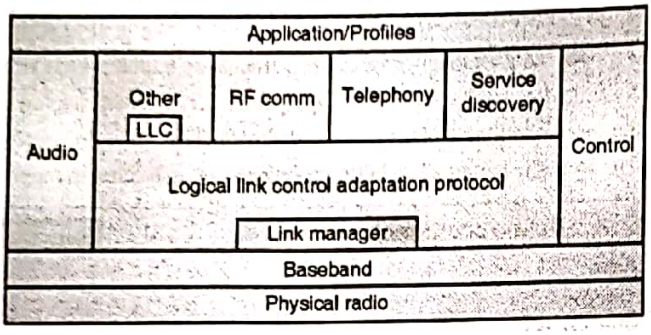


Fig. 7.3 : Bluetooth protocol stack

The lower layer consists the Bluetooth specific components. The transmission characteristics are defined by the **Bluetooth radio layer.** It transfers the data bits from the slave to the master and vice-versa. With range of 10 m, it is a low per system. FHSS and Gaussian Frequency Shift Keying (GFSK) modulation are used in the Bluetooth transceivers. Although the maximum throughput rate is 1 Mbps, practically it cannot support such data rates because of communication overhead.

The Bluetooth networks can support speech and data channels. Packet switching allows the Bluetooth devices to send multiple data packets on the same path. The Bluetooth **baseband layer** is link level protocol that allows links to be established between the Bluetooth devices. It encapsulates the raw bit stream into frames. Many different formats are possible. In one format, the master provides TDM time slots of 625 μs.

The master's transmissions begin in the even slot and slaves transmissions begin in the odd ones, giving the master half the slots with all the slaves sharing the other half. The frames can be sized 1, 3 or 5 slots in length. A logical channel called **link** is used to transfer data between the master and the slave.

Two links are possible

i) For the packet switched data **an Asynchronous connectionless (ACL)** link is used. The data is obtained from the L2CAP layer on the transmitting side. The data is delivered to the L2CAP layer on the receiving side.

ii) For real time data like telephony, **Synchronous Connection Oriented (SCO)** link is used. Here a fixed slot in each direction is allocated to the channel. Because of the time critical nature of the SCO links, the frames are never retransmitted and forward correction is used to provide high reliability. A slave can have upto 3 SCO channels with its master and each link can transmit one 64 kbps PCM audio channel.

A data link layer protocol that communicates with its peer in the target device is called as the **Link Manager Protocol (LMP).** This protocol defines the messages. The messages are used by software in the master for polling the client in cases where the master has no data to send. Between participating devices the messages are exchanged. This is done in order to set up and maintain the radio links.

In the payload data field of Bluetooth data packet, the LMP messages are transported. Authentication and encryption is controlled by these messages. Authentication is done with the help of a response/challenge protocol between the claimant and the verifier. After authentication, the participating devices must agree on common encryption parameters including encryption type and key.

The logical link control and adaptation protocol (L2CAP) is used by upper-layer protocols for data transport. It can be thought of as an adapter between the upper and lower layers. It provides both connectionless and connection oriented service. L2CAP messages are transported in the payload data field of Bluetooth data packets as LMP messages are.

It is responsible for upper-level protocol protocol data segmentation and reassembly as well as transport of QoS (Quality of service) information. It can accept blocks of data upto 64 kB in length and reliability transport them to its peer in the target device using services provided by the baseband layer by creating a logical channel from one device to the other. The bluetooth audio protocol belongs to data link level. It is the only protocol to use the SCO link for synchronous communication. An application can obtain synchronous services by opening a voice data link.

The **Service Discovery Protocol (SDP)** is used to find new services as they become available and to deregister services that become unavailable. It is optimized for fast changing environment.

Q. 6 Explain the frame format in Bluetooth technology.

Dec. 11, Dec. 12, Dec. 14

Scanned by CamScanner

Ans. :

Bluetooth Frame Structure and Network Connection

Fig. 7.4 shows the Bluetooth frame structure.

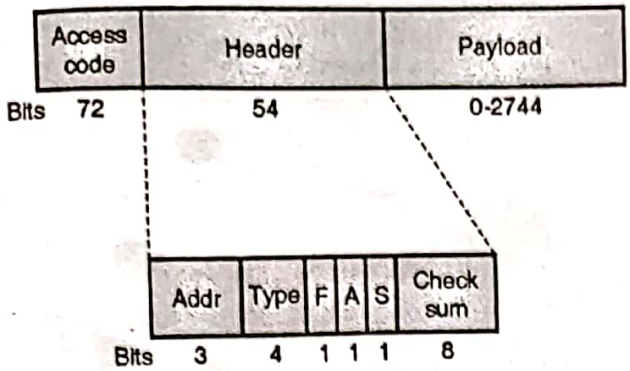


Fig. 7.4 : Bluetooth frame structure

The **access code** identifies the master so that slaves within the radio range of two masters can tell which is traffic for them. The 54 bit header contains an 18 bit header that is repeated 3 times for a total of 54 bits. It allows a receiver to examine all three copies of each bit and reject the ones that does not have a majority.

The **address field** in the header identifies which of the eight devices the frame is intended for. The **type field** identifies whether it is an ACL, SCO, pull or null frame type, the type of error correction used in the data field and how many slots long the frame is. The **flow bit** is used for primitive type of flow control and is asserted by slave when its buffer is full and cannot receive any more data.

The **ACK bit** is used to piggy back an acknowledgement onto a frame. The **sequence bit** is used to number the frames to detect retransmissions in a stop-and-wait protocol. It is followed by 8 bit **checksum**. The data field is upto 2744 bits in the case of five slot transmission and is 240 bits for a single time slot.

