WIRELESS TECHNOLOGY

SEMESTER-VII (CBGS)

INFORMATION TECHNOLOGY BRANCH

PREPARED BY

MR. NILESH M. PATIL

BATCH: 2016-17

CHAPTER 1

FUNDAMENTALS OF WIRELESS COMMUNICATION

1.1.Introduction

- Wireless systems have a unique capability of maintaining the same contact number even if one moves from one location to another. This has made them increasingly popular.
- The wireless telephones are not only convenient but also provide flexibility and versatility; there have been growing number of wireless phone subscribers as well as service providers.
- A combination of wireless communication and computer technologies has revolutionized the world of telecommunications.
- Wireless and mobile communications have found usefulness in areas such as commerce, education, defense, etc.
- According to the nature of a particular application, they can be used in home-based and industrial systems or in commercial and military environment.
- There can many novel applications of such a wireless system; for example, a bracelet worn can constantly monitor the body parameters and take needful actions (like informing the family physician about the problem).
- In commercial system, the wireless communications can be employed for purchase or selling of goods and services, playing audio and video, payment of telephone bills, payment of electricity bills, airline/ railway/ bus reservations, etc.
- The difference between *wireless* and *mobile* devices is not much and they are used interchangeably. However, mobile just means portable.
- A laptop is a mobile device, as is a personal digital assistant (PDA). A desktop would be a mobile device if you had the inclination to carry it around with you.
- A wireless device has some sort of network connectivity. A cell phone is wireless, and a laptop or a PDA would be wireless if they had a wireless modem.
- Similarly, applications are wireless when they connect and exchange data with a network.

1.2.Wireless Communication System

- The major function of the communication system is to convert information into a format appropriate for the transmission medium and to modulate analog signals or bits for transmission over channel.
- The channel (either wired or wireless medium) propagates the electromagnetic waves (signals)and the intended recipient picks the signal. Wireless communication systems exchange electronic data among different users through a wireless media.
- Analog communication systems convert (modulate) analog signals into modulated (analog) signals whereas digital communication systems convert information in

the form of bits into digital signals. Computers naturally generate information as bits.

- Analog signals can be converted into bits by quantizing and digitizing for use in digital communication.
- A typical wireless system communication consisting of sender and receiver is shown in figure 1.1 below.

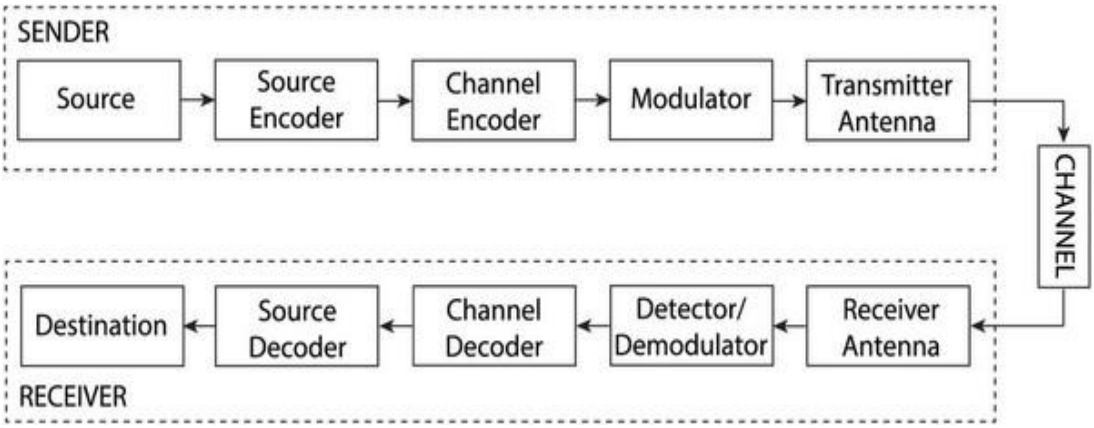


Figure 1.1 Wireless Communication System

- The sender receives the information from the source and encodes it using a source encoder.
- The source encoder encodes the information into a binary data sequence. Methods for source encoding are waveform coding, linear predictive coding, etc.
- The channel encoder encodes the signal for error detection and correction by adding some redundant bits. Methods for channel encoding are hamming codes, cyclic codes, block codes, etc.
- The encoded signal is modulated by using the digital modulation schemes such as binary phase shift keying (BPSK), quadrature phase shift keying (QPSK), minimum shift keying (MSK), Gaussian MSK (GMSK), etc.
- The transmitter antenna, which is the interface between the transmitter hardware and the channel, converts the modulated signal into a suitable energy form that can be transmitted through the physical channel.
- The transmitted waveforms propagate along the channel and presumably reach to the receiver antennas with additional noise whose extent mostly depends on the physical characteristics of the channel.
- The waveforms detected at the receiver antennas are transmitted to the demodulator which converts the signal into a binary bit stream according to a predefined demodulation scheme.
- The function of the channel decoder is the removal of the redundant bits.
- The source decoder converts the binary stream into the symbols, and transmits them to the destination as the recovered information.

The main design goals of the transmitter and the receiver are to mitigate distortion and noise from the channel. Performance metric for analog system is fidelity, whereas digital systems are analyzed based on data rate and bit error probability as performance metrics.

- **Fidelity**: Fidelity describes how close is the received signal to the original signal. Fidelity defines acceptability.
- **Data Rate**: Data rates over channels with noise have a fundamental capacity limit. Data rate is limited by signal power, noise power, distortion, and bit error probability. Without distortion or noise, we can have maximum data rate with zero bit error probability.
- **Bit Error Probability**: It is defined as the ratio of the number of bits, elements, characters, or blocks incorrectly received to the total number of bits, elements, characters, or blocks sent during a specified time interval. For example, if 10 bits are altered when 10,000 bits are transmitted, the bit error probability equals 10/10,000 = 0.001.

An important parameter in communication channel is **bandwidth**. For digital communications, bandwidth of a channel is defined as the maximum number of bits transmitted in a second (bits per second or bps) whereas for analog systems bandwidth is defined in terms of hertz (Hz).

Shannon capacity defines maximum possible data rate for systems with noise and distortion. In noisy channel, data rate C is defined as

$$C = B \log_2 (1 + S/N) \text{ bps}$$

where B is the bandwidth in Hz and S/N is the signal-to-noise ratio.

Problem 1.1

In a communication channel, the channel bandwidth is 3.4 kHz and output S/N power ratio is 20dB. Calculate the channel capacity.

Solution:

Given, channel bandwidth, B = 3.4 kHz

Output S/N power ratio = 20 dB

Therefore, $10 \log_{10} S/N = 20$ dB

$\log_{10} S/N = 2$

$S/N = 10^2 = 100$

Channel capacity is $C = B \log_2 (1 + S/N)$ bps

$= 3.4 * 10^3 \log_2(1 + 100)$ bps

C = 22.638Kbps

Problem 1.2

Calculate the minimum SNR required to support information transmission through the telephone channel of bandwidth 3.4 kHz at the data rate of 4800 bps.

Solution:

Given, channel data rate, C = 4800 bps; bandwidth, B = 3.4 kHz

Channel capacity is $C = B \log_2 (1 + S/N)$ bps

$4800 = 3.4 * 10^3 \log_2(1 + S/N)$

$1.411 = \log_2(1 + S/N)$

$1 + S/N = 2^{1.411}$

$1 + S/N = 2.659$

$S/N = 1.659$

$(S/N)\ dB = 10 \log_{10} 1.659 = 2.2\ dB$

S/N = 2.2 dB

Problem 1.3

In a communication channel, the bandwidth is 10 MHz and SNR is 100.

(a) Determine the channel capacity.

(b) If SNR drops to 10, how much bandwidth is needed to achieve the same channel capacity as in (a).

Solution:

Given, channel bandwidth = 10MHz and S/N = 100

Channel capacity is $\boldsymbol{C = B \log_2 (1 + S/N)\ bps}$

$C = 10 * 10^6 \log_2 (1 + 100)$

C = 66.6 Mbps

If the SNR drops to 10, that is, S/N = 10, the bandwidth is

$B = C/ \log_2(1 + S/N) = C/\log_2(1 + 10)$

$B = 66.6 * 10^6 / 3.47$

B = 19.19 MHz

1.3.Advantages

- Users can *move around freely* within the area of the network with their laptops, handheld devices, etc. and get an internet connection.
- Users are also able to *share files* and other resources with other devices that are connected to the network without having to be cabled to a port.
- Not having to lay lots of *cables* and put those through walls etc. can be a considerable advantage in terms of time and expense. It also makes it easier to add extra devices to the network, as no new cabling is needed.
- If you are a *business* such as a cafe, having a wireless network that is accessible to customers can bring you extra business. Customers generally love wireless networks because they are convenient.
- Wireless networks can sometimes handle a *larger amount of users* because they are not limited by a specific number of connection ports.
- *Instant transfer of information* to social media is made much easier. For instance, taking a photograph and uploading it to Facebook can generally be done much quicker with wireless technology.

1.4.Limitations

(a) Bandwidth

- Bandwidth is still a limited resource in wireless environments. When transmitting data, users must sometimes send smaller bits of data to accommodate within the available bandwidth so that the information moves very quickly.
- The size of the device that is accessing the information is also still an issue. Most recent phones and PDAs have small screens, often only a couple of inches in diameter, and smaller memory, and it is hard to read large documents on them. These may require information of lesser bandwidth.
- Larger computing devices connected in wireless environments may require more bandwidth information as there is no constraint on the screen and the memory.
- The available wireless local networks in the market operate with a maximum of 55 Mbps whereas some of the user's applications aggregate demand is10 Gbps. This imbalance forces us to have clever wireless networking environments.
- Many applications need to be reconfigured if they are going to be used through wireless connections. Most client/server applications rely on a persistent connection, which is not the case with wireless applications. Transactional systems require safeguards for dropped wireless connections (due to bandwidth limitations).

(b) Frequency Spectrum

- The frequency spectrum is limited and finite. The number of users who can be connected to a wireless network at a given time are limited. However, dynamic channel allocation schemes can be used to optimize the frequency usage of the given wireless communication area.

(c) Power

- The power density from a wireless antenna decreases rapidly with the square of the distance as one move away from the antenna. However, because radio frequency (RF) energy travels as waves, there are effects from reflections, interactions among waves from multiple antennas, and spikes of intensity due to each antenna pattern. This produces a pattern of peaks and valleys in field intensity as one move away from the source.
- The intensity of RF energy depends onseveral factors, including design characteristics of the antenna, power transmitted to the antenna, height of the antenna, and distance from the antenna.

(d) Interference

- Radio transmission cannot be protected against interference using shielding as this is done in coaxial cable or shielded twisted pair.
- For example, electrical engines and lightning cause severe interference and result in higher loss rates for transmitted data or higher bit error rates respectively.

(e) High delays, large delay variation

- A serious problem for communication protocols used in today's Internet (TCP/IP) is the big variation in link characteristics.
- In wireless systems, delays of several seconds can occur, and links can be very asymmetrical (i.e., the links offer different service quality depending on the direction to and from the wireless device).
- Applications must be tolerant and use robust protocols.

(f) Lower security, simpler to attack

- Not only can portable devices be stolen more easily, but the radio interface is also prone to the dangers of eavesdropping.
- Wireless access must always include encryption, authentication, and other security mechanisms that must be efficient and simple to use.

1.5.Applications

The following applications describe the need of wireless communications.

(a) Vehicles

- Transmission of news, road conditions, weather, music via Digital Audio Broadcasting (DAB)
- Current position of the vehicle can be known via the Global Positioning System (GPS)
- Cars in the same area could build a local ad-hoc network to ensure a minimum safe distance from other cars. This network could also be used to alert other cars and hospitals in case of an accident.

(b) Emergencies and Natural Disasters

- The condition of the patient can be transmitted to the hospital from the ambulance itself. The hospital can then make the necessary arrangements to speed up the network.
- In case of disasters like earthquakes, cyclones, heavy rains, etc. most of the wired networks and the infrastructure based networks completely fail. On demand, ad-hoc networks are the only way for communication in such cases.
- Ad-hoc wireless networks are also useful on the battlefield (in wars) as the existent communication network might have already been destroyed (jammed) by the enemy.

(c) Replacement of Fixed (Wired) Networks

- Remote sensors used for weather forecasts, earthquake detection, etc. can be wireless, this allows freedom from miles of cabling.
- Instead of fixed networks, wireless networks can be used for information display and enforcing security measures in historical monuments, as the cabling required for the fixed network may cause damage to the monument.

(d) Businesses

- A travelling salesman can have instant access to the company's database. Thus, he can easily provide the latest product information to the customers.
- Also, the managers can keep track of the performance of the salesman.
- The laptop can truly be turned into a mobile device.

(e) Infotainment and Entertainment

- Wireless networks can provide instant outdoor internet access.
- Travel guides can push historical information about a building or a place on to the user's mobile devices such as a PDA or a mobile phone.
- Wireless networks can be used to set up ad-hoc gaming consoles during online gaming competitions.

(f) Transport

- Wireless communication could be used to create and co-ordinate car sharing schemes amongst villages where public transport modes are not easily available.

(g) Micro-Commerce

- Small businesses in rural areas often have to travel significant distances to markets or other places where they can distribute their goods, and hence they cannot make arrangements in advance with the buyers.
- Mobile phones could significantly change the logistical issues faced by traders and home entrepreneurs, by providing affordable mobile-based ordering systems and the ability to make more reliable and advance arrangements with business partners or clients.

(h) Healthcare

- New mobile services in rural areas could allow for better connectivityamong rural communities.
- Villages can now create networks to share and discuss health information and advice.

(i) Education

- Educational services could be provided to children in remote villages and communities, particularly where personal computers or connections to the Internet are not available.
- Mobile phones could serve as an essential means for children to connect to one another for educational and peer-learning activities.
- These are particularly important for communities that are either nomadic or transitional on account of displacements due to a natural disaster or for other reasons.

1.6.Wireless Media

- "Wireless" means transmitting signals over invisible radio waves instead of wires.
- Garage door openers and television remote controls were the first wireless devices to become a part of everyday life.
- Even though many mobile and wireless devices are available, there will be manymore in the future. There is no precise classification of such devices, by size,shape, weight, or computing power.

- Currently, laptops are considered the upper end of the mobile device range. The following list gives some examples of mobile and wireless devices graded by increasing performance (CPU, memory, display, input devices etc.).
- However, there is no sharp line between the categories and companies tend to invent more and more new categories.

1. **Sensors:** A very simple wireless device is represented by a sensor transmitting state information. One example could be a switch sensing the office door. If the door is closed, the switch transmits this to the mobile phone inside the office which will not accept incoming calls. Without user interaction, the semantics of a closed door is applied to phone calls.
2. **Embedded controllers**: Many appliances already contain a simple or sometimes more complex controller. Keyboards, mice, headsets, washing machines, coffee machines, hair dryers and TV sets are just some examples. Why not have the hair dryer as a simple mobile and wireless device (from a communication point of view) that is able to communicate with the mobile phone? Then the dryer would switch off as soon as the phone starts ringing – that would be a nice application!
3. **Pager**: As a very simple receiver, a pager can only display short text messages, has a tiny display, and cannot send any messages. Pagers can even be integrated into watches. The tremendous success of mobile phones has made the pager virtually redundant in many countries. Short messages have replaced paging. The situation is somewhat different for emergency services where it may be necessary to page a larger number of users reliably within short time.
4. **Mobile phones**: The traditional mobile phone only had a simple black and white text display and could send/receive voice or short messages. Today,mobile phones migrate more and more toward PDAs. Mobile phones with fullcolor graphic display, touch screen, and Internet browser are easily available.
5. **Personal digital assistant**: PDAs typically accompany a user and offersimple versions of office software (calendar, note-pad, mail). The typicalinput device is a pen, with built-in character recognition translating handwritinginto characters. Web browsers and many other software packagesare available for these devices.
6. **Pocket computer**: The next steps toward full computers are pocket computersoffering tiny keyboards, color displays, and simple versions of programsfound on desktop computers (text processing, spreadsheets etc.).
7. **Notebook/laptop**: Finally, laptops offer more or less the same performanceas standard desktop computers; they use the same software – the only technicaldifference being size, weight, and the ability to run on a battery. Ifoperated mainly via a sensitive display (touch sensitive or electromagnetic),the devices are also known as notepads or tablet PCs.