Q. 7 Explain Bluetooth security aspect. **May 16**

Ans. :

Security Aspects

Due to the aspect of radio waves, experts fear a security concern with Bluetooth. The issue can be addressed with three aspects: specific sequence of channel hopping known only to the sending and receiving devices, challenge-response authentication routine to verify the validity of the receiving unit, and the 128-bit key encryption standard for securing transmission between devices.

Q. 8 Explain the ZigBee (LR-WPAN) Stack Architecture with a neat diagram. **Dec. 15, Dec. 17**

Ans. :

LR-WPAN (IEEE 802.15.4) ZigBee

Zigbee is a wireless protocol used for wireless networking and connectivity. It is the recently emerged technology of network communication based on the IEEE 802.15.4 standards where IEEE stands for the institute of electrical and electronics engineers. ZigBee is a new standard developed by the ZigBee Alliance for personal-area networks (PANs).

Consisting of more than 270 companies (including Freescale, Ember, Mitsubishi, Philips, Honeywell, and Texas Instruments), the ZigBee Alliance is a consortium that promotes the ZigBee standard for a low-rate/low-power wireless sensor and control network.

Like bluetooth is used for large packet user devices, such as laptops and phones, so in the same way Zigbee is designed for connectivity between small packet devices. Looking at growing demand for a capable wireless networking between low-power devices Zigbee was developed. The ZigBee specification has two implementation options or Feature Sets: ZigBee and ZigBee PRO.

The ZigBee feature set is designed to support smaller networks with hundreds of devices in a single network. The ZigBee PRO feature set is the most popular choice of developers and the specification used for most Alliance developed standards. Zigbee PRO maximizes all the capabilities of the ZigBee feature set, and also facilitates ease-of-use and advanced support for larger networks comprised of thousands of devices. Both Feature Sets are designed to interoperate with each other, ensuring long-term use and stability.

The ZigBee specification enhances the IEEE 802.15.4 standard by adding network and security layers and an application framework. From this foundation, Alliance developed standards, technically referred to as public application profiles, can be used to create a multi-vendor interoperable solutions. For custom application where interoperability is not required, manufacturers can create their own manufacturer specific profiles.

Its operations are simplified and is actively limited to a through-rates are of 250 kbps compared to bluetooth as bluetooth has much larger pipeline of 1 Mbps. Along with giving its support in official field zigbee is also actively working in the consumer market. It is been explored for linking household devices which require less power like smoke alarm, central housing control unit and light control unit.

Scanned by CamScanner

There have been several modifications in the ZigBee specification. The major changes in its revision history are given below :

The ZigBee Alliance in the year 2004 released its first specification. This specification supported a home control lighting profile. However, the ZigBee Alliance now does not support this specification. The ZigBee Alliance in February 2006, released the ZigBee Stack 2006, that comprises modifications to ZigBee 2004 specification.

The ZigBee Alliance in October 2007, released two feature sets called as ZigBee and ZigBee PRO. The ZigBee feature set is interoperable with ZigBee PRO. The devices from the ZigBee feature set stack can combine to the network as end devices, in case if the network is based on the ZigBee PRO stack. Similarly, if a network is based on the ZigBee stack, then the ZigBee PRO devices can combine to the network as end devices. The ZigBee features are backward compatible with the ZigBee 2006 specifications and vice versa.

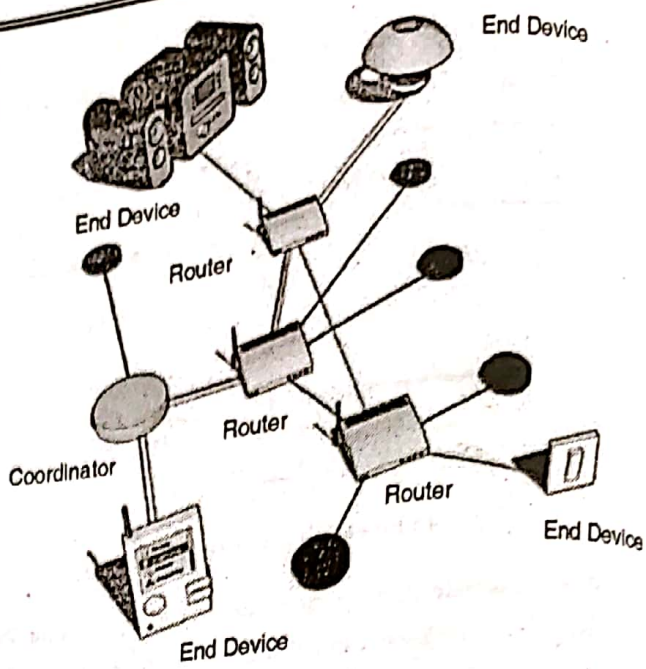


Fig. 7.5 : ZigBEE Network

Chapter 8 : Wireless Metropolitan Area Networks

Q. 1 Write short note on WiMAX and explain WiMAX standards. **Dec. 15, Dec. 16, Dec. 17**

Ans. :

WiMAX

WiMAX provides wireless transmission of data using a variety of transmission modes from point to multipoint links to portable and fully mobile internet access.

WiMAX Standards

WiMAX is associated to IEEE 802.16a / REV d / e standards. These standards were issued by IEEE 802.16 subgroup that originally covered the Wireless Local Loop (WLL) technologies with radio spectrum from 10 to 66 GHz. Recently these specifications were extended below 10 GHz. In January 2003, the IEEE approved 802.16a as an amendment to IEEE 802.16 defining line – of – sight capability.

In July 2004, the IEEE 802.16 REVd was introduced to support indoor **Customer Premises Equipment (CPE)** (NLOS) through additional radio capabilities like antenna beam forming and OFDM sub-channelling. In 2005, an IEEE 802.16e variant was developed for supporting mobility.

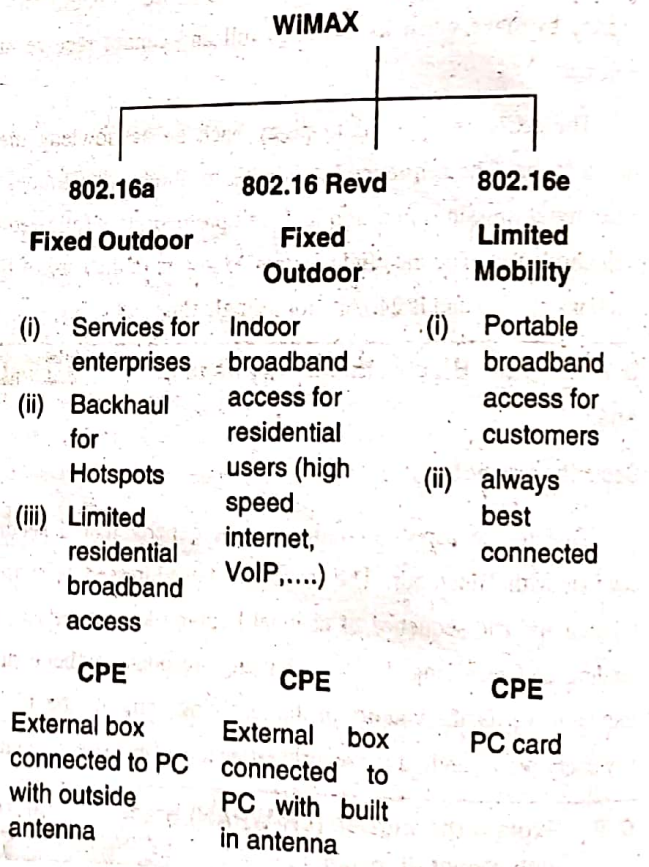


Fig. 8.1 : Standard associated with WiMAX and their applications

Scanned by CamScanner

Table 8.1 gives the details of WiMAX standards.

Table 8.1 : WiMAX standards

Parameter	802.16	802.16a	802.16 e
Spectrum	10-66 GHz	2-11 GHz	< 6 GHz
Configuration	Line of Sight (LOS)	Non-line of Sight (NLOS)	Non-line of Sight (NLOS)
Modulation	QPSK-16 QAM 64 QAM	256 subcarrier OFDM using QPSK, 16 QAM, 64QAM, 256-QAM	256 subcarrier OFDM using QPSK, 16 QAM, 64 QAM, 256-QAM
Mobility	Fixed	Fixed	< 75 mph
Channel bandwidth	20, 25 MHz, 28 MHz	Selectable 1.25-20 MHz	5 MHz planned
Typical cell radius	1-3 miles	3-5 miles	1-3 miles
Completion	Dec 2001	Jan 2003	2nd Half of 2005

WiMAX Forum

WiMAX forum is an industry led non-profit corporation formed to promote and certify compatibility and interoperability of broadband wireless products. The function of the WiMAX forum is to harmonize standards and certify interoperability between equipment from different vendors. Standardized interoperable solutions will result in mass volume and bring down cost. It's function is also to promote and establish a brand for the technology.

WiMAX forum has more than 400 members from equipment manufacturers, semiconductor suppliers and services providers. Some of its members are Alcatel, AT & T, Fujitsu, Intel, Motorola, SBC, Siemens and Nortel.

Q. 2 Write features of WIMAX.

Ans. :

WIMAX Features

1. Very high peak data rates and coverage range

A maximum of **75 Mbps** bandwidth is achievable with a 20 MHz channel under best channel conditions. However, the maximum bandwidth is reduced in the areas where regulators allow only narrower channels.

More typically, using a 10 MHz spectrum operating using TDD scheme with a 3 : 1 downlink-to-uplink ratio, the peak data rate is about 25Mbps and 6.7Mbps for the downlink and the uplink, respectively.

The theoretical coverage range is about 30 miles under optimal conditions and with a reduced data rate. At extremely long range, the data rate drops to 1.5 Mbps. The typical coverage with indoor Customer Premises Equipment (CPE) is about 5 Km and with a CPE connected to an external antenna (LOS), it is around 15 Km.

2. Scalable bandwidth and data rate support

WiMAX has a scalable physical-layer architecture that allows for the data rate to scale easily with available channel bandwidth. For example, a WiMAX system may use 128, 512, or 1,048-bit FFTs (fast fourier transforms) based on whether the channel bandwidth is 1.25MHz, 5MHz, or 10MHz, respectively. This scaling may be done dynamically to support user roaming across different networks that may have different bandwidth allocations.

3. Support for TDD and FDD

IEEE 802.16 REVd and IEEE 802.16e standards supports both Time Division Duplexing and Frequency Division Duplexing, as well as a half-duplex FDD, that allows for a low-cost system implementation.

4. WiMAX- Radio Channel Bandwidth

Wimax equipments are allowed to operate in both licensed and unlicensed bands. The minimum channel bandwidth for WiMAX usage is 1.75 MHz per channel, while 10 MHz is considered as an optimum. Although 2.4 GHz and 5 GHz non-licensed bands are largely available, their usage could be limited to trials because of the risks of interference preventing QoS commitments. The 2.5 and 3.5 GHz licensed bands will be the most common bands for WiMAX applications. The 5 GHz band is also partially licensed in some countries.