1.7.Frequency Spectrum

- An ordered array of the components of an emission or wave is called **spectrum**.
- A **frequency spectrum** is the range of frequencies of electromagnetic radiation from zero to infinity.

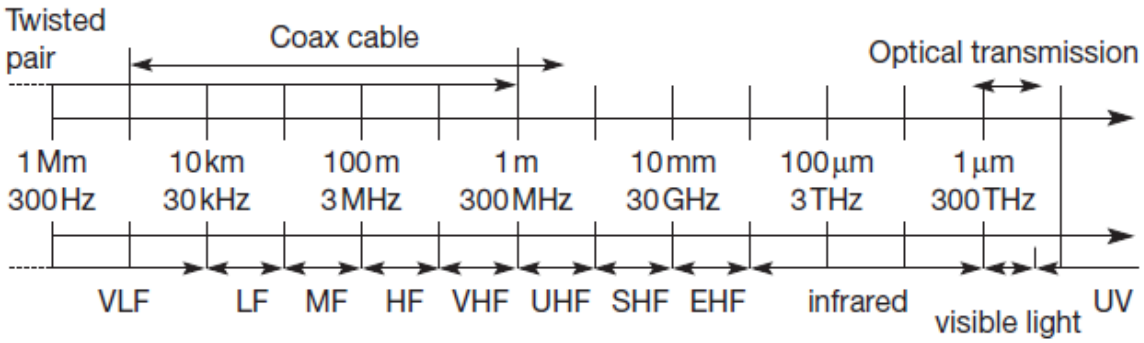


Figure 1.2 Frequency Spectrum

- Radio transmission can take place using many different frequency bands. Each frequency band exhibits certain advantages and disadvantages. Figure above gives a rough overview of the frequency spectrum that can be used for data transmission.The figure shows frequencies starting at 300 Hz and going up to over 300 THz.
- Directly coupled to the frequency is the wavelength λ via the equation: $\lambda = c/f$, where $c \cong 3 \cdot 10^8$ m/s (the speed of light in vacuum) and f the frequency.
- For traditional wired networks, frequencies of up to several hundred kHz are used for distances up to some km with twisted pair copper wires, while frequencies of several hundred MHz are used with coaxial cable (new coding schemes work with several hundred MHz even with twisted pair copper wires over distances of some 100 m). Fiber optics are used for frequency ranges of several hundred THz, but here one typically refers to the wavelength which is, e.g., 1500 nm, 1350 nm etc. (infra red).
- Radio transmission starts at several kHz, the **very low frequency (VLF)** range. These are very long waves. Waves in the **low frequency (LF)** range are used by submarines, because they can penetrate water and can follow the earth's surface. Some radio stations still use these frequencies, e.g., between 148.5 kHz and 283.5 kHz in Germany. The **medium frequency (MF)** and **high frequency (HF)** ranges are typical for transmission of hundreds of radio stations either as amplitude modulation **(AM)** between 520 kHz and 1605.5 kHz, as short wave **(SW)** between 5.9 MHz and 26.1 MHz, or as frequency modulation **(FM)** between 87.5 MHz and 108 MHz. The frequencies limiting these ranges are typically fixed by national regulation and, vary from country to country. Short waves are typically used for (amateur) radio transmission around the world, enabled by reflection at the ionosphere. Transmit power is up to 500 kW – which is quite high compared to the 1 W of a mobile phone.
- As we move to higher frequencies, the TV stations follow. Conventional analog TV is transmitted in ranges of 174–230 MHz and 470–790 MHz using the very high frequency **(VHF)** and ultra-high frequency **(UHF)** bands. In this range, digital audio broadcasting (DAB) takes place as well (223–230 MHz and 1452–1472 MHz) and digital TV is planned or currently being installed (470– 862 MHz), reusing some of the old frequencies for analog TV. UHF is also used for mobile phones with analog technology (450–465 MHz), the digital GSM (890–960 MHz, 1710–1880 MHz), digital cordless telephones following the DECT standard (1880–1900 MHz), 3G cellular systems following the

UMTS standard (1900–1980 MHz, 2020–2025 MHz, 2110–2190 MHz) and many more. VHF and especially UHF allow for small antennas and relatively reliable connectionsfor mobile telephony.

- **Super high frequencies (SHF)** are typically used for directed microwavelinks (approx. 2–40 GHz) and fixed satellite services in the C-band (4 and6 GHz), Ku-band (11 and 14 GHz), or Ka-band (19 and 29 GHz). Some systemsare planned in the **extremely high frequency (EHF)** range which comes closeto infrared. All radio frequencies are regulated to avoid interference, e.g., theGerman regulation covers 9 kHz–275 GHz.
- The next step into higher frequencies involves optical transmission, whichis not only used for fiber optical links but also for wireless communications.**Infrared (IR)** transmission is used for directed links, e.g., to connect differentbuildings via laser links. The most widespread IR technology, infrared data association(IrDA), uses wavelengths of approximately 850–900 nm to connectlaptops, PDAs etc. Finally, visible light has been used for wireless transmissionfor thousands of years. While light is not very reliable due to interference, but itis nevertheless useful due to built-in human receivers.

1.8.Spread Spectrum

- As the name implies, **spread spectrum** techniques involve spreading the bandwidthneeded to transmit data.

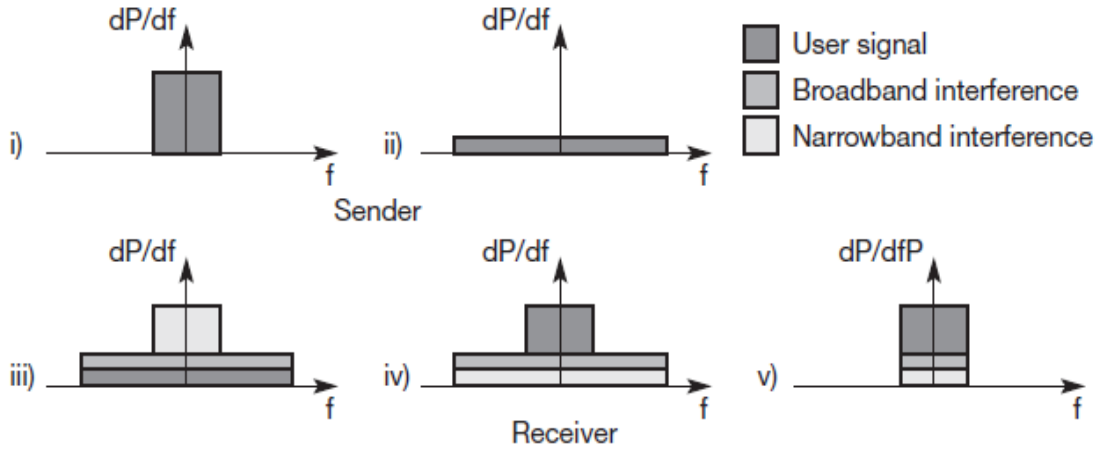


Figure 1.3 Spreading and Despreading of the User Signal

- The figure 1.3 above shows the basic steps involved in this technology.

(a) It is the idealized narrowband signal that is to be transmitted by the sender.

(b) This narrowband signal is first converted in to broadband signal i.e. the signal is spread. The energy needed to transmit the signal is still the same; however, the required power level reduces.

(c) During transmission, narrowband and broadband interference gets added to the spread signal. The sum of interference and user signal is received.

(d) The receiver now knows how to despread the signal, converting the spread user signal into a narrowband signal again, while spreading the narrowband interference and leaving the broadband interference.

(e) The signal is now applied to a band pass filter that cuts off the frequencies to the left and right of the narrowband signal. The original user signal can now be recovered.

- The above scenario can also be applied simultaneously to many channels.

- Figure 1.4 below shows a snapshot of the channel quality of six channels using FDM. The situation may be completely different at the next instant.

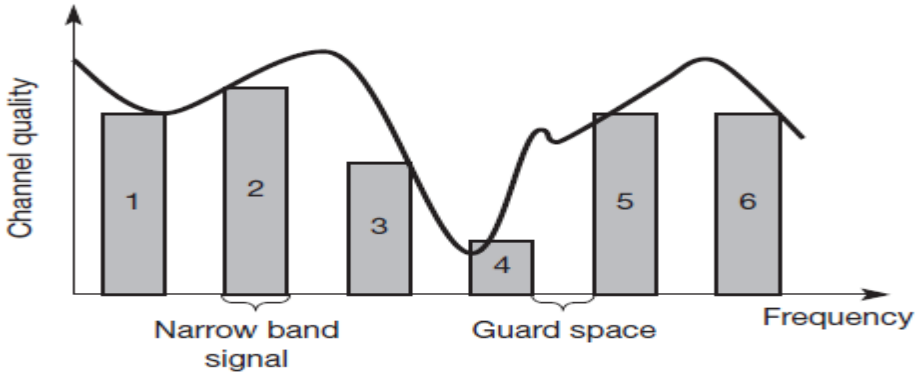


Figure 1.4 Multiple Channels Making use of Narrowband Signals

- Each channel has its own narrowband frequency of transmission. Guard spaces are required between the channels to avoid adjacent channel interference.
- Using FDM requires careful planning of the frequencies. Also, we can see that the quality of channels 3 and 4 is too bad (due to narrowband interference) to recover the data.
- In order to solve these problems, we can apply spread spectrum to all the six channels.
- As shown in figure 1.5 below, the narrow band signals for each of the channels are converted to broadband signals.

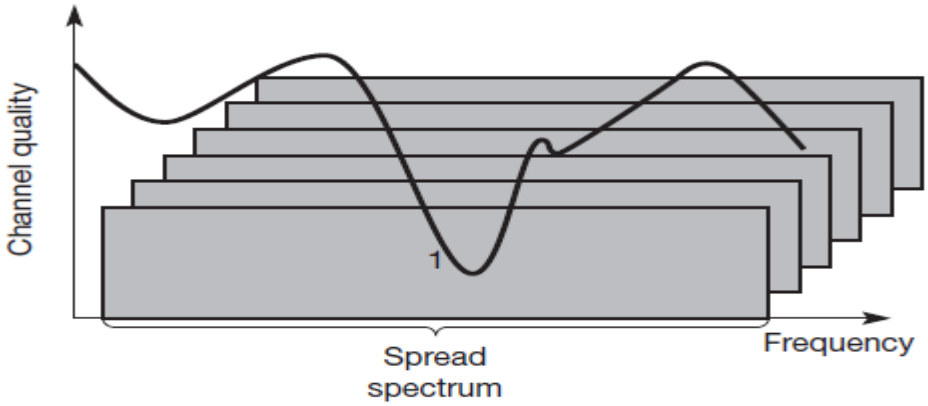


Figure 1.5 Spread Spectrum to avoid Narrowband Interference

- Each channel now uses the same frequency band, CDM has to be used to separate each channel.
- Each channel has to be assigned its own code for transmitting and recovering data.

Advantages of Spread Spectrum

- Provides resistance to narrowband interference.
- It allows co-existence of several signals without the need of dynamic co-ordination among the signals.
- Relatively high security allows use in military applications. In fact, one of the key applications of spread spectrum is for building anti-jam communication systems, which is a communication system designed to resist intentional jamming (by the enemy) in a hostile environment.

Disadvantages of Spread Spectrum

- Increased complexity of the senders and receivers.
- The spread signal requires a larger frequency band.

- The spread signals increase the background noise level and may interfere with other transmission.
- Precise power control is necessary.

1.9.Direct Sequence Spread Spectrum (DSSS)

- In this scheme, the user signal is spread by performing an XOR with a fixed sequence called as a chipping sequence.
- As shown in figure 1.6, a user signal 01, is XORed with the chipping sequence 0110101, the resulting signal is either 0110101 (if the user bit is 0) or its complement 1001010 (if the user bit is 1).

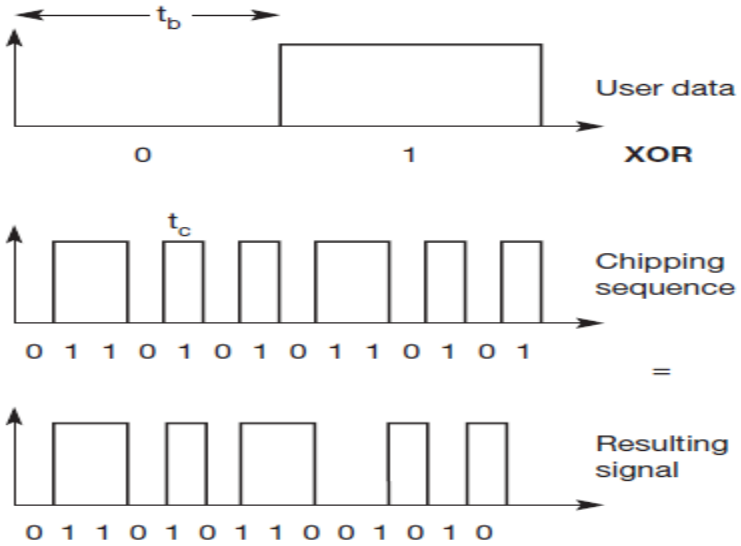


Figure 1.6 Spreading of signal using DSSS

- Each user bit has duration of t_b. The chipping sequence consists of smaller pulses called chips each having duration of t_c.
- The spreading factor $S = t_b/t_c$, determines the bandwidth of the spread signal. Thus, if the original signal needed a bandwidth of B, the spread signal would require a bandwidth of S*B.
- Barker codes are usually used for spreading the signals as these codes are insensitive to multipath propagation and also exhibit good robustness against interference.

DSSS Transmitter

- The figure 1.7 shows the typical DSSS transmitter.
- The user data is first XORed with the chipping sequence to obtain the spread signal.
- This signal is then converted to an analog baseband signal by digital modulation.
- The baseband signal is then subject to analog modulation and transmitted.

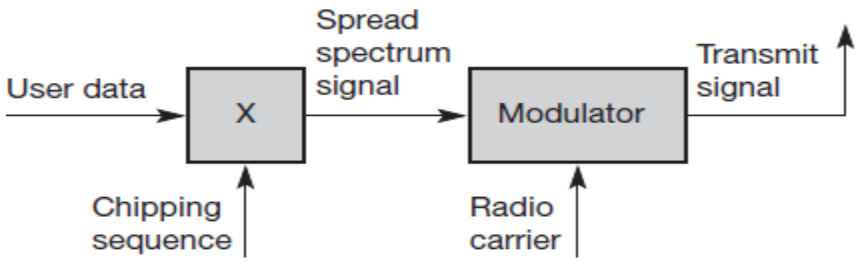


Figure 1.7 DSSS Transmitter

DSSS Receiver

- The DSSS receiver is comparatively more complex than the transmitter (refer figure 1.8).
- The received signal is first converted to the baseband signal by the demodulator. Additional mechanisms also need to be applied as data may be distorted due to noise and multipath propagation.
- The low pass filtered signal is now applied to a correlator; the correlator performs two steps which need precise synchronization with the sender.
  - Firstly, the signal is once again XORed with a chipping sequence to generate products; this chipping sequence is the same as that used by the transmitter to transmit the data.
  - The integrator then adds all the products.
- For each bit period, the output of the integrator is fed to the decision unit that decides whether the user data is a binary 0 or 1.

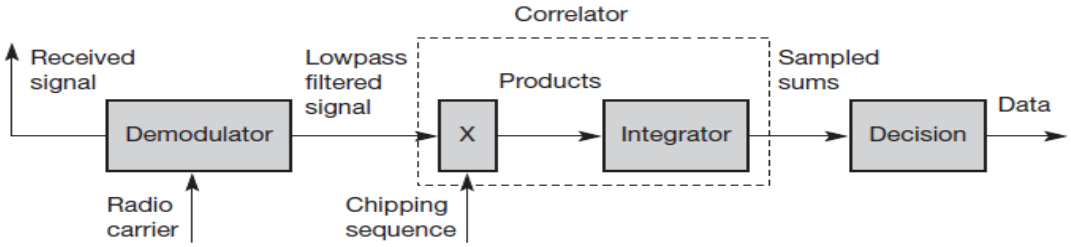


Figure 1.8 DSSS Receiver

Advantages of DSSS

- Reduces frequency selective fading.
- In case of cellular systems, several base stations can use the same frequency for transmission.
- A soft handover is possible using DSSS.

Disadvantages of DSSS

- The overall system is complex to implement.
- Precise power control required.
- Synchronization required between the sender and the receiver.

1.10. Frequency Hopping Spread Spectrum (FHSS)

- For **frequency hopping spread spectrum (FHSS)** systems, the total available bandwidth is split into many channels of smaller bandwidth plus guard spaces between the channels.
- Transmitter and receiver stay on one of these channels for a certain time and then hop to another channel. This system implements FDM and TDM.
- The pattern of channel usage is called the **hopping sequence**, the time spend on a channel with a certain frequency is called the **dwell time**.
- FHSS comes in two variants, slow and fast hopping (refer figure 1.9)

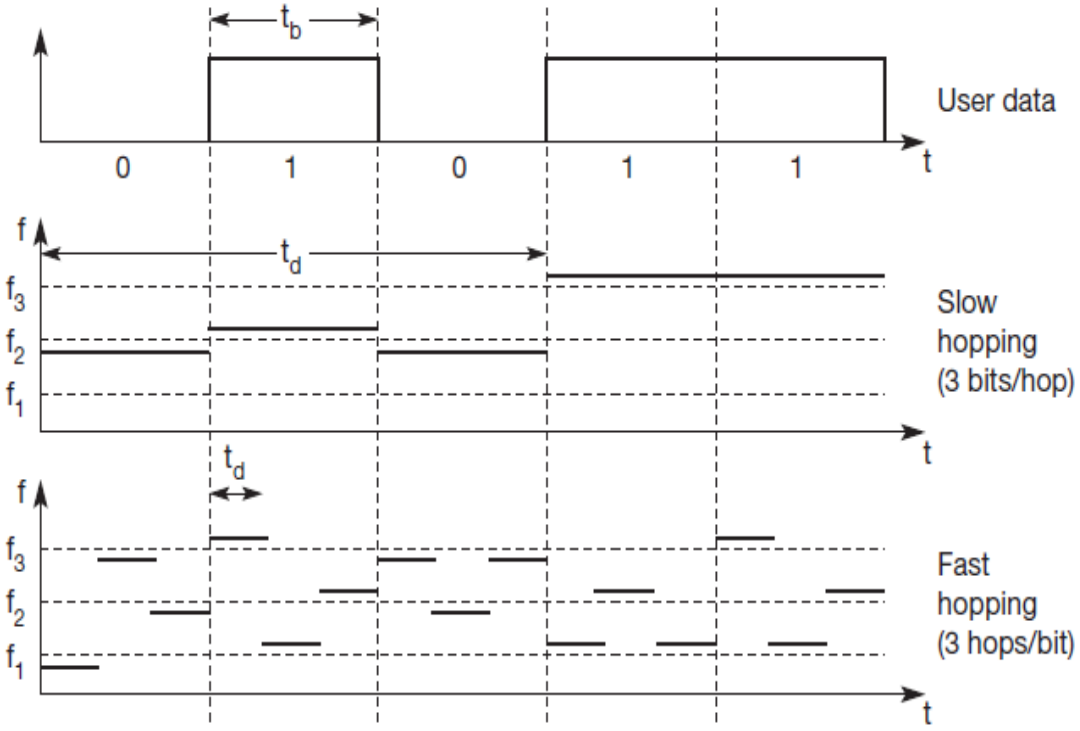


Figure 1.9 Slow Hopping and Fast Hopping

Sr. No.	Slow Hopping	Fast Hopping
1	Several user bits transmitted at the same frequency. Therefore, $t_d > t_b$	Several frequencies may be used to transmit a single user bit.
2	Provides lesser resistance to narrowband interference.	Better resistance against narrowband interference and frequency selective fading as compared to slow hopping.
3	Lower security as compared to fast hopping.	Better security as compared to slow hopping.
4	Slow hopping systems are cheaper and have relaxed tolerances.	Comparatively costlier with smaller tolerances.
5	Very tight synchronization is not required.	Very tight synchronization is required.
6	Can be used GSM.	Used by Bluetooth.

FHSS Transmitter

- The simplified block diagram of FHSS transmitter is shown in the figure 1.10.
- The user data is first converted to a narrowband signal using digital modulation (FSK or BPSK).
- Frequency hopping is then performed using the hopping sequence. The hopping sequence is applied to the frequency synthesizer that generates the corresponding carrier frequencies.
- Analog modulation is then applied to shift the narrowband frequency by the carrier frequency.
- Thus, the spread signal is generated.
- The hopping sequences used by various transmitters should have low cross-correlation among them.

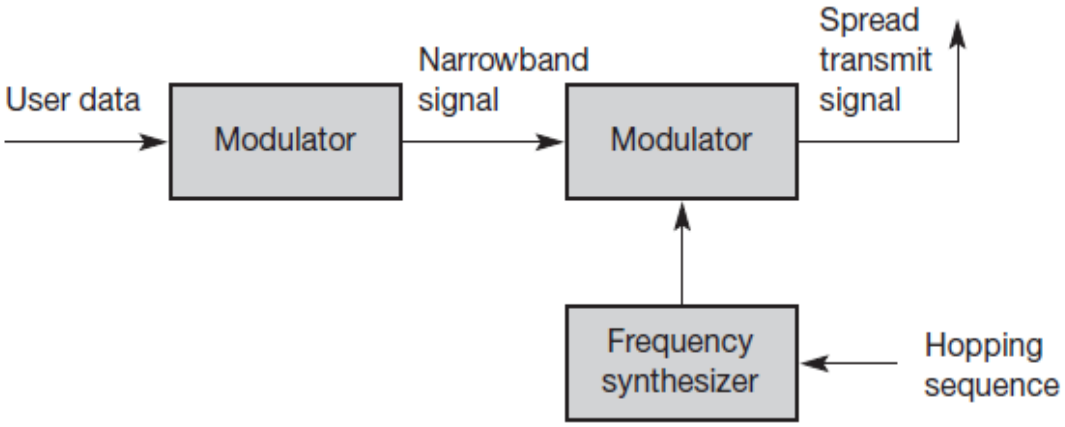


Figure 1.10 FHSS Transmitter

FHSS Receiver

- As shown in figure 1.11, the reverse process needs to be applied at the receiver.
- The received signal is first subject to a demodulation process to generate the narrowband signal. The same hopping sequence used to spread the data needs to be regenerated at the receiver and then applied to the frequency synthesizer.
- The narrowband signal is then demodulated again to get the user data.

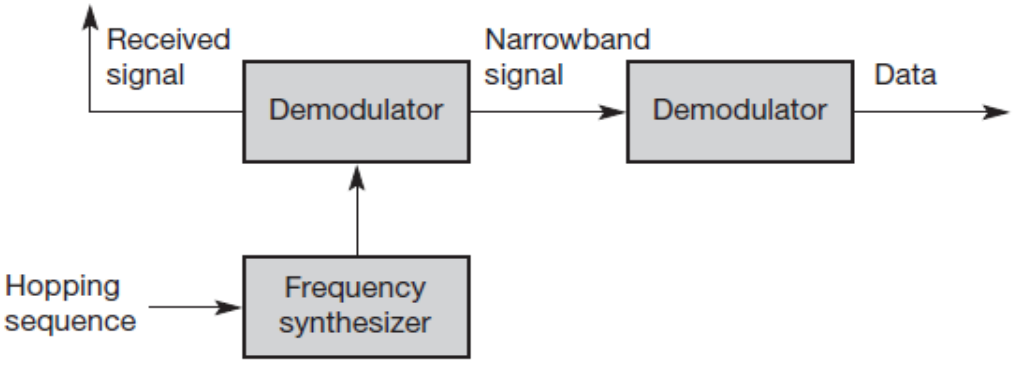


Figure 1.11 FHSS Receiver

Advantages of FHSS

- Spreading of signals is simpler.
- Frequency selective fading and interference is limited to short period only.
- Use only a small portion of the total bandwidth at any time.

Disadvantages of FHSS

- Not as robust as DSSS.
- Signals are easier to detect, thus, lower security.

Sr. No.	DSSS	FHSS
1	Implementation is complex.	Simple to implement.
2	At any time, it uses all of the total available bandwidth.	It uses only a small portion of the available bandwidth at any time.
3	It provides better security; without knowing the spreading code it is very hard to detect the signal.	Signals are easier to detect.
4	More resistant to frequency selective fading.	Less resistant to frequency selective fading.
5	More resistant to multipath propagation.	Less resistant to multipath propagation.

1.11. Multiplexing

- Multiplexing describes how several users can share a medium with minimum or no interference.
- In wireless communication, multiplexing can be carried out in four dimensions viz. space, time, frequency, and code.
- The goal of multiplexing is to assign space, time, frequency, and code to each communication channel for maximum medium utilization and minimum interference.

(a) Space Division Multiplexing (SDM)

- Consider six communication channels k_1 to k_6.
- We use 3D co-ordinate system with frequency, time, and code as x, y and z-axis respectively.
- Each of the channels are mapped on to the spaces (figure 1.12 shows for only three channels).

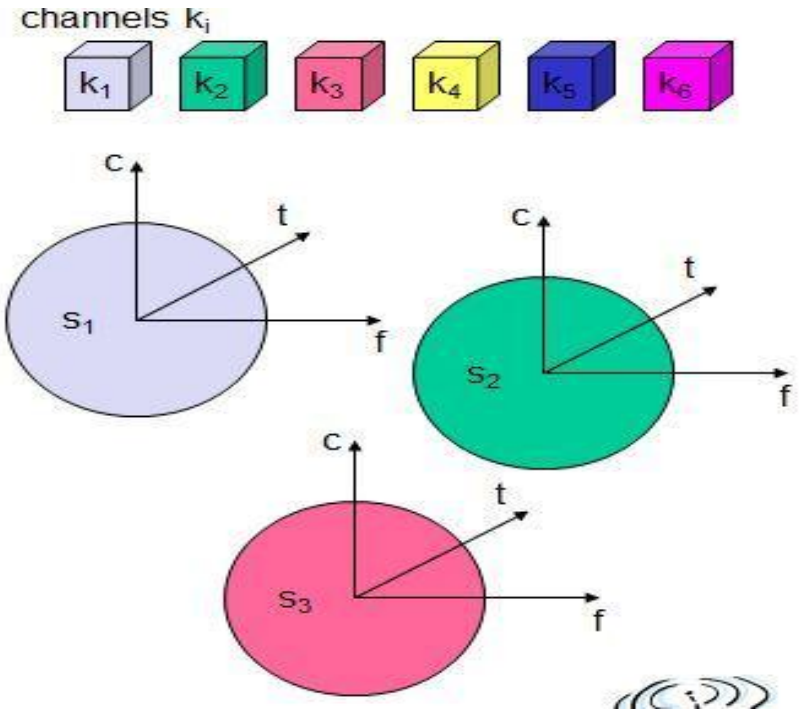


Figure 1.12 Space Division Multiplexing

- The interference range of one space should not overlap with the interference range of the other space.
- The space between interference ranges is called as the guard space.
- Thus, SDM separates the senders via a space wide enough to avoid interference.
- **Advantages**: Very simple and easy to implement.
- **Disadvantages**: Clearly causes a waste of space. If multiple users want to use the space for communication, other multiplexing schemes like FDM, TDM or CDM need to be applied.

(b) Frequency Division Multiplexing (FDM)

- As shown in figure 1.13, this scheme divides the frequency dimension into several non-overlapping frequency bands.
- Each channel is allocated its own frequency band.
- Guard spaces are required between the bands to avoid adjacent channel interference.
- To receive the signal, receiver has to tune in to a particular frequency.
- **Advantages:**
  - No complex co-ordination required between the sender and the receiver.
  - Works for analog signals also.
- **Disadvantages:**
  - Waste of bandwidth if the traffic is distributed unevenly.
  - Inflexible

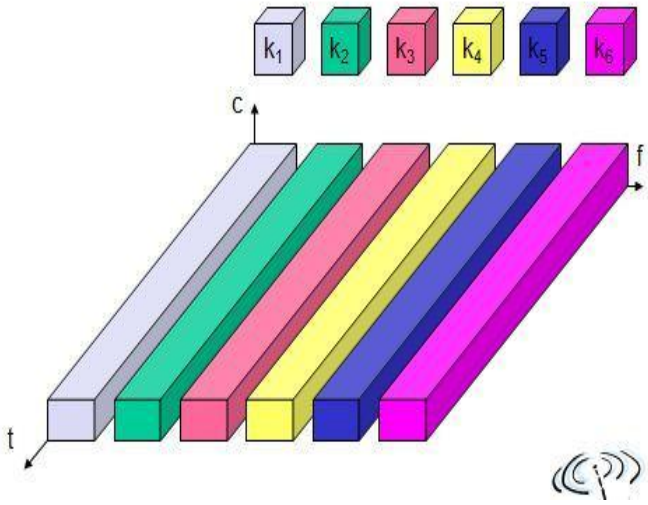


Figure 1.13 Frequency Division Multiplexing

(c) Time Division Multiplexing (TDM)

- Each channel is given the entire bandwidth for a certain period of time.
- As shown in figure 1.14, all the channels use same frequency but at different point of time.
- To avoid co-channel interference, guard spaces are required.
- In order to receive the signal, receive need to tune in at the right time.
- **Advantages:**
  - Flexible: Time allocation can be done with respect to load.
  - Efficient channel utilization
  - High throughput
- **Disadvantages:**
  - Tight synchronization required between the sender and the receiver.
  - Complex to implement.

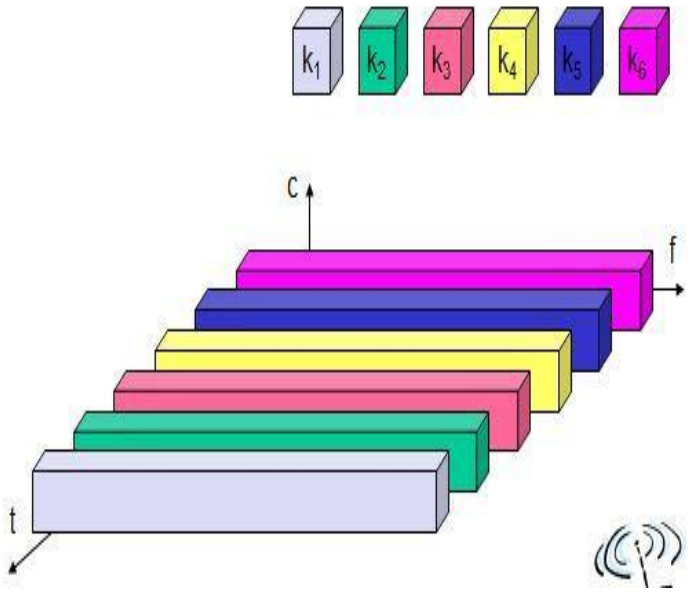


Figure 1.14 Time Division Multiplexing

(d) Code Division Multiplexing (CDM)

- As shown in figure 1.15, in this scheme channel separation is done with the help of codes i.e. each channel is assigned a unique code.
- All the senders now transmit at the same time with same frequency but different codes.
- Guard spaces are required to avoid interference.
- **Advantages**:
  - Efficient bandwidth utilization
  - No co-ordination required between sender and receiver
  - Provides good protection against tapping and interference
- **Disadvantages:**
  - Lower data rates
  - Precise power control is necessary.