5. Flexible and dynamic per user resource allocation

Both uplink and downlink resource allocation are controlled by a scheduler in the base station. Capacity is shared among multiple users on a demand basis, using a burst TDM scheme.

6. Quality-of-service support

The WiMAX MAC layer has a connection-oriented architecture. It is designed in order to support many applications that include the voice and multimedia services. The WiMAX system gives support for variable bit rate, constant bit rate, real-time, and non-real-time traffic flows etc. The medium access control layer is designed in order to support a large number of users, with multiple connections per terminal, each with its own QoS requirement.

Scanned by CamScanner

7. Robust security

WiMAX supports strong encryption, using Advanced Encryption Standard (AES) and has a robust privacy and key-management protocol. The system also offers a very flexible authentication architecture based on **Extensible Authentication Protocol (EAP)**, which allows for a variety of user credentials, including username/password, digital certificates, and smart cards.

8. Support for mobility

The mobile WiMAX variant of the system has mechanisms to support secure seamless handovers for delay-tolerant full-mobility applications, such as VoIP.

9. IP-based architecture

A reference network architecture that is based on an all-IP platform is defined by the Wimax forum. Over an IP architecture all the end-to-end services are delivered. They rely on the IP-based protocols for QoS, end-to-end transport, mobility, session management, and security.

10. Forward Error Correction (FEC)

Error correction techniques are also a key feature of WiMAX technology. Errors are detected and corrected using Reed Solomon FEC, convolutional encoding and interleaving algorithms. All these techniques help in recovering the errored frames that might have got corrupted due to frequency selective fading or burst errors.

Q. 3 Give advantages and disadvantages of WiMAX.

Ans. :

Advantages of WiMAX

1. Single station can serve hundreds of users.
2. Much faster deployment of new users comparing to wired networks.
3. Speed of 10 Mbps at 10 kilometers with line-of-sight.
4. It Creates a volume opportunity for silicon suppliers.
5. It is innovate more rapidly because there exists a standards-based, stable platform upon which to rapidly add new capabilities.
6. WiMAX will also enable end-users to benefit from an **"Always Best Connected"** experience when accessing their applications through the best available network, at home, or on the move. WiMAX becomes an additional radio access solution in the global network architecture.

Disadvantages of WiMAX

1. Line of sight is needed for longer connections. With line-of-sight (optical visibility), you could have speed of 10 Mbps at 10 Kilometers. In the urban environment (without the optical visibility) users can have 10 Mbps at 2 Kilometers. If users are moving, speed can drop significantly.
2. Weather conditions like rain could interrupt the signal.
3. Other wireless equipment could cause interference.
4. Multiplied frequencies are used.
5. WiMAX is very power intensive technology and requires strong electrical support.
6. It has a big installation and operational cost.
7. Common misconception is that the WiMAX can offer 70 Mbps in range of 70 miles (113 Kilometers) with moving stations. In practice situation is a very different. It is true only in ideal circumstances with only one recipient.
8. Bandwidth is shared among users in a given radio sector. If there are many users in one sector, they will have lower speed. Users could have 2, 4, 6, 8, or 10 Mbps of the shared bandwidth.

Q. 4 Compare the different 802.16 standards. **Dec. 16**

Ans. :

Comparison of 802.16 standards

Feature	WIMax (802.16a)	WI-FI (802.11b)	WI-FI (802.11a/g)
Primary Application	Broadband Wireless Access	Wireless LAN	Wireless LAN
Frequency Band	Licensed / Unlicensed 2 G to 11 GHz	2.4 GHz ISM	2.4 GHz ISM (g) 5 GHz U-NII (a)
Channel Bandwidth	Adjustable 1.25 M to 20 MHz	25 MHz	20 MHz
Half / Full Duplex	Full	Half	Half
Radio Technology	OFDM (256-channels)	Direct Sequence Spread Spectrum	OFDM (64-channels)
Bandwidth Efficiency	≤ 5 bps/Hz	≤ 0.44 bps/Hz	≤ 2.7 bps/Hz
Modulation	BPSK, QPSK, 16-, 64-, 256-QAM	QPSK	BPSK, QPSK, 16-, 64-QAM
FEC	Convolutional Code Reed-Solomon	None	Convolutional Code
Encryption	Mandatory – 3DES Optional - AES	Optional- RC4 (AES in 802.11i)	Optional - RC4 (AES in 802.11i)
Mobility	Mobile WiMax (802.16e)	In development	In development

Scanned by CamScanner

Feature	WIMax (802.16a)	WI-FI (802.11b)	WI-FI (802.11a/g)
Mesh	Yes	Vendor Proprietary	Vendor Proprietary
Access Protocol	Request / Grant	CSMA/CA	CSMA/CA

Q. 5 Give in detail comparison between WIMax and LTE/3GPP. **May 17**

Ans. :

WIMAX and LTE/3GPP Comparison

Parameter	WiMAX	LTE/3GPP
Air interface	OFDMA based QPSK – 64 QAM	OFDMA based QPSK 64 QAM
Duplexing	TDD	FDD/TDD
Frequency band	2.3 – 2.4 GHz 2.496 – 2.69 GHz 3.3 – 3.8 GHz	Existing and new frequency bands
Technology	IP based packet switching technology	Circuit/Packet switching
Cell radius	2 – 7 Km	5 Km
Number of users	100 – 200 users	> 400 users for large bandwidth > 200 users at 5 MHz
Speed	upto 120 Km/hr	upto 350 km/hr
Channel bandwidth	5, 8.75 MHz, 10 MHz	1.25 – 20 MHz
Handovers	Provided	Soft handovers are supported.