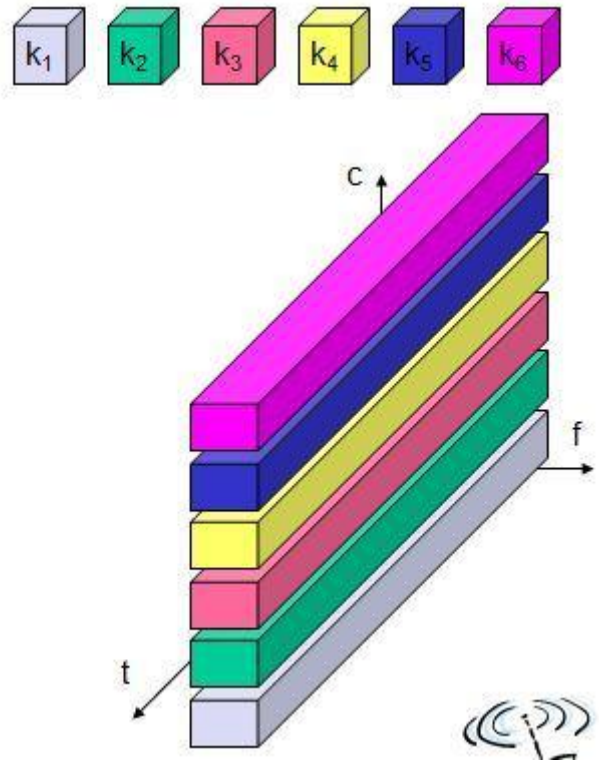


Figure 1.15 Code Division Multiplexing

1.12. Modulation Techniques

- Modulation is the process of converting analog or digital information to a waveform suitable for transmission over a given medium.
- *Consider a cosine function* $g(t) = A_t \cos(2\pi f_t t + \varphi_t)$.
- This function has three parameters: amplitude A_t, frequency f_t, and phase $\varphi_t$which may be varied in accordance with data or another modulating signal.
- For **digital modulation**, which is the main topic in this section, digital data (0 and 1) is translated into an analog signal (baseband signal).
- Digital modulation is required if digital data has to be transmitted over a medium that only allows for analog transmission.

(a) Amplitude shift keying

- Figure 1.16 illustrates **amplitude shift keying (ASK)**, the most simple digital modulation scheme.
- The two binary values, 1 and 0, are represented by two different amplitudes. In the example, one of the amplitudes is 0 (representing the binary 0).
- This simple scheme only requires low bandwidth, but is very susceptible to interference.
- Effects like multi-path propagation, noise, or path loss heavily influence the amplitude.
- In a wireless environment, a constant amplitude cannot be guaranteed, so ASK is typically not used for wireless radio transmission.
- However, the wired transmission scheme with the highest performance, namely optical transmission, uses ASK. Here, a light pulse may represent a 1, while the absence of light represents a 0.
- ASK can also be applied to wireless infra red transmission, using a directed beam or diffuse light.

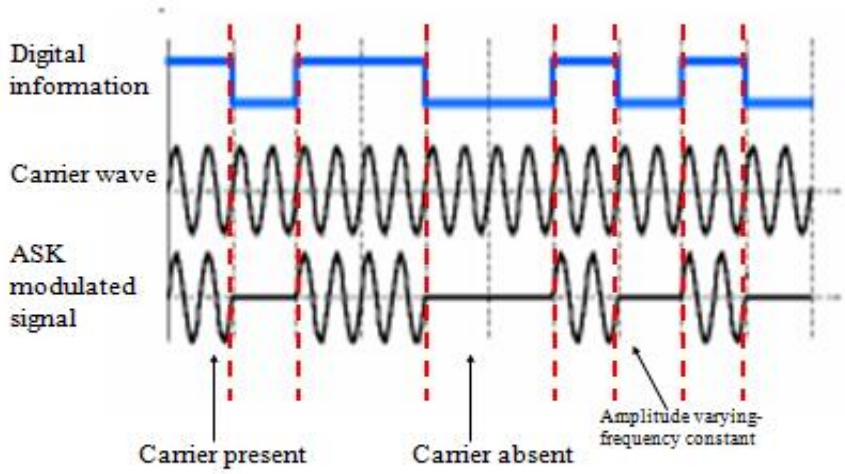


Figure 1.16 Amplitude Shift Keying

(b) Frequency shift keying

- A modulation scheme often used for wireless transmission is **frequency shiftkeying (FSK)** (see figure 1.17).
- The simplest form of FSK, also called **binary FSK (BFSK)**, assigns one frequency f1 to the binary 1 and another frequency f2 to the binary 0.
- A very simple way to implement FSK is to switch between two oscillators, one with the frequency f1 and the other with f2, depending on the input.
- To avoid sudden changes in phase, special frequency modulators with **continuous phase modulation**, **(CPM)** can be used. Sudden changes in phase cause high frequencies, which is an undesired side-effect.

- A simple way to implement demodulation is by using two bandpass filters, one for f1 the other for f2.
- A comparator can then compare the signal levels of the filter outputs to decide which of them is stronger.
- FSK needs a larger bandwidth compared to ASK but is much less susceptible to errors.

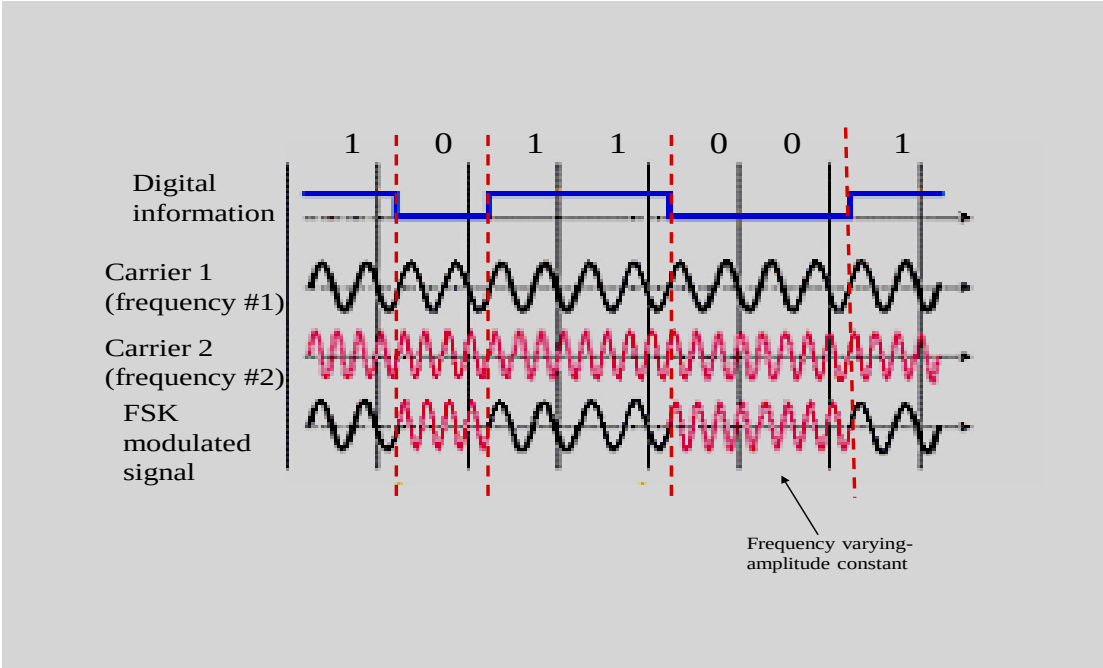


Figure 1.17 Frequency Shift Keying

(c) Phase shift keying

- Finally, phase shift keying (PSK) uses shifts in the phase of a signal to represent data.
- Figure 1.18 shows a phase shift of 180° or π as the 0 follows the 1 (the same happens as the 1 follows the 0).
- This simple scheme, shifting the phase by 180° each time the value of data changes, is also called binary PSK (BPSK).
- A simple implementation of a BPSK modulator could multiply a frequency f with +1 if the binary data is 1 and with –1 if the binary data is 0.
- To receive the signal correctly, the receiver must synchronize in frequencyand phase with the transmitter. This can be done using a **phase lock loop (PLL)**.
- Compared to FSK, PSK is more resistant to interference, but receiver and transmitterare also more complex.

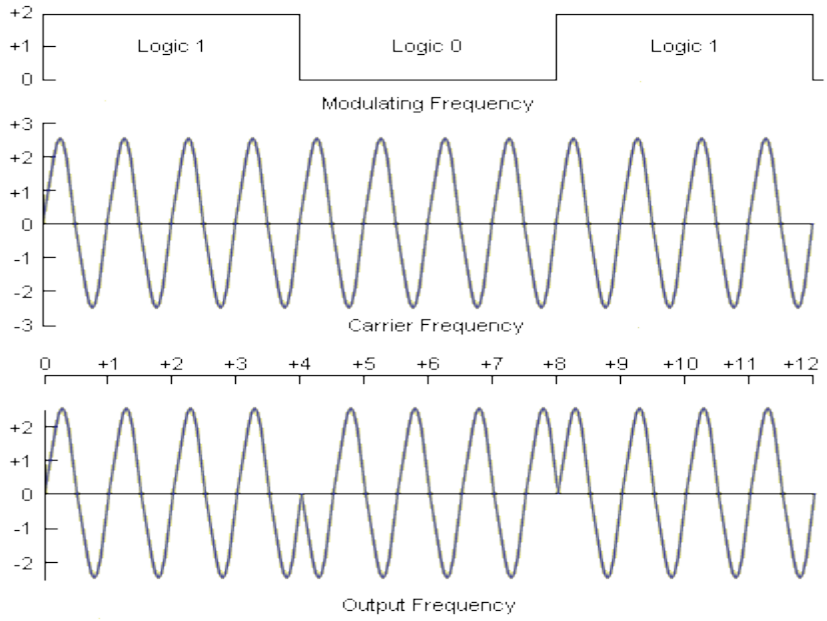


Figure 1.18 Phase Shift Keying

1.13. Multiple Access Methods

- Multiple access techniques are used to allow a large number of mobile users to share the allocated spectrum in the most efficient manner.
- As the spectrum is limited, so the sharing is required to increase the capacity of cell or over a geographical area by allowing the available bandwidth to be used at the same time by different users.
- And this must be done in a way such that the quality of service doesn't degrade within the existing users.

(a) Space Division Multiple Access (SDMA)

- It implements SDM.
- It divides the available space into cells and further divides the cells into sectors. This allows for frequency reuse in different sectors by using directed antennas.
- Typically, SDMA is never used in isolation. It is always combined with some other schemes like FDMA, TDMA, CDMA, etc.
- A new application of SDMA comes up together with beam-forming antenna arrays.
- Single users are separated in space by individual beams. This can improve the overall capacity of a cell (e.g., measured in bit/s/m2 or voice calls/m2) tremendously.

(b) Frequency Division Multiple Access (FDMA)

- It implements FDM.
- In pure FDMA, non-overlapping frequency bands are assigned to users on a continuous time basis.

- FDMA is usually combined with TDMA (as in GSM); frequency allocation can now vary with time according to a certain pattern called as the hopping pattern.
- In cellular networks, FDM is often used to provide the base station and the mobile station a simultaneous access to the medium. The two partners establish a duplex channel.
- The scheme itself is called as Frequency Division Duplex (FDD). The mobile station communicates with the base station at one frequency whereas the base station communicates with the mobile host at another frequency.
- Thus, the communication in the two directions is now separated via two different frequencies.
- The frequency from the mobile station to the base station is called as uplink frequency and the frequency from the base station to the mobile station is called as downlink frequency.

(c) Time Division Multiple Access (TDMA)

- It implements TDM.
- Different users can access the medium at different time.
- This is much flexible scheme as compared to pure FDMA.
- In this mode, the receiver just has to tune in to the frequency at the right time.
- This technique works well with slow voice data signals, but it's also useful for compressed video and other high-speed data.
- The basic GSM (Global System of Mobile Communications) cellular phone system is TDMA-based.

(d) Code Division Multiple Access (CDMA)

- CDMA (Code-Division Multiple Access) is a channel access method used by various radio communication technologies.
- It is a form of multiplexing, which allows numerous signals to occupy a single transmission channel, optimizing the use of available bandwidth.
- The technology is used in ultra-high-frequency (UHF) cellular telephone systems in the 800-MHz and 1.9-GHz bands.
- CDMA employs analog-to-digital conversion (ADC) in combination with spread spectrum technology.
- Audio input is first digitized into binary elements.
- The frequency of the transmitted signal is then made to vary according to a defined pattern (code), so it can be intercepted only by a receiver whose frequency response is programmed with the same code, so it follows exactlyalong with the transmitter frequency.
- There are trillions of possible frequency-sequencing codes, which enhance privacy and makes cloning difficult.
- The original CDMA standard, also known as CDMA One and still common in cellular telephones in the U.S offers a transmission speed of only up to 14.4 Kbps in its single channel form and up to 115 Kbps in an eight-channel form. CDMA2000 and Wideband CDMA deliver data many times faster.

- CDMA devices use a rake receiver, which exploits multipath delay components to improve the performance of the system.
- In a CDMA system, the same frequency can be used in every cell, because channelization is done using the pseudo-random codes.
- Reusing the same frequency in every cell eliminates the need for frequency planning in a CDMA system.
- CDMA systems use the soft hand off, which is undetectable and provides a more reliable and higher quality signal.

(e) Carrier Sense Multiple Access (CSMA)

- **Carrier sense multiple access** (**CSMA**) is a probabilistic media access control (MAC) protocol in which a node verifies the absence of other traffic before transmitting on a shared transmission medium, such as an electrical bus, or a band of the electromagnetic spectrum.
- *Carrier sense* means that a transmitter uses feedback from a receiver to determine whether another transmission is in progress before initiating a transmission. That is, it tries to detect the presence of a carrier wave from another station before attempting to transmit.
- If a carrier is sensed, the station waits for the transmission in progress to finish before initiating its own transmission. In other words, CSMA is based on the principle "sense before transmit" or "listen before talk".
- *Multiple access* means that multiple stations send and receive on the medium. Transmissions by one node are generally received by all other stations connected to the medium.

CSMA Access Modes

1-persistent

- 1-persistent CSMA is an aggressive transmission algorithm.
- When the sender (station) is ready to transmit data, it senses the transmission medium for idle or busy.
- If idle, then it transmits immediately. If busy, then it senses the transmission medium continuously until it becomes idle, then transmits the message (a frame) unconditionally (i.e. with probability=1).
- In case of a collision, the sender waits for a random period of time and attempts to transmit again unconditionally (i.e. with probability=1).
- 1-persistent CSMA is used in CSMA/CD systems including Ethernet.

Non-persistent

- Non persistent CSMA is a non aggressive transmission algorithm.
- When the sender (station) is ready to transmit data, it senses the transmission medium for idle or busy.
- If idle, then it transmits immediately. If busy, then it waits for a random period of time (during which it does not sense the transmission medium) before repeating the whole logic cycle (which started with sensing the transmission medium for idle or busy) again.

- This approach reduces collision, results in overall higher medium throughput but with a penalty of longer initial delay compared to 1–persistent.

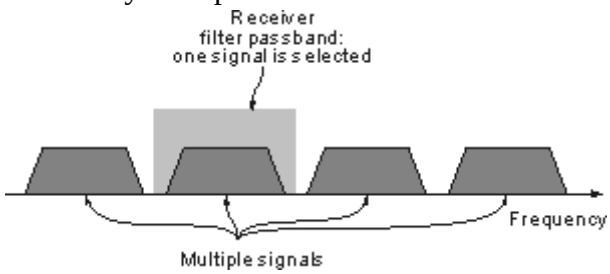
P-persistent

- This is an approach between 1-persistent and non-persistent CSMA access modes.
- When the sender (station) is ready to transmit data, it senses the transmission medium for idle or busy.
- If idle, then it transmits immediately. If busy, then it senses the transmission medium continuously until it becomes idle, then transmits a frame with probability*p*.
- If the sender chooses not to transmit (the probability of this event is *1-p*), the sender waits until the next available time slot.
- If the transmission medium is still not busy, it transmits again with the same probability *p*. This probabilistic hold-off repeats until the frame is finally transmitted or when the medium is found to become busy again (i.e. some other sender has already started transmitting their data).
- In the latter case the sender repeats the whole logic cycle (which started with sensing the transmission medium for idle or busy) again.
- p-persistent CSMA is used in CSMA/CA systems including Wi-Fi and other packet radio systems.

(f) OFDMA

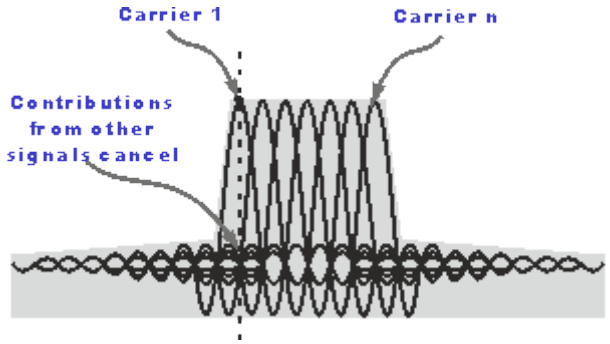
- Orthogonal Frequency Division Multiplexing (OFDM) is a form of signal modulation that divides a high data rate modulating stream placing them onto many slowly modulated narrowband close-spaced subcarriers, and in this way is less sensitive to frequency selective fading.
- Orthogonal Frequency Division Multiplexing or OFDM is a modulation format that is being used for many of the latest wireless and telecommunications standards.
- OFDM has been adopted in the Wi-Fi arena where the standards like 802.11a, 802.11n, 802.11ac and more. It has also been chosen for the cellular telecommunications standard LTE / LTE-A, and in addition to this it has been adopted by other standards such as WiMAX and many more.
- Orthogonal frequency division multiplexing has also been adopted for a number of broadcast standards from DAB Digital Radio to the Digital Video Broadcast standards, DVB.
- Although OFDM, orthogonal frequency division multiplexing is more complicated than earlier forms of signal format, it provides some distinct advantages in terms of data transmission, especially where high data rates are needed along with relatively wide bandwidths.
- OFDM is a form of multicarrier modulation. An OFDM signal consists of a number of closely spaced modulated carriers.

- When modulation of any form - voice, data, etc. is applied to a carrier, then sidebands spread out either side.
- It is necessary for a receiver to be able to receive the whole signal to be able to successfully demodulate the data.
- As a result when signals are transmitted close to one another they must be spaced so that the receiver can separate them using a filter and there must be a guard band between them. This is not the case with OFDM.
- Although the sidebands from each carrier overlap, they can still be received without the interference that might be expected because they are orthogonal to each another. This is achieved by having the carrier spacing equal to the reciprocal of the symbol period.



Traditional view of receiving signals carrying modulation

- To see how OFDM works, it is necessary to look at the receiver. This acts as a bank of demodulators, translating each carrier down to DC. The resulting signal is integrated over the symbol period to regenerate the data from that carrier.
- The same demodulator also demodulates the other carriers. As the carrier spacing is equal to the reciprocal of the symbol period means that they will have a whole number of cycles in the symbol period and their contribution will sum to zero - in other words there is no interference contribution.



OFDM Spectrum

Comparison of SDMA, TDMA, FDMA and CDMA

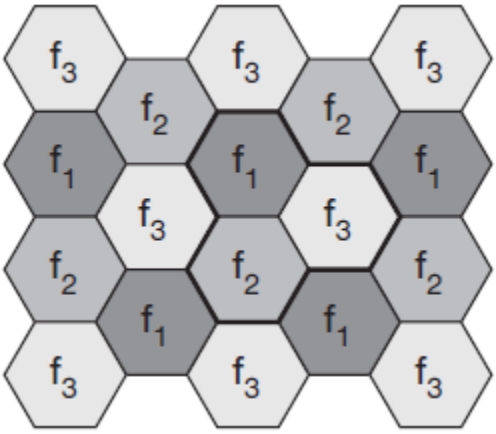
Approach	SDMA	TDMA	FDMA	CDMA
Idea	segment space into cells/sectors	segment sending time into disjoint time-slots, demand driven or fixed patterns	segment the frequency band into disjoint sub-bands	spread the spectrum using orthogonal codes
Terminals	only one terminal can be active in one cell/one sector	all terminals are active for short periods of time on the same frequency	every terminal has its own frequency, uninterrupted	all terminals can be active at the same place at the same moment, uninterrupted
Signal separation	cell structure, directed antennas	synchronization in the time domain	filtering in the frequency domain	code plus special receivers
Advantages	very simple, increases capacity per km²	established, fully digital, flexible	simple, established, robust	flexible, less frequency planning needed, soft handover
Disadvantages	inflexible, antennas typically fixed	guard space needed (multipath propagation), synchronization difficult	inflexible, frequencies are a scarce resource	complex receivers, needs more complicated power control for senders
Comment	only in combination with TDMA, FDMA or CDMA useful	standard in fixed networks, together with FDMA/SDMA used in many mobile networks	typically combined with TDMA (frequency hopping patterns) and SDMA (frequency reuse)	higher complexity, lowered expectations; integrated with TDMA/FDMA

CHAPTER 2

WIRELESS TECHNOLOGY

2.1 Cellular Concept

- The cellular concept refers to a system-level concept that focuses on substituting a single, high-powered transmitter with several low-powered transmitters, each targeted at providing coverage to a small part of the service area.
- The cellular systems for mobile communications implements space division multiplexing.
- Base station covers a certain transmission area called cell wherein it provides its service.
- Mobile stations communicate only via the base station.
- We consider the cell shapes to be hexagonal.However, cells are never perfect hexagons or circles; they vary depending on the environment, weather conditions and even on the system load.
- Cell radii sizes from some 100 m in cities to, e.g., 35 km on the country side (GSM).



Cellular System with 3 Cell Clusters

Advantages and Disadvantages of Cellular System

Advantages:

1. ***Higher capacity***
   Implementing SDM allows frequency reuse.If one transmitter is far away from another,i.e. outside the interference range it can reuse the same frequency.As most of mobile phone systems assign frequencies to certain users,this frequency is blocked for other users .But as frequency is a scarce resource the number of concurrent users per cell is also very limited.
2. ***Less transmission power***
   While power aspects are not a big problem for base stations, they are indeed a problematic for mobile stations.A receiver far away from the base station would need much more transmit power than the current few watts.But energy is a serious problem for mobile handling devices.

3. ***Local interference only***
   Having long distances between sender and receiver results even more interference problems.With the small cell mobile stations and base stations only have to deal with local interference.
4. ***Robustness***
   Cellular systems are decentralized and so,more robust again the failure of single components.If one antenna fails,this only influences communication within small area.

Disadvantages:

1. ***Infrastructure needed***
   Cellular systems need a complex infrastructure to connect all base stations .This includes many antennas, switches for forwarding, location registers to find a mobile station etc,which make the whole system quite expensive.
2. ***Handover needed***
   The mobile station has to perform a handover when changing from one cell to another.Depending on the cell size and the speed of movement,this can happen quite soon
3. ***Frequency planning***
   To avoid interference, frequency spectrum should be distributed properly with a very less range of frequency spectrum.

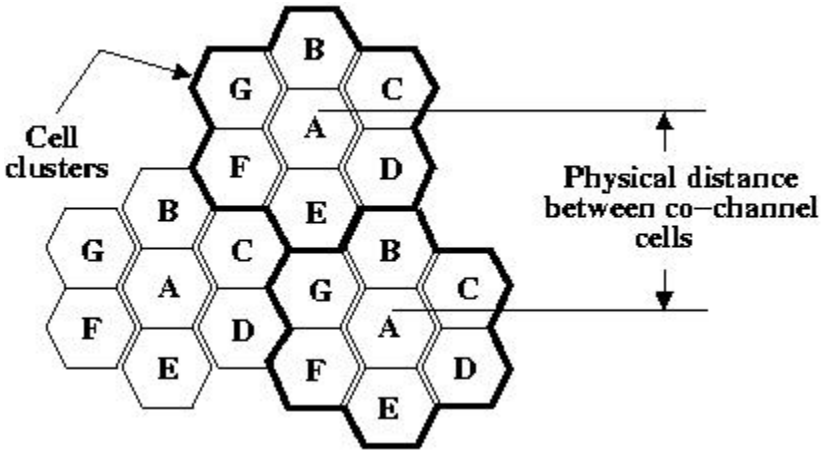
Some important cellular concepts are as follows:

1. Frequency Reuse
2. Channel Assignment Strategies
3. Handoff strategies
4. Interference and system capacity

1. Frequency Reuse

- *Frequency reuse, or, frequency planning, is a technique of reusing frequencies and channels within a communication system to improve capacity and spectral efficiency.*
- Frequency reuse is one of the fundamental concepts on which commercial wireless systems are based that involve the partitioning of an RF radiating area into cells.
- The increased capacity in a commercial wireless network, compared with a networkwith a single transmitter, comes from the fact that the same radio frequency can bereused in a different area for a completely different transmission.
- *Frequency reuse in mobile cellular systems means that frequencies allocated to the service are reused in a regular pattern of cells, each covered by one base station.*
- The repeating regular pattern of cells is called **cluster**.The radio coverage for a cell is popularly called a **footprint**.

- Since each cell is designed to use radio frequencies only within its boundaries, the same frequencies can be reused in other cells not far away without interference, in another cluster. Such cells are called '**co-channel**' cells.
- The reuse of frequencies enables a cellular system to handle a huge number of calls with a limited number of channels.



Frequency reuse technique of a cellular system.

- Figure showsa frequency planning with cluster size of 7, showing the co-channels cells in differentclusters by the same letter.
- The closest distance between the co-channel cells (indifferent clusters) is determined by the choice of the cluster size and the layout ofthe cell cluster.
- Consider a cellular system with S duplex channels available foruse and let N be the number of cells in a cluster. If each cell is allotted K duplexchannels with all being allotted unique and disjoint channel groups we have $S = KN$under normal circumstances.
- Now, if the cluster are repeated M times within thetotal area, the total number of duplex channels, or, the total number of users in thesystem would be $T = MS = KMN$.
- Clearly, if K and N remain constant, then $T \propto M$ and, if T and K remain constant, then $N \propto 1/M$.
- Hence the capacity gain achieved is directly proportional to the number of times a cluster is repeated, as well as, for a fixed cell size, small N decreases the size of the cluster which in turn results in the increase of the number of clusters and hence the capacity.
- However for small N, co-channel cells arelocated much closer and hence more interference.
- The value of N is determined by calculating the amount of interference that can be tolerated for a sufficient quality communication. Hence the smallest N having interference below the tolerated limit is used. However, the cluster size N cannot take on any value and is given only by the following equation

$$K = i^2+ij+j^2$$

Where, K = number of cells per cluster or cluster size

i = number of cells (centre to centre) along any chain of hexagon

j = number of cells (centre to centre) in 60 degree counterclockwise of i.

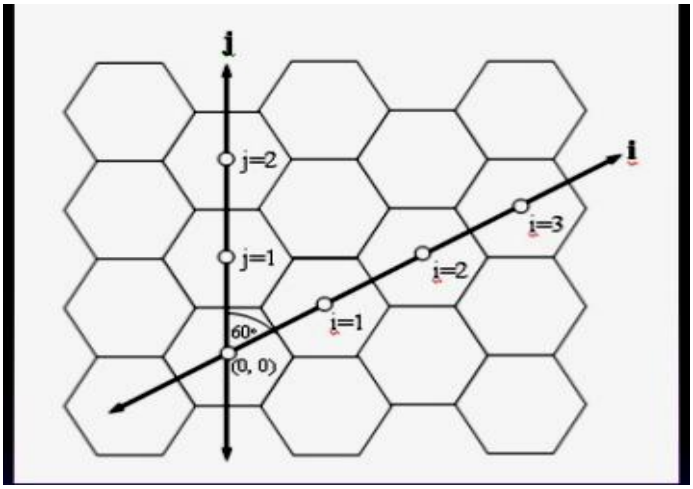
==========

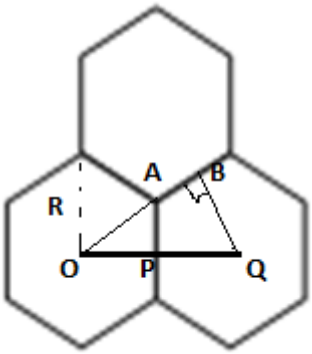
1. Prove that for a hexagonal geometry, the cell cluster size is given by the relation
   $K = i^2+ij+j^2$
   Where, K = number of cells per cluster or cluster size
   i = number of cells (centre to centre) along any chain of hexagon
   j = number of cells (centre to centre) in 60 degree counterclockwise of i.

Solution:

Rules for determining the nearest co-channel cell using "Shift parameters" (i, j) to lay out a cellular system is:

Step 1: Move i cells along any side of ahexagon.
Step 2: Turn 60 degrees anticlockwise
Step 3: Move j cells.
where i and j are shift parameters and can haveinteger value 0, 1, 2, 3, and so on …

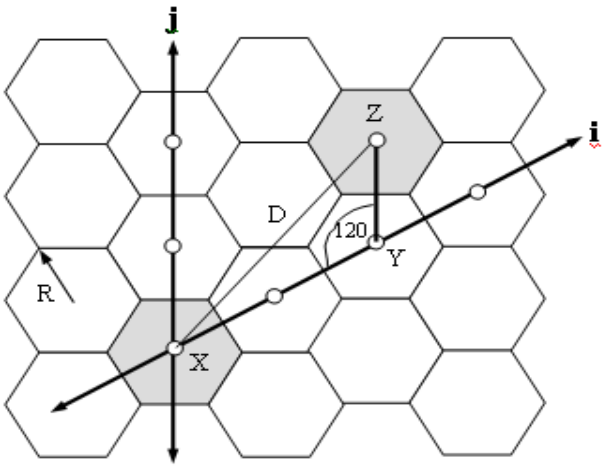




Let R be the distance from the centre of a regular hexagon and any of its vertex. A regular hexagon is one whose sides are also equal to R.
Let d be the distance between the centres of two adjacent regular hexagons.

From the geometry of the figure, OA = R and AB = R/2, OQ = d
Then, OB = OA + AB = R + R/2 = 3R/2
Then, in right-angled ΔOAP, OP = OA sin 60° = (√3/2)R
Let the distance between the centres of two adjacent hexagonal cells, OQ, be denoted by d. Then,
OQ = OP + PQ (where OP = PQ)
Therefore, d = [(√3/2)R + (√3/2)R]
Hence, **d= √3 R**

To establish relation between D, d and shift parameters.



Let d be the distance between two adjacent cells and D be the distance from the centre of the cell under consideration to the centre of nearest co-channel cell.
Using Cosine formula for ΔXYZ in figure above, we have,

$XZ^2 = XY^2 + YZ^2 - 2*XY*YZ \cos 120^\circ$

$D^2 = (i*d)^2 + (j*d)^2 - 2*(i*d)*(j*d)\cos 120^\circ$

$D^2 = (i*d)^2 + (j*d)^2 - 2*(i*d)*(j*d)\ (-1/2)$

$D^2 = (i*d)^2 + (j*d)^2 + (i*d)*(j*d)$

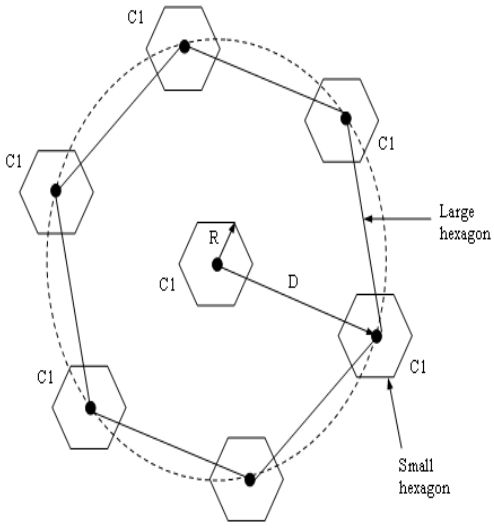
$D^2 = d^2(i^2 + j^2 + i*j)$

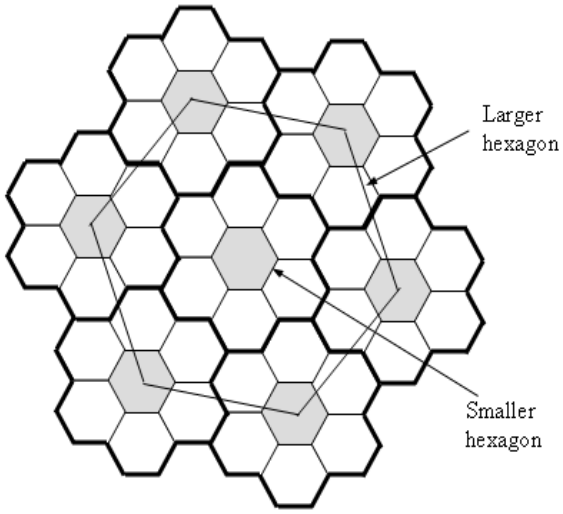
We have **d= √3 R**

Therefore, $D^2 = 3*R^2 * (i^2 + j^2 + i*j)$

Area of small hexagon, $A_{smallhexagon} = (3\sqrt{3}/2) *R^2$

By joining the centres of the six nearest neighboring cochannel cells, a large hexagon is formed with radius equal to D, which is also the cochannel cell separation.