Chapter 9 : Wireless Network Design Considerations

Q. 1 Explain in detail Cisco Unified Wireless Network.

Ans. :

Cisco Unified Wireless Network

The Cisco Unified Wireless Network provides seamless connectivity to unified wired as well wireless networks. The wireless networks are profitable from the business point of view. The Cisco unified wireless networks provide users with end-point mobility and network access anywhere. This has led to the development of for innovative applications to improve business operations and increase productivity.

The Cisco unified wireless network provides manageable, scalable, reliable and secure WLANs that are cost-effective. The wireless LANs can be easily deployed and can be easily managed. It uses both the elements of wired as well as wireless networks. The Cisco unified wireless network provides real time access to business applications with a secured connectivity of enterprise class. It provides 24 hour product support to the users delivering a good wireless LAN security as well as investment protection.

The Cisco Unified Wireless Network provides an integrated solution to wired and wireless networks addressing all the layers of the WLAN, from the client devices and access points, to the network infrastructure, to network management.

Cisco unified wireless network integrates the access point technology with real time location services, intelligent control, centralized management system, real time location services and an array to compatible client devices.

The Cisco unified wireless network can be easily centrally deployed. This decreases the network deployment and management cost. A centralized management console is responsible for managing the several access points that are remotely connected. All these features allow the network managers to design integrated networks satisfying their criteria.

The Cisco Unified wireless networks can be deployed across hospitals, offices, retail stores, educational institutes, railway stations, airports, banks and other financial institutions, manufacturing floors, central and state governments and other world -wide locations. It also supports Wi-Fi enabled business applications. The RFID devices are also supported by Cisco unified wireless networks for applications like inventory management, healthcare, video surveillance, accessing real-time data.

We can access Cisco unified wireless networks from onroad locations like convention centres, hotels, public hotspots , public places etc. Thus, the Cisco unified wireless networks provide real time mobility and security to users on the network. Fig. 9.1 shows the elements of Cisco unified wireless network that provide an enterprise class unified wireless solution.

Scanned by CamScanner

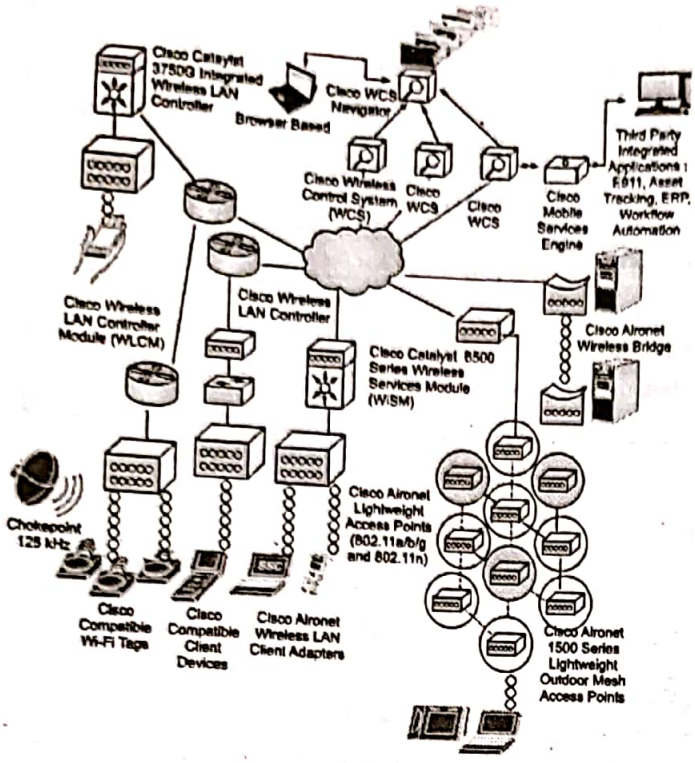


Fig. 9.1 : Cisco Unified wireless network providing enterprise class unified wireless solution

The five elements of Cisco Unified wireless network are integrated together to provide an enterprise class WLAN solution. The elements of Cisco Unified wireless network are as follows :

1. Client devices

Most of the laptops, notebooks, computers used world-wide are Wi-Fi enabled. For industry specific applications many specialized Wi-Fi client devices are available. The function of the client devices is to securely interoperate with the existing WLAN infrastructure and meet the requirements desired by the organizations. Hence, for Cisco Unified Wireless Network : Cisco Aironet client devices or Cisco compatible client devices are preferred to be used. It also supports Wi-Fi or IEEE 802.11 certified clients.

Today there are more than 300 wireless devices that are Cisco compatible or have Cisco extension programs for interoperating with Cisco wireless networks. More than 90 percent of notebooks are Cisco Compatible certified.

2. Network unification

For a unified network control it is essential to integrate the wired as well as wireless network. This will ensure network features like security, reliability, scalability, RF management, QoS, intrusion prevention to as to support enterprise class wireless applications.

3. Access points

For connecting WLAN clients with organizations, access points are used for providing reliable WLAN solution. Cisco provides many enterprise class access points and bridges to complete the client requirements. The **Cisco LAP** (Light weight Access Point) is part of the Cisco Unified Wireless Network architecture. A LAP is an access point (AP) designed to be connected to a wireless LAN (WLAN) controller (WLC).