Area of large hexagon, $A_{largehexagon} = (3\sqrt{3}/2) *D^2$

$= (3\sqrt{3}/2) * 3*R^2 * (i^2 + j^2 + i*j)$

Number of cells in largehexagon, $L = D^2/R^2$

Number of cells enclosedby large hexagon,

L = K+6*[(1 /3)* K] = 3 * K
K = D^2/ (3 * R^2);;;
K = $i^2 + j^2 + i * j$

Note: Larger hexagon encloses the entire cluster of k cells plus (1/3)rd the number of cells associated with six other peripheral clusters in the first tier.

2. Prove that for a regular hexagonal geometry, the frequency reuse ratio is given by the relationship $q = \sqrt{(3K)}$, where K = K = i^2+ij+j^2, i and j being the shift parameters.

Solution:
Frequency reuse ratio q = D/R
Where, D= the distance from the centre of the cell under consideration to the centre of nearest co-channel cell.
R = radius of the cell under consideration.
From previous problem, we have,
$D^2 = 3*R^2 * (i^2 + j^2 + i*j)$
Given, $K = i^2 + j^2 + i*j$
Therefore, $D^2 = 3*R^2 *K$
$q= D/R = \sqrt{(3K)}*R/R$
Hence, $q = \sqrt{(3K)}$

2. Channel Assignment Strategies

- With the rapid increase in number of mobile users, the mobile service providers had to follow strategies which ensure the effective utilization of the limited radio spectrum.
- With increased capacity and low interference being the prime objectives,a frequency reuse scheme was helpful in achieving these objectives.
- A variety ofchannel assignment strategies have been followed to aid these objectives.
- Channelassignment strategies are classified into two types: fixed and dynamic, as discussedbelow.

a) Fixed Channel Assignment (FCA)

- In fixed channel assignment strategy each cell is allocated a fixed number of voicechannels.
- Any communication within the cell can only be made with the designated unused channels of that particular cell.
- Suppose if all the channels are occupied, then the call is blocked and subscriber has to wait. This is simplest of the channel assignment strategies as it requires very simple circuitry but provides worst channel utilization.
- Later there was another approach in which the channels were borrowed from adjacent cell if all of its own designated channels were occupied. This was named as ***borrowing strategy*.**
- In such cases the MSC supervises the borrowing process and ensures that none of the calls in progress are interrupted.

b) Dynamic Channel Assignment (DCA)

- In dynamic channel assignment strategy channels are temporarily assigned for use in cells for the duration of the call.

- Each time a call attempt is made from a cell the corresponding BS requests a channel from MSC. The MSC then allocates a channel to the requesting the BS.
- After the call is over the channel is returned and kept in a central pool.
- To avoid co-channel interference any channel that in use in one cell can only be reassigned simultaneously to another cell in the system if the distance between the two cells is larger than minimum reuse distance.
- When compared to the FCA, DCA has reduced the likelihood of blocking and even increased the trunking capacity of the network as all of the channels are available to all cells, i.e., good quality of service.
- But this type of assignment strategy results in heavy load on switching center at heavy traffic condition.

3. Consider that a geographical service area of a cellular system is 4200 km^2. A total of 1001 radio channels are available for handling traffic suppose the area of a cell is 12 km^2.

a) How many times would the cluster of size 7 have to be replicated in order to cover the entire service area? Calculate the number of channels per cell and the system capacity.

b) If the cluster size is decreased from 7 to 4, then does it result into increase in system capacity? Comments on the results obtained.

Solution:

Service area of a cellular system, A_{sys} = 4200 km^2

Coverage area of a cell, A_{cell} = 12 km^2

Total number of channels available,N = 1001

a) To calculate number of clusters, cell capacity and system capacity

Cluster size, K = 7

The coverage area of the cluster, $A_{cluster} = K * A_{cell} = 7 * 12\ km^2 = 84\ km^2$

The number of times that the cluster has to be replicated to cover the entire service area of cellular system, $M = A_{sys}/ A_{cluster}$ = 4200/84 = **50 clusters**

Since total number of available channels are allocated to one cluster, therefore, the number of channels per cell, J = N/K = 1001/7 = **143 channels/cell**

The system capacity C = N*M = 1001*50 = **50050 channels**

b) To calculate new system capacity for reduced K

New cluster size, K = 4

The coverage area of the cluster, $A_{cluster} = K * A_{cell} = 4 * 12\ km^2 = 48\ km^2$

The number of times that the cluster has to be replicated to cover the entire service area of cellular system, $M = A_{sys}/ A_{cluster}$ = 4200/48 = **87 clusters (approx.)**

Since total number of available channels are allocated to one cluster, therefore, the number of channels per cell, J = N/K = 1001/4 = **250 channels/cell**

The system capacity C = N*M = 1001*87 = **87087 channels (87000 channels approx.)**

c) Comments on the result

From (a) and (b), it is seen that, decreasing the cluster size, increases the number of clusters and hence, also increases the system capacity.

---

4. If a 20 MHz of total spectrum is allocated for a duplex wireless cellular system and each simplex channel has 25KHz RF bandwidth find

a) The no. of duplex channels.
b) The no. of channels per cell site where N = 4, N = 7

Solution:

Available bandwidth = 20 MHz
Channel bandwidth = 25 KHz

a) Total no. of duplex channels available = $(20 * 10^6) / (2*25*10^3)$ = **400 channels**
b) If, N=4, the number of channels per cell site = 400/4 = 100
If, N=7, the number of channels per cell site = 400/7 = 57

---

5. If a total of 33 MHz of bandwidth is allocated to a particular cellular system which uses two 25 KHz Simplex channels to provide full Duplex voice. Compute the number of channels available per cell if the system uses:
(i) 4 cell reuse (ii) 7 cell reuse (iii) 12 cell reuse
If 1 MHz of the allocated spectrum is dedicated to control channels, determine an equitable distribution of control channels and voice channels in each cell for each of the three systems

Solution:

Available bandwidth = 33 MHz
Channel bandwidth = 25 KHz

a) Total no. of duplex channels available = $(33 * 10^6) / (2*25*10^3)$ = **660 channels**
b) If, N=4, the number of channels per cell site = 660/4 = 165
If, N=7, the number of channels per cell site = 660/7 = 95
If, N=12, the number of channels per cell site = 660/12 = 55

A 1MHz spectrum of control channels means that $(1 * 10^6) / (2*25*10^3)$ = 20 control channels out of 660 channels available.
If, N=4, the number of control channels = 20/4 = 5. Therefore, out of 165 channels, 5 will be assigned to control channels and 160 to voice channels.
If, N=7, the number of control channels = 20/7 = 3 (approx.). Therefore, out of 95 channels, 3 will be assigned to control channels and 92 to voice channels.
If, N=12, the number of control channels = 20/12 = 2 (approx.). Therefore, out of 55 channels, 2 will be assigned to control channels and 53 to voice channels.

---

6. Consider a single high-power transmitter that can support 40 voice channels over an area of $140km^2$ with the available spectrum. If the area is equally divided into seven smaller areas (cells), each supported by lower transmitters so that each cell supports 30% of the channels, then determine
(a) Coverage area of the cell
(b) Total number of voice channels available in cellular system
(c) Comment on the results obtained.

Solution:

Total service area to be covered = $140km^2$ ……..(given)
Total number of channels available = 40 ……..(given)
Number of cells = 7……...(given)

(a) Coverage area of the cell = Total service area / Number of cells = $140km^2/ 7$ = **$20km^2$**
(b) Number of voice channels per cell = 30% of original channels = 0.3 * 40 = 12 channels/cell.
Total number of voice channels available in cellular system
= Number of channels per cell * Number of cells in the service area
= 12 * 7 = **84 channels**

(c) There is significant increase in the number of available channels in the cellular system. This means, the system capacity is increased.

---

7. Calculate the number of times the cluster of size 4 have to be replicated in order to approximately cover the entire service area of 1765km^2 with the adequate number of uniform-sized cells of 7km^2 each.

Solution:

Size of the cluster, K = 4……..(given)
Area of the cell, A_{cell} = 7km^2……....(given)
Total service area, A_{system} = 1765km^2…....(given)
Area of cluster, $A_{cluster} = K * A_{cell} = 4 * 7 = 28km^2$.
Number of clusters in service area = $A_{system} / A_{cluster}$ = 1765 / 28 = 63.
Hence, the number of times the cluster of size 4 has to be replicated is **63**.

(a) Assume a cellular system of 32 cells with a cell radius of 1.6 km, a total frequency bandwidth that supports 336 traffic channels, and a reuse factor of N = 7. If there are 32 total cells, what geographic area is covered, how many channels are there per cell, and what is the total system capacity? Assume regular hexagonal cellular topology.

(b) Let the cell size be reduced to the extent that the same area as covered in Part (a) with 128 cells. Find the radius of the new cell, and new system capacity.

(c) Comment on the results obtained.

Solution:

(a) Total number of cells in service area = 32……..(given)
Radius of a cell, R = 1.6km…….(given)
The area of a hexagon of radius R = $(3\sqrt{3}/2) * R^2$.
$A_{cell} = (3\sqrt{3}/2) * (1.6\ km)^2 = 6.65\ km^2$,
Hence, the total service area covered = A_{cell} * No. of cells in total area = 6.65 X 32 = **213km^2**.
Total number of available traffic channels = 336 ……...(given)
Frequency reuse pattern (cluster size) = 7 ……..(given)
Hence, the number of channels per cell = 336/7 = **48**
Total system capacity = Number of channels per cell * Number of cells = 48*32 = **1536 channels.**

(b) Total number of available cells = 128 ……..(given)
Total service area = **213km^2**…….(Part a)
Area of a regular hexagonal area = Total service area / Number of cells = 213/128 = **1.66km^2**.
The area of a hexagon of radius R = $(3\sqrt{3}/2) * R^2$.
Therefore, $(3\sqrt{3}/2) * R^2 = (3\sqrt{3}/2) * R^2$
i.e. R = 0.8km
Hence, **radius of new smaller cell, R = 0.8km.**
New system capacity = number of channels per cell * number of cells
= 48 * 128 = 6144 channels
Hence, **new system capacity = 6144 channels**.

(c) It is observed that as the number of cells are increased from 32 to 128 to cover the same service area (**213km^2**), the size of the cell (in terms of radius R) is decreased from 1.6km to 0.8km. Keeping the identical number of channels (48) per cell, the total system capacity is increased from 1536 channels to 6144 channels.

---

9. A mobile communication system is allocated RF spectrum of 25 MHz and uses RF channel bandwidth of 25 kHz so that a total number of 1000 voice channels can be supported in the system.

(a) If the service area is divided into 20 cells with a frequency reuse factor of 4, compute the system capacity.
(b) The cell size is reduced to the extent that the service area is now covered with 100 cells. Compute the system capacity while keeping the frequency reuse factor as 4.
(c) Consider the cell size is further reduced to the extent that the service area is now covered with 700 cells with the frequency reuse factor as 7. Compute the system capacity.
(d) Comment on the results obtained.

Solution:
Number of available voice channels, N = 1000.
Therefore, each cluster can serve 1000 active users simultaneously.
In other words, the capacity of a cluster = 1000.

(a) To compute the system capacity for given K
Number of cells covering the area = 20 (given)
Frequency reuse factor or cluster size = 4 (given)
Number of clusters = number of cells / cluster size = 20 / 4 = 5
Thus, the number of channels in 5 clusters = 1000 * 5 = 5000
Hence, **the system capacity = 5000 users**.

(b) To compute new system capacity for increased number of cells
Number of cells covering the area = 100 (given)
Frequency reuse factor or cluster size = 4 (given)
Number of clusters = number of cells / cluster size = 100 / 4 = 25
Thus, the number of channels in 5 clusters = 1000 *25 = 25000
Hence, **the system capacity = 25000 users**.

(c) To compute new system capacity for increased number of cells and cluster size
Number of cells covering the area = 700 (given)
Frequency reuse factor or cluster size = 7 (given)
Number of clusters = number of cells / cluster size = 700 / 7 = 100
Thus, the number of channels in 5 clusters = 1000 *100 = 100,000
Hence, **the system capacity = 100,000 users**.

(d) It is observed that as the number of cells covering a given service area is increased, the number of clusters having all available number of channels increases. This results into significant increase in the number of active users in the system or the system capacity. Hence, it is concluded that frequency reuse enhances system capacity.

---

10. Determine the distance from the nearest cochannel cell for a cell having a radius of 0.64km and a cochannel reuse factor of 12.

Solution:
The radius of a cell, R = 0.64km (given)
The cochannel reuse factor, q = 12 (given)
To determine the distance from the nearest cochannel cell, D
We know that, q = D/R
Therefore, D = q * R = 12 * 0.64 = 7.68km
Hence, ***the distance from the nearest cochannel cell, D = 7.68km***

---

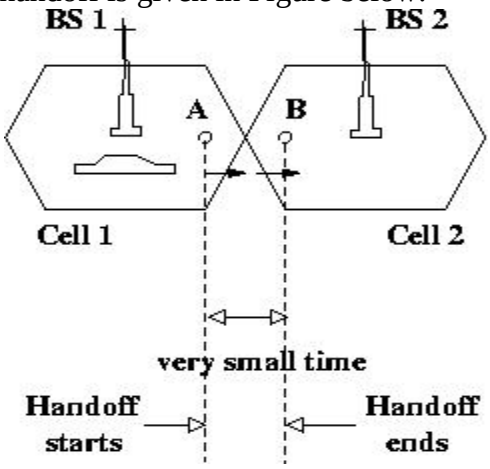
11. Determine the frequency reuse ratio for a cell radius of 0.8km separated from the nearest cochannel cell by a distance of 6.4km.

Solution:
The radius of a cell, R = 0.8km (given)
The distance between nearest cochannel cells, D = 6.4km (given)
To determine the frequency reuse ratio, q

We know that, q = D/R
Therefore, q = 6.4 / 0.8 = 8
Hence, **the frequency reuse ratio, q = 8.**

3. Handoff Process

- When a user moves from one cell to the other, to keep the communication between the user pair, the user channel has to be shifted from one BS to the other without interrupting the call, i.e., when a MS moves into another cell, while the conversation is still in progress, the MSC automatically transfers the call to a new FDD channel without disturbing the conversation. This process is called as *handoff*.
- A schematicdiagram of handoff is given in Figure below.



Handoff scenario at two adjacent cell boundary.

- Processing of handoff is an important task in any cellular system. Handoffs must be performed successfully and be imperceptible to the users.

Factors Influencing Handoffs

The following factors influence the entire handoff process:

a) **Transmitted power**: As we know that the transmission power is different for different cells, the handoff threshold or the power margin varies from cell to cell.
b) **Received power**: the received power mostly depends on the Line of Sight (LoS) path between the user and the BS. Especially when the user is on the boundary ofthe two cells, the LoS path plays a critical role in handoffs.
c) **Area and shape of the cell**: Apart from the power levels, the cell structure also a plays an important role in the handoff process.
d) **Mobility of users**: The number of mobile users entering or going out of a particularcell, also fixes the handoff strategy of a cell.

Handoffs In Different Generations

- In **1G analog cellular system**, the signal strength measurements were made bythe BS and in turn supervised by the MSC. The handoffs in this generation canbe termed as **Network Controlled Hand-Off (NCHO)**. The BS monitors the signal strengths of voice channels to determine the relative positions of the subscriber. The special receivers located on the BS are controlled by the MSC to monitor the signal strengths

of the users in the neighboring cells which appear to be in need of handoff. Based on the information received from the special receivers the MSC decides whether a handoff is required or not. The approximate time needed to make a handoff successful was about 5-10s.

- In the **2G systems**, the MSC was relieved from the entire operation. In thisgeneration, which started using the digital technology, handoff decisions were mobileassisted and therefore it is called **Mobile Assisted Hand-Off (MAHO)**. In MAHO,the mobile center measures the power changes received from nearby base stationsand notifies the two BS. Accordingly the two BS communicate and channel transferoccurs. As compared to 1G, the circuit complexity was increased here whereas thedelay in handoff was reduced to 1-5s.
- In the **3G systems**, the MS measures the power from adjacent BS and automatically upgrades the channels to its nearer BS. Hence this can be termed as **Mobile Controlled Hand-Off (MCHO)**. When compared to the other generations, delay during handoff is only 100ms. The Quality of Service (QoS) has improved a lot although the complexity of the circuitry has further increased which is inevitable.

All these types of handoffs are usually termed as **hard handoff** as there is a shiftin the channels involved. There is also another kind of handoff, called **soft handoff**,as discussed below.

- ***Handoff in CDMA***: In spread spectrum cellular systems, the mobiles share the same channels in every cell. The MSC evaluates the signal strengths received from different BS for a single user and then shifts the user from one BS to the other without actually changing the channel. These types of handoffs are called as **soft handoff** as there is no change in the channel.

Handoff Priority

While assigning channels using either FCA or DCA strategy, a guard channel conceptmust be followed to facilitate the handoffs. This means, a fraction of total availablechannels must be kept for handoff requests. But this would reduce the carriedtraffic and only fewer channels can be assigned for the residual users of a cell. Agood solution to avoid such a dead-lock is to use DCA with handoff priority (demandbased allocation).

A Few Practical Problems in Handoff Scenario

a) **Different speed of mobile users**: With the increase of mobile users in urban areas, microcells are introduced in the cells to increase the capacity. The users with high speed frequently crossing the micro-cells become burdened to MSC as it has to take care of handoffs. Several schemes thus have been designed to handle the simultaneous traffic of high speed and low speed users while minimizing the handoff intervention from the MSC, one of them being the '**Umbrella Cell**' approach. This technique provides large area coverage to high speed users while providing small area coverage to users traveling at low speed. By using different antenna heights and different power

levels, it is possible to provide larger and smaller cells at a same location. The umbrella cell is co-located with few other microcells. The BS can measure the speed of the user by its short term average signal strength and decides which cell to handle that call. If the speed is less, then the corresponding microcell handles the call so that there is good corner coverage. This approach assures that handoffs are minimized for high speed users and provides additional microcell channels for pedestrian users.

b) **Cell dragging problem**: This is another practical problem in the urban area with additional microcells. For example, consider there is a LOS path between the MS and BS1 while the user is in the cell covered by BS2. Since there is a LOS with the BS1, the signal strength received from BS1 would be greater than that received from BS2. However, since the user is in cell covered by BS2, handoff cannot take place and as a result, it experiences a lot of interferences. This problem can be solved by judiciously choosing the handoff threshold along with adjusting the coverage area.

c) **Inter-system handoff**: If one user is leaving the coverage area of one MSC and is entering the area of another MSC, then the call might be lost if there is no handoff in this case too. Such a handoff is called inter-system handoff and in order to facilitate this, mobiles usually have roaming facility.

4. **Interference & System Capacity**

- Susceptibility and interference problems associated with mobile communicationsequipment are because of the problem of time congestion within the electromagneticspectrum. It is the limiting factor in the performance of cellular systems.
- This interference can occur from clash with another mobile in the same cell or because of a call in the adjacent cell. There can be interference between the base stations operating at same frequency band or any other non-cellular system's energy leaking inadvertently into the frequency band of the cellular system.
- If there is an interference in the voice channels, cross talk is heard will appear as noise between the users.
- The interference in the control channels leads to missed and error calls because of digital signaling. Interference is more severe in urban areas because of the greater RF noise and greater density of mobiles and base stations.
- The interference can be divided into 2 parts: co-channel interference and adjacent channel interference.

Co-channel interference (CCI)

- For the efficient use of available spectrum, it is necessary to reuse frequency bandwidth over relatively small geographical areas. However, increasing frequency reuse also increases interference, which decreases system capacity and service quality.
- The cells where the same set of frequencies is used are call **co-channel cells**.
- **Co-channel interference** is the cross talk between two different radio transmitters using the same radio frequency as is the case with the co-channel cells.

- The reasons of CCI can bebecause of either adverse weather conditions or poor frequency planning or overlycrowdedradio spectrum.
- If the cell size and the power transmitted at the base stations are same then CCIwill become independent of the transmitted power and will depend on radius of thecell (R) and the distance between the interfering co-channel cells (D).
- If D/R ratio is increased, then the effective distance between the co-channel cells will increaseand interference will decrease. The parameter Q is called the frequency reuse ratioand is related to the cluster size.
- For hexagonal geometry $Q = D/R = \sqrt{(}3K)$.
- From the above equation, small of 'Q' means small value of cluster size 'K' andincrease in cellular capacity. But large 'Q' leads to decrease in system capacitybut increase in transmission quality.

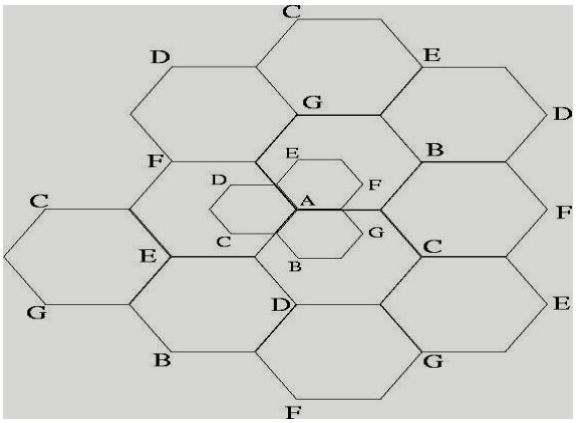
Adjacent Channel Interference (ACI)

- This is a different type of interference which is caused by adjacent channels i.e.channels in adjacent cells.
- It is the signal impairment which occurs to one frequencydue to presence of another signal on a nearby frequency.
- This occurs when imperfectreceiver filters allow nearby frequencies to leak into the passband.
- This problem isenhanced if the adjacent channel user is transmitting in a close range compared tothe subscriber's receiver while the receiver attempts to receive a base station on thechannel. This is called **near-far** effect.
- The more adjacent channels are packed into the channel block, the higher the spectral efficiency, provided that the performancedegradation can be tolerated in the system link budget. This effect can also occurif a mobile close to a base station transmits on a channel close to one being usedby a weak mobile.
- This problem might occur if the base station has problem in discriminating the mobile user from the "bleed over" caused by the close adjacent channel mobile.
- Adjacent channel interference occurs more frequently in small cell clusters and heavilyused cells.
- If the frequency separation between the channels is kept large this interference can be reduced to some extent. Thus assignment of channels is given such that they do not form a contiguous band of frequencies within a particular cell and frequency separation is maximized.
- Efficient assignment strategies are very much important in making the interference as less as possible.

5. Cell Splitting

- Cell splitting is a method in which congested (heavy traffic) cell is subdivided into smaller cells, and each smaller cell is having its own base station with reduction in antenna height and transmitter power.

- The original congested bigger cell is called **macrocell** and the smaller cells are called **microcells**.
- Capacity of cellular network can be increased by creating micro-cells within the original cells which are having smaller radius than macro-cells, therefore, the capacity of a system increases because more channels per unit area are now available in a network.
- Figure below shows a cell splitting in which a congested cell, divided into smaller microcells, and the base stations are put up at corners of the cells.
- The micro-cells are to be added in such a way in order to the frequency reuse plan of the system should be preserved. For micro-cells, the transmit power of transmitter should be reduced, and each micro-cell is having half the radius to that of macro-cell.
- Therefore, transmit power of the new cells can be calculated by analyzing the received power at the cell boundaries. This is required in order to make sure that frequency reuse plan for the micro-cells is also working the same way as it was working for the macro-cells.

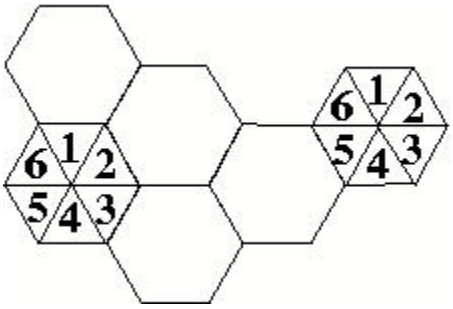


6. Sectoring

- Another way of improving the channel capacity of a cellular system is to decrease the D/R ratio while keeping the same cell radius.
- Improvement in the capacity can be accomplished by reducing the number of cells in a cluster, hence increasing the frequency reuse.
- To achieve this, the relative interference must be minimized without decreasing the transmit power.
- For minimizing co-channel interference in a cellular network, a single omni-directional antenna is replaced with multiple directional antennas, with each transmitting within a smaller region. These smaller regions are called sectors and minimizing co-channel interference while improving the capacity of a system by using multiple directional antennas is called sectoring.
- The amount up to which co-channel interference is minimized depends on the amount of sectoring used.
- A cell is generally divided either into three 120 degree or six 60 degree sectors. In the three-sector arrangement, three antennas are generally located in each sector

with one transmit and two receive antennas. The placement of two receive antennas provide antenna diversity, which is also known as space diversity.

- Space diversity greatly improves the reception of a signal by efficiently providing a big target for signals transmitted from mobile units.
- The division between the two receive antenna depends on the height of the antennas above ground.
- When sectoring technique is used in cellular systems, the channels used in a particular sector are actually broken down into sectored groups, which are only used inside a particular sector.
- With 7-cell reuse pattern and 120 degree sectors, the number of interfering cells in the neighboring tier is brought down from six to two.
- Cell sectoring also improves the signal-to-interference ratio, thereby increasing the capacity of a cellular system. This method of cell sectoring is very efficient, because it utilized the existing system structures.
- Cell sectoring also minimized the co-channel interference, with the use of directional antennas, a particular cell will get interference and transmit only a fraction of the available co-channel cells.



2.2 Evolution of Cellular Networks

Firstly, when wireless generation started, it was analog communication. That generation is 1G. They used various analog modulations for data transfer. Now when the communication migrated from analog to digital, the foundation of latest communication were led. Hence came 2G.

1G Technology:

- 1G refers to the first generation of wireless telephone technology, mobile telecommunications which was first introduced in 1980s and completed in early 1990s.
- Itsspeed was upto 2.4kbps, allowed the voice calls in 1 country.
- It used Analog Signal and AMPS was first launched in USA in 1G mobile system.

Drawbacks:

- Poor Voice Quality
- Poor Battery Life

- Large Phone Size
- No Security
- Limited Capacity
- Poor Handoff Reliability

2G Technology:

- 2G technology refers to the 2nd generation which is based on GSM.
- It was launched in Finland in the year 1991 and used digital signals.
- Its data speed was upto 64kbps.

Features include:

- It enables services such as text messages, picture messages and MMS (multimedia message).
- It provides better quality and capacity.

Drawbacks:

- 2G requires strong digital signals to help mobile phones work. If there is no network coverage in any specific area,digital signals would weak.
- These systems are unable to handle complex data such as Videos.

2.5G Technology

- 2.5G is a technology between the second (2G) and third (3G) generation of mobile telephony.
- It is sometimes described as 2G Cellular Technology combined with GPRS.

Features Includes:

- Phone Calls
- Send/Receive E-mail Messages
- Web Browsing
- Speed : 64-144 kbps
- Camera Phones

3G Technology:

- 3G technology refer to third generation which was introduced in year 2000s.
- Data Transmission speed increased from 144kbps- 2Mbps.
- Typically called Smart Phones and features increased its bandwidth and data transfer rates to accommodate web-based applications and audio and video files.

Features Include:

- Providing Faster Communication
- Send/Receive Large Email Messages
- High Speed Web / More Security
- Video Conferencing / 3D Gaming
- TV Streaming/ Mobile TV/ Phone Calls
- Large Capacities and Broadband Capabilities
- 11 sec – 1.5 min. time to download a 3 min Mp3 song.

Drawbacks:

- Expensive fees for 3G Licenses Services
- It was challenge to build the infrastructure for 3G
- High Bandwidth Requirement
- Expensive 3G Phones.
- Large Cell Phones

4G Technology:

- 4G technology refer to or short name of fourth Generation which was started from late 2000s.
- Capable of providing 100Mbps – 1Gbps speed.
- One of the basic term used to describe 4G is **MAGIC**.

MAGIC:

- Mobile Multimedia
- Ubiquitous
- Global Mobility Support
- Integrated Wireless Solution
- Customized Personal Services
- Also known as Mobile Broadband Everywhere
- The next generations of wireless technology that promises higher data rates and expanded multimedia services.
- Capable to provide speed 100Mbps-1Gbps.
- High QOS and High Security
- Provide any kind of service at any time as per user requirements, anywhere.

Features Include:

- More Security
- High Speed
- High Capacity
- Low Cost Per-bit

Drawbacks:

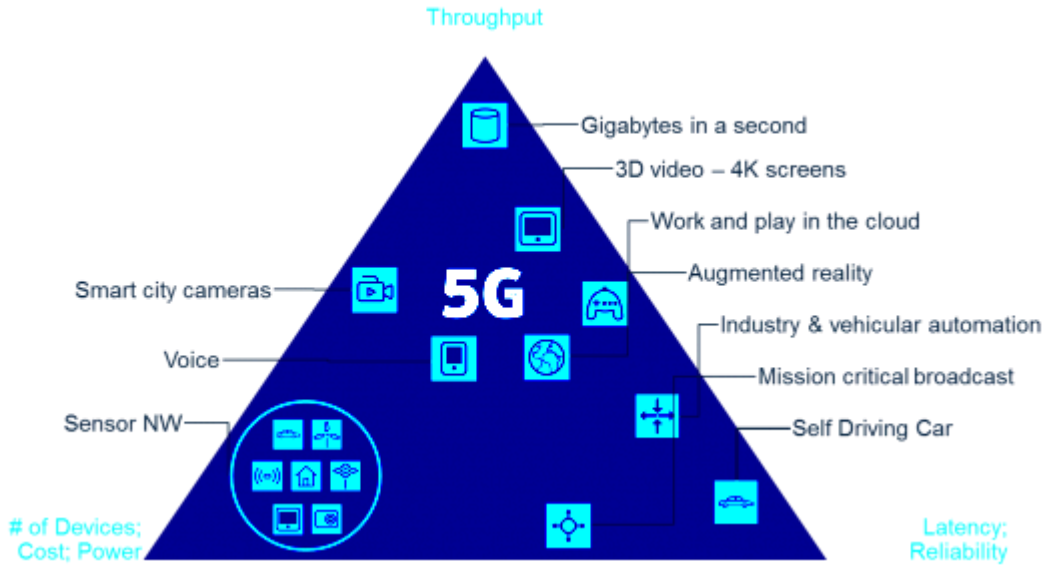
- Battery uses is more
- Hard to implement
- Need complicated hardware
- Expensive equipment required to implement next generation network.

The basic difference between 3G and 4G is in data transfer and signal quality.

Technology	**3G**	**4G**
Data Transfer Rate	3.1 MB/sec	100 MB/sec
Internet Services	Broadband	Ultra Broadband

Mobile – TV Resolution	Low	High
Bandwidth	5-20 MHz	100MHz
Frequency	1.6-2 GHz	2-8 GHz
Download and upload	5.8 Mbps	14 Mbps

5G Technology:



- It refers to short name of fifth Generation which was started from late 2010s.
- Complete wireless communication with almost no limitations.
- It is highly supportable to WWWW (Wireless World Wide Web).

Features Include:

- High Speed, High Capacity
- 5G technology providing large broadcasting of data in Gbps .
- Multi – Media Newspapers, watch T.V programs with the clarity as to that of an HD Quality.
- Faster data transmission that of the previous generations.
- Large Phone Memory, Dialing Speed, clarity in Audio/Video.
- Support interactive multimedia ,voice, streaming video, Internet and other
- 5G is More Effective and More Attractive.