The LAP is responsible for providing dual band support for IEEE 802.11a, 802.11b, and 802.11g to securely support audio, video, and data applications. APs are **"lightweight,"** this indicates that they cannot act independently of a wireless LAN controller (WLC). They can handle real time applications. The WLC is responsible for managing the access point configurations and the firmware.

4. World class network management

The Cisco Unified wireless network managers require a secure, cost-effective, reliable tool for wireless LAN planning, configuration, and management. The tool should be centrally deployed and must be available to support wireless operations as well as for graphical interfaces. **Cisco's world-class WLAN management interface is called Cisco Wireless Control System (WCS).** Cisco WCS supports wireless LAN management through a centralized management tool designing, controlling and managing the wireless networks.

5. Management and Mobility services

The Cisco Unified Wireless LAN should be able to support the newly developed wireless technologies and mobility applications. The function of management and mobility services is to allow easy and cost effective deployment and implementation of WLAN.

Q. 2 Give advantages of Cisco Unified Wireless Network.

Ans. :

Advantages of Cisco Unified Wireless Network

(1) Voice over IP

(2) Ease of upgrades and deployment

(3) Guest networking

(4) Layer 2 and 3 roaming

(5) Location services

(6) Lowered total cost of ownership

(7) Optimized user performance

(8) Reliable connectivity

(9) Wired and wireless unification

Scanned by CamScanner

Chapter 10 : Wireless Network Security

Q. 1 What is need of wireless network security ? **May 13**

Ans. :

Need for Wireless Network Security

Nowadays wireless local area networks are mostly used in place of wired local area networks in offices, industries, multinational companies, buildings etc. The wireless LAN systems send and receive data through wireless medium i.e. over the air with RF technology. This reduces the hardware needed for wired connections and also infrastructure required.

The wireless LANs provide the user with data connectivity and mobility. This increases their use in devices like notebook computers, handheld terminals, laptops, smart phones, tablets etc. for sending the real time data to be processed to the centralized unit. Many business customers, industries are using wireless LAN systems.

However, the security of wireless LAN systems is of prime importance as data sent through wireless medium can be broken easily and is insecure incomparison to that of wired networks. The data transmitted through wireless medium over the air can be received by anyone. Hence, care must be taken while transmitting important data using wireless LANs.

Whether using wireless or wired network any computer is subject to following security issues :

(i) Privacy

(ii) Threat to the physical security of the network

(iii) Unwanted users accessing the network in unauthorized manner.

For transmitting data on local area networks there should be some security irrespective of the type of communication i.e. wired or wireless inorder to ensure that the data is not transmitted to unauthorized users, hackers, network attackers. Extreme security, privacy is needed if the data transmitted is related to financial institutions, banks, Military, e-government, e-commerce, air-fare, railway bookings etc. as the data is very confidential and of utmost importance.

Q. 2 Explain possible attacks on WLAN. **Dec. 11, May 12, Dec. 12, Dec. 14, Dec. 15, Dec. 17**

Ans. :

Attacks on Wireless Networks

With the advancements in technology the use of computer networks using wireless networks has grown up in the recent years. Most of the industries and businesses are dependent on correct, secure and safe operation of the wireless local area networks. The data related to banking operations, income tax, trading, military data, users credit records, national security data are stored in computers. The security of this confidential data is extremely important. If there is an attack on the network, this data can be leaked and unauthorized users or enemies can misuse the data or modify it.

There are two types of attacks on computer networks. They are :

(i) Passive attack (ii) Active attack

Passive attacks are attacks where the attacker tries to access the data that is being transmitted over the network. Passive attacks are **eavesdropping – easy to perform almost impossible to detect** or snooping during data is transmitted. By default, everything is transmitted in text e.g. usernames, passwords, content etc, no security is offered by the transmission medium.

In passive attacks there are two types of attacks.

(i) Traffic analysis and

(ii) Release of the message contents

(i) In the **traffic analysis attack**, the attacker can get data about the user location, frequency and length of the message that is transmitted that can help him to determine the nature of message that is being transmitted.

(ii) In **release of message contents attack**, the attacker can attack the users email or file that is being transmitted.

Passive attacks are very difficult to detect. However if measures are taken they can be avoided. **Active attacks** are attacks where the user data is modified or fraud data is created. It is very difficult to avoid active attacks on the computer networks.

The different types of active attacks on computer networks are as follows :

1. Masquerade
2. Reply
3. Modification
4. Denial of service

1. A **masquerade attack** is observed when identity behaves like another identity e.g. : an authorized user may replace his identity by the user's identity.
2. **Reply :** It deals with capturing the data unit passively and retransmit the data to build undesired access.
3. **Modification of messages** indicates that some part of the message is modified, recorded or delayed so as to produce an unauthorized result.
4. **Denial of service** indicates that the service is unauthorized.

Scanned by CamScanner

The different attacks on wireless networks are as follows :

1. **Service interruption :** In this attack the system resources are destroyed or service to the network is made unavailable.
2. **Modification :** In this attack, the attacker accesses the data of the network and also he can modify the data or destroy the data.
3. **Jamming :** In this attack the network service is interrupted if the traffic is such that it cannot reach the client. The attackers floods the 2.4 GHz band, degrading the signal strength.
4. **Fabrication :** In this attack the network authenticity is attacked. The attacker puts obstruction objects in file records.
5. **Attacks against encryption :** Wired Equivalent Privacy (WEP) is used as an encryption method in IEEE 802.11b standard. It has some drawbacks. The attacker can break the WEP.
6. **Misconfiguration :** Some of the access points (APs) have unsecured configuration as they are rapidly deployed. Hence, each access point must be secured otherwise, it can be attacked by unauthorized users.
7. **Interception :** For capturing the data in a network, this attack is an attack on the network confidentiality.

   Eavesdropping is easy because if one message is sent the sender may not be able to determine whether his message is eavesdropped or not, if in a building there is no electromagnetic shielding, the traffic can be eavesdropped.
8. **Client-to-client attacks :** The clients need to protect themselves against attacks similar to wired networks. The service can be interrupted even if IP or MAC addresses of networks are duplicated.
9. **Brute-force attacks against passwords of access points :** Usually the wireless users that use an Access point share a single password or key. An attacker or hacker can hack the password by guessing the password. Once the password is known to the attacker, he can access that entire network or even change the password, causing a threat to system security.
10. **Insertion attacks :** Insertion attacks occur because of deploying wireless network without implementing security methods or installing unauthorized devices on the network. e.g. : an organization may not be aware that its employees have deployed wireless facilities on its network by connecting their mobile devices to an access point without authorization from the company. Hence, we need to securely configure all the access points in the organisation.

Q. 3 Explain the WEP. State the different fields present in the WEP frame. Dec. 10, May 11, Dec. 11, May 12, Dec. 12, May 13, Dec. 13, Dec. 14, Dec. 15, May 16, Dec. 17, May 17

Ans. :

Wired Equivalent Privacy (WEP) Protocol

It is a **security protocol widely used for IEEE 802.11 WLAN systems** and provides the security level same as that is seen in wired LAN systems. This protocol was developed to support network confidentiality with wireless protocols. It is designed to protect the wireless networks from unauthorized user access to the network and eavesdropping.

It provides same protection as that in wired networks by encrypting the data that is transmitted in the WLAN systems. The wireless node and the access point share a secret key. This data packets are encrypted with the help of the secret key before that are transmitted. Generally a single key is shared between the nodes and the access points. This protocol is dependent on the keys shared between the access points and WLAN adapters.

The manufacturers of different companies have developed different WLAN systems that are compatible with the WLAN standard and can be worldwide. The security of WLAN systems is a major reason of concern.

The attackers must not be able to access the network and also they should not be able to capture the network traffic. To prevent eavesdropping WEP uses a RC4 algorithm that generates a random number depending on the secret key. It uses a stream cipher for confidentiality. It also uses checksum CRC-32 for integrity. Fig. 10.1 shows how data is encrypted using WEP algorithm.

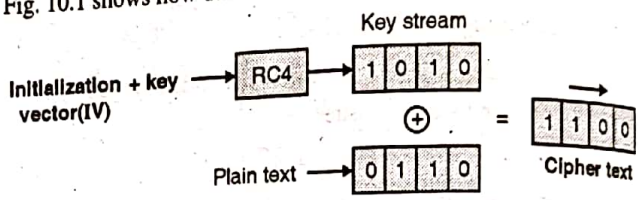


Fig. 10.1 : WEP encryption

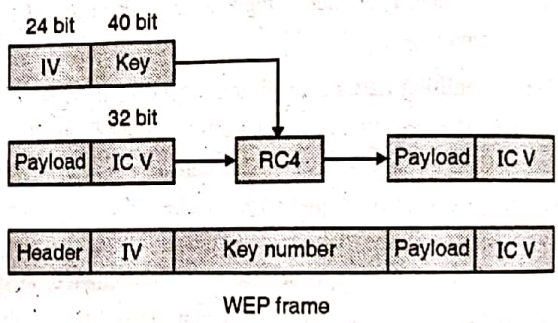


Fig. 10.2 : WEP Authenticated frame

It has a key that is concatenated with initialization vector (IV) to generate the 128 bit RC4 traffic key. This method works well with Secure Socket Layer (SSL). The encryption must provide integrity, confidentiality authentication of data that is sent over the wireless network. RC4 encryption is a standard widely used for IEEE 802.11 WLAN security worldwide.

Scanned by CamScanner

For authentication two methods are used. They are :

(i) Open System Authentication

(ii) Shared key Authentication

In Open System authentication, during authentication the user does not require to provide its details to the Access Point. Any user can authenticate with the Access Point and then attempt to associate. If no authentication has taken place , WEP keys are used for encrypting data frames and for correct authentication user must have knowledge about the correct WEP keys.

In Shared Key authentication, the WEP key is used for authentication. The authentication takes place as follows :

Step 1 : The user client sends an authentication request to the Access Point.

Step 2 : The Access Point acknowledges the request by sending a clear text.

Step 3 : The user encrypts the text with WEP key. Then the encrypted data is sent in another authentication request to the access point.

Step 4 : The Access Point decrypts the message received. If it matches with the text, then it sends back a positive acknowledgment.

The shared key authentication is more secure in comparison to open system authentication.

Q. 4 State weaknesses in the WEP. **May 13, Dec. 14**

Ans. :

Weaknesses in WEP

There are many weaknesses in WEP with respect to security of WLAN systems.

1. The initialization vectors are short and not protected from reuse.
2. Cryptographic keys are short. They are susceptible to attacks.
3. There is no protection against message reply.
4. The message integrity is weak.
5. There is no method to update the cryptographic keys frequently.
6. RC4 provides weak keys that are easy to crack.
7. Keys are static.
8. Security features in products are not enabled. For security purposes user needs to enable them himself.

Q. 5 Explain in detail Mobile IP.

Dec. 11, Dec. 15, Dec. 16, May 17

Ans. :

Mobile IP

Mobile IP (or MIP) is a communications protocol to allow mobile device users to move from one network to another while maintaining a permanent IP address. The Mobile IP allows location-independent routing of IP datagrams on the Internet. Every mobile terminal is identified by its own address irrespective of its current location in the Internet.

When user is away from its home network, its mobile node is associated with a proxy address which identifies its current location and its home address is linked with the local endpoint of a tunnel to its home network. Mobile IP specifies how a mobile node registers with its home network. It also specifies how the network routes the data to the mobile node.

With the help of Mobile IP a user can send and receive the data from any point in the network irrespective of its location in network. But this poses a security problem of redirection attacks. A redirection attack happens when a suspicious user provides wrong information to the home agent in the mobile IP network. The home network is intimated that the user has new proxy address and thus all IP data addressed to the original user are redirected to the suspicious user.

Mobile IP can face two types of attacks:

(i) A suspicious user can reply to the previous registration messages and cut the mobile node from its network.

(ii) A mobile node can behave as if it is new to the network or foreign and send a registration request to home network to divert traffic to it.

To protect mobile IP from the attacks we need to authenticate the messages and correctly use the registration request identification field and reply message. The fields in the registration request and reply are as follows :

1. **Type :** It is an 8 bit field indicating the nature of authentication
2. **Length :** It is also an 8 bit field. It indicated the number of bytes in the authenticator.
3. **Authenticator :** It has a code shared by sender with the help of secret key. The receiver has to insert the same code to check that message is not modified.
4. **Security parameter index :** This field is of 4 bytes and is used to indicate the security context between the nodes in accordance with the authentication method.

Scanned by CamScanner

Q. 6 Explain VPN along with tunneling protocol.

May 11, Dec. 16

Ans. :

Virtual Private Network (VPN)

A **Virtual Private Network (VPN)** is a reliable network used for connecting the networks and resources of a network over another network that are located over different places. VPN uses a public network (internet) inorder to connect to the computer networks making data communication easy and cheap.

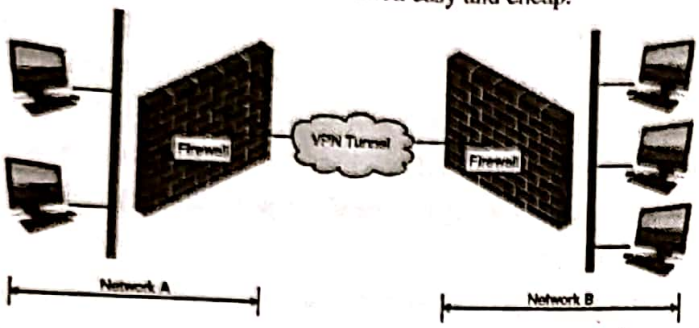


Fig. 10.3 : VPN architecture

Whenever data is exchanged between two devices over the internet they must transfer it in regards to some communication protocol. These different communication protocols split the message into different parts such that one part comprises the data that is to be sent and other comprises the different rules to be followed for sending the data.

The sender and the receiver both must use the same communication protocol so that data is correctly sent and received. Tunneling protocol is used for securely sending the data. VPN is based on tunnelling protocol. A tunneling protocol encloses in its datagram another complete data packet that uses a different communication protocol.

It creates a tunnel between two points on a network that can securely transmit any kind of data between them. Tunneling protocols are used for transmitting private data on a public network usually in developing **virtual private networks (VPN).** Tunneling protocols when transmitted over a public network provide security to the transmitted data. Today for secure data transmission we use various tunneling protocols like PPTP (point-to-point tunneling), SSH (secure socket), IPSEC, L2TP (layer 2 tunneling protocol) etc.

Fig. 10.4 shows Tunneling

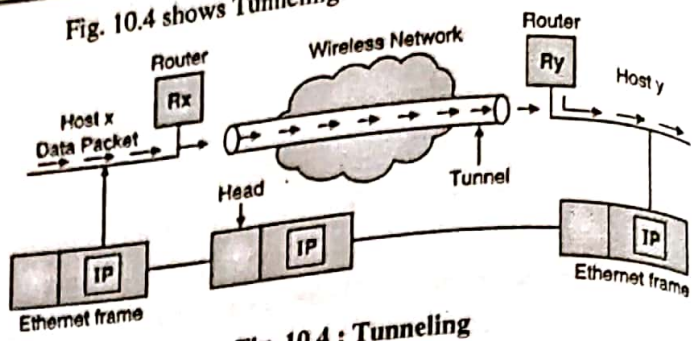


Fig. 10.4 : Tunneling

Host x wishes to send a data packet to Host y. The data packet at Host A has the IP address of Host y. Host A transmits the data packet. When the data packet receives Router R_x, the IP packet is removed. The Router inserts the payload field and sends it to Router R_y. On receiving the packet Router R_y removes the IP packets and sends it to Host y in an Ethernet frame.

A VPN is a group of two or more computer systems that is connected to a private network that is maintained by an institution or company for its own use with public access. Today for secure data transmission the following tunnelling protocols are used as result of developments in VPN.

(i) PPTP (Point to Point Tunneling)

(ii) SSH (Secure Socket)

(iii) L2TP (Layer 2 Tunneling Protocol)

(iv) IPsec (Internet Protocol Security)

VPN is already deployed in various organizations to enable remote workers to access the organisation network data through the internet securely.

VPN technology needs three parameters. They are :

(i) Traffic control

(ii) Security

(iii) Enterprise management.

For ensuring VPN security, different tunneling protocols are used. We will study them in following subsections.

Scanned by CamScanner