Technology	1G	2G/2.5G	3G	4G	5G
Deployment	1970/1984	1980/1999	1990/2002	2000/2010	2014/2015
Bandwidth	2kbps	14-64kbps	2mbps	200mbps	>1gbps
Technology	Analog cellular	Digital cellular	Broadband width/ CDMA/ IP technology	Unified IP & seamless combo of LAN/WAN/WLAN/PAN	4G+WWWW (Wireless WWW)
Service	Mobile telephony	Digital voice,short messaging	Integrated high quality audio, video & data	Dynamic information access, variable devices	Dynamic information access, variable devices with AI capabilities
Multiplexing	FDMA	TDMA/CDMA	CDMA	CDMA	CDMA
Switching	Circuit	Circuit/circuit for access network&air interface	Packet except for air interface	All packet	All packet
Core network	PSTN	PSTN	Packet network	Internet	Internet
Handoff	Horizontal	Horizontal	Horizontal	Horizontal&Vertical	Horizontal& Vertical

2.3 Global System for Mobile Communication (GSM)

- GSM stands for Global System for Mobile Communication. It is a digital cellular technology used for transmitting mobile voice and data services.

- The concept of GSM emerged from a cell-based mobile radio system at Bell Laboratories in the early 1970s.
- GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard.
- GSM is the most widely accepted standard in telecommunications and it is implemented globally.
- GSM is a circuit-switched system that divides each 200 kHz channel into eight 25 kHz time-slots. GSM operates on the mobile communication bands 900 MHz and 1800 MHz in most parts of the world. In the US, GSM operates in the bands 850 MHz and 1900 MHz.
- GSM owns a market share of more than 70 percent of the world's digital cellular subscribers.
- GSM makes use of narrowband Time Division Multiple Access (TDMA) technique for transmitting signals.
- GSM was developed using digital technology. It has an ability to carry 64 kbps to 120 Mbps of data rates.
- Presently GSM supports more than one billion mobile subscribers in more than 210 countries throughout the world.
- GSM provides basic to advanced voice and data services including roaming service. Roaming is the ability to use your GSM phone number in another GSM network.

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

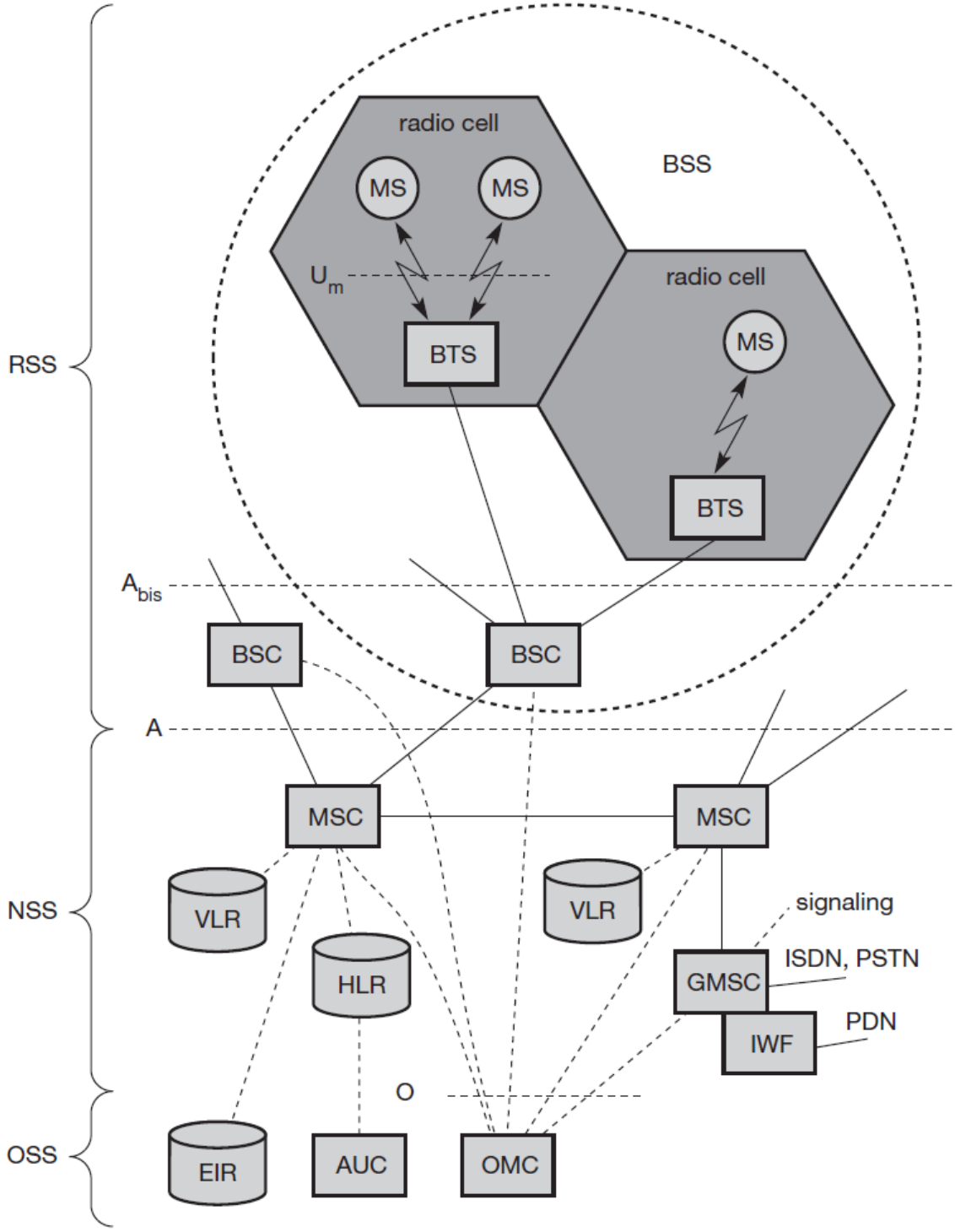
Why GSM?

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

- Improved spectrum efficiency
- International roaming
- Low-cost mobile sets and base stations (BSs)
- High-quality speech
- Compatibility with Integrated Services Digital Network (ISDN) and other telephone company services
- Support for new services

2.3.1 GSM Architecture

Figure below gives a simplified overview of the GSM system as specifiedin ETSI (1991b). A GSM system consists of three subsystems, the radio subsystem (RSS), the network and switching subsystem (NSS), and the operationsubsystem (OSS).



Radio subsystem

As the name implies, the **radio subsystem (RSS)** comprises all radio specificentities, i.e., the **mobile stations (MS)** and the **base station subsystem (BSS)**.Figure above shows the connection between the RSS and the NSS via the **A interface**(solid lines) and the connection to the OSS via the **O interface** (dashedlines). The A interface is typically based on circuit-switched PCM-30 systems(2.048 Mbit/s), carrying up to thirty 64 kbit/s connections, whereas the O interfaceuses the Signalling System No. 7 (SS7) based on X.25 carrying management datato/from the RSS.

- **Base station subsystem (BSS)**: A GSM network comprises many BSSs, each controlled by a base station controller (BSC). The BSS performs all functions necessary to maintain radio connections to an MS, coding/decoding of voice, and rate adaptation to/from the wireless network part. Besides a BSC, the BSS contains several BTSs.
- **Base transceiver station (BTS)**: A BTS comprises all radio equipment, i.e., antennas, signal processing, amplifiers necessary for radio transmission. A BTS can form a radio cell or, using sectorized antennas, several cells and is connected to MS via the **Um interface** (ISDN U interface for mobile use), and to the BSC via the **Abis interface**. The Um interface contains all the mechanisms necessary for wireless transmission (TDMA, FDMA etc.). The Abis interface consists of 16 or 64 kbit/s connections. A GSM cell can measure between some 100 m and 35 km depending on the environment (buildings, open space, mountains etc.) and also expected traffic.
- **Base station controller (BSC)**: The BSC basically manages the BTSs. It reserves radio frequencies, handles the handover from one BTS to another within the BSS, and performs paging of the MS. The BSC also multiplexes the radio channels onto the fixed network connections at the A interface.
- **Mobile station (MS)**: The MS comprises all user equipment and software needed for communication with a GSM network. An MS consists of user independent hard- and software and of the **subscriber identity module (SIM)**, which stores all user-specific data that is relevant to GSM. While an MS can be identified via the **international mobile equipment identity (IMEI)**, a user can personalize any MS using his or her SIM, i.e., user-specific mechanisms like charging and authentication are based on the SIM, not on the device itself. Device-specific mechanisms, e.g., theft protection, use the device specific IMEI. Without the SIM, only emergency calls are possible. The SIM card contains many identifiers and tables, such as card-type, serial number, a list of subscribed services, a **personal identity number (PIN)**, a **PIN unblocking key (PUK)**, an **authentication key Ki**, and the **international mobile subscriber identity (IMSI)**. The PIN is used to unlock the MS. Using the wrong PIN three times will lock the SIM. In such cases, the PUK is needed to unlock the SIM. The MS stores dynamic information while logged onto the GSM system, such as, e.g., the **cipher key Kc**and the location information consisting of a **temporary mobile subscriber identity (TMSI)** and the **location area identification (LAI)**. Typical MSs for GSM 900 have a transmit power of up to 2 W, whereas for GSM 1800 1 W is enough due to the smaller cell size.

Network and switching subsystem

The “heart” of the GSM system is formed by the **network and switching subsystem(NSS)**. The NSS connects the wireless network with standard publicnetworks, performs handovers between different BSSs, comprises functions forworldwide localization of users and supports charging, accounting, and roamingof users between different providers in different countries. The NSS consists ofthe following switches and databases:

- **Mobile services switching center (MSC)**: MSCs are high-performance digital ISDN switches. They set up connections to other MSCs and to the BSCs via the A interface, and form the fixed backbone network of a GSM system. Typically, an MSC manages several BSCs in a geographical region. A **gatewayMSC (GMSC)** has additional connections to other fixed networks, such as**PSTN** and **ISDN**. Using additional **interworking functions (IWF)**, an MSC can also connect to **public data networks (PDN)** such as X.25. An MSC handles all signaling needed for connection setup, connection release and handover of connections to other MSCs. The **standard signaling system No. 7 (SS7)** is used for this purpose. SS7 covers all aspects of control signaling for digital networks (reliable routing and delivery of control messages, establishing and monitoring of calls). Features of SS7 are number portability, free phone/toll/collect/credit calls, call forwarding, three-way calling etc. An MSC also performs all functions needed for supplementary services such as call forwarding, multi-party calls, reverse charging etc.
- **Home location register (HLR)**: The HLR is the most important database in a GSM system as it stores all user-relevant information. This comprises static information, such as the **mobile subscriber ISDN number (MSISDN)**, subscribed services (e.g., call forwarding, roaming restrictions, GPRS), and the **international mobile subscriber identity (IMSI)**. Dynamic information is also needed, e.g., the current **location area (LA)** of the MS, the **mobile subscriber roaming number (MSRN)**, the current VLR and MSC. As soon as an MS leaves its current LA, the information in the HLR is updated. This information is necessary to localize a user in the worldwide GSM network. All these user-specific information elements only exist once for each user in a single HLR, which also supports charging and accounting. HLRs can manage data for several million customers and contain highly specialized data bases which must fulfill certain real-time requirements to answer requests within certain time-bounds.
- **Visitor location register (VLR)**: The VLR associated to each MSC is a dynamic database which stores all important information needed for the MS users currently in the LA that is associated to the MSC (e.g., IMSI, MSISDN, HLR address). If a new MS comes into an LA the VLR is responsible for, it copies all relevant information for this user from the HLR. This hierarchy of VLR and HLR avoids frequent HLR updates and long-distance signaling of user information.

Operation subsystem

The third part of a GSM system, the **operation subsystem (OSS)**, contains thenecessary functions for network operation and maintenance. The OSS possessesnetwork entities of its own and accesses other entities via SS7 signaling. The following entities have been defined:

- **Operation and maintenance center (OMC)**: The OMC monitors and controls all other network entities via the O interface (SS7 with X.25). Typical OMC management functions are traffic monitoring, status reports of network entities, subscriber and security management, or accounting and billing. OMCs use the concept of **telecommunication management network (TMN)** as standardized by the ITU-T.

- **Authentication centre (AuC)**: As the radio interface and mobile stations are particularly vulnerable, a separate AuC has been defined to protect user identity and data transmission. The AuC contains the algorithms for authentication as well as the keys for encryption and generates the values needed for user authentication in the HLR. The AuC may, in fact, be situated in a special protected part of the HLR.
- **Equipment identity register (EIR)**: The EIR is a database for all IMEIs, i.e., it stores all device identifications registered for this network. As MSs are mobile, they can be easily stolen. With a valid SIM, anyone could use the stolen MS. The EIR has a blacklist of stolen (or locked) devices. In theory an MS is useless as soon as the owner has reported a theft. Unfortunately, the blacklists of different providers are not usually synchronized and the illegal use of a device in another operator's network is possible. The EIR also contains a list of valid IMEIs (white list), and a list of malfunctioning devices (gray list).

2.3.2 GSM Services

GSM offers three basic types of services:

1. **Teleservices**

   The abilities of a Bearer Service are used by a Teleservice to transport data. These services are further transited in the following ways:

- ***Voice Calls:*** The most basic Teleservice supported by GSM is telephony. This includes full-rate speech at 13 kbps and emergency calls, where the nearest emergency-service provider is notified by dialing three digits.
- ***Videotext and Facsimile:*** Another group of teleservices includes Videotext access, Teletex transmission, Facsimile alternate speech and facsimile Group 3, Automatic facsimile Group 3, etc.
- ***Short Text Messages*****:** Short Messaging Service (SMS) service is a text messaging service that allows sending and receiving text messages on your GSM mobile phone. In addition to simple text messages, other text data including news, sports, financial, language, and location-based data can also be transmitted.

2. **Bearer Services**

   Data services or Bearer Services are used through a GSM phone. to receive and send data is the essential building block leading to widespread mobile Internet access and mobile data transfer. GSM currently has a data transfer rate of 9.6k. New developments that will push up data transfer rates for GSM users are HSCSD (high speed circuit switched data) and GPRS (general packet radio service) are now available.

3. **Supplementary Services**

   Supplementary services are additional services that are provided in addition to teleservices and bearer services. These services include caller identification, call forwarding, call waiting, multi-party conversations, and barring of outgoing

(international) calls, among others. A brief description of supplementary services is given here:

- **Conferencing**: It allows a mobile subscriber to establish a multiparty conversation, i.e., a simultaneous conversation between three or more subscribers to setup a conference call. This service is only applicable to normal telephony.
- **Call Waiting**: This service notifies a mobile subscriber of an incoming call during a conversation. The subscriber can answer, reject, or ignore the incoming call.
- **Call Hold**: This service allows a subscriber to put an incoming call on hold and resume after a while. The call hold service is applicable to normal telephony.
- **Call Forwarding**: Call Forwarding is used to divert calls from the original recipient to another number. It is normally set up by the subscriber himself. It can be used by the subscriber to divert calls from the Mobile Station when the subscriber is not available, and so to ensure that calls are not lost.
- **Call Barring**: Call Barring is useful to restrict certain types of outgoing calls such as ISD or stop incoming calls from undesired numbers. Call barring is a flexible service that enables the subscriber to conditionally bar calls.
- **Number Identification**: There are following supplementary services related to number identification:
    - **Calling Line Identification Presentation**: This service displays the telephone number of the calling party on your screen.
    - **Calling Line Identification Restriction**: A person not wishing their number to be presented to others subscribes to this service.
    - **Connected Line Identification Presentation**: This service is provided to give the calling party the telephone number of the person to whom they are connected. This service is useful in situations such as forwarding's where the number connected is not the number dialed.
    - **Connected Line Identification Restriction**: There are times when the person called does not wish to have their number presented and so they would subscribe to this person. Normally, this overrides the presentation service.
    - **Malicious Call Identification**: The malicious call identification service was provided to combat the spread of obscene or annoying calls. The victim should subscribe to this service, and then they could cause known malicious calls to be identified in the GSM network, using a simple command.

2.3.3 GSM Radio Subsystem

- Two frequency bands, of 25 MHz each one, have been allocated for the GSM system.
- The band 890-915 MHz has been allocated for the uplink direction (transmitting from the mobile station to the base station).
- The band 935-960 MHz has been allocated for the downlink direction (transmitting from the base station to the mobile station).
- Both the frequency bands are divided into 200KHz channels called Absolute Radio Frequency Channel Numbers (ARFCNs).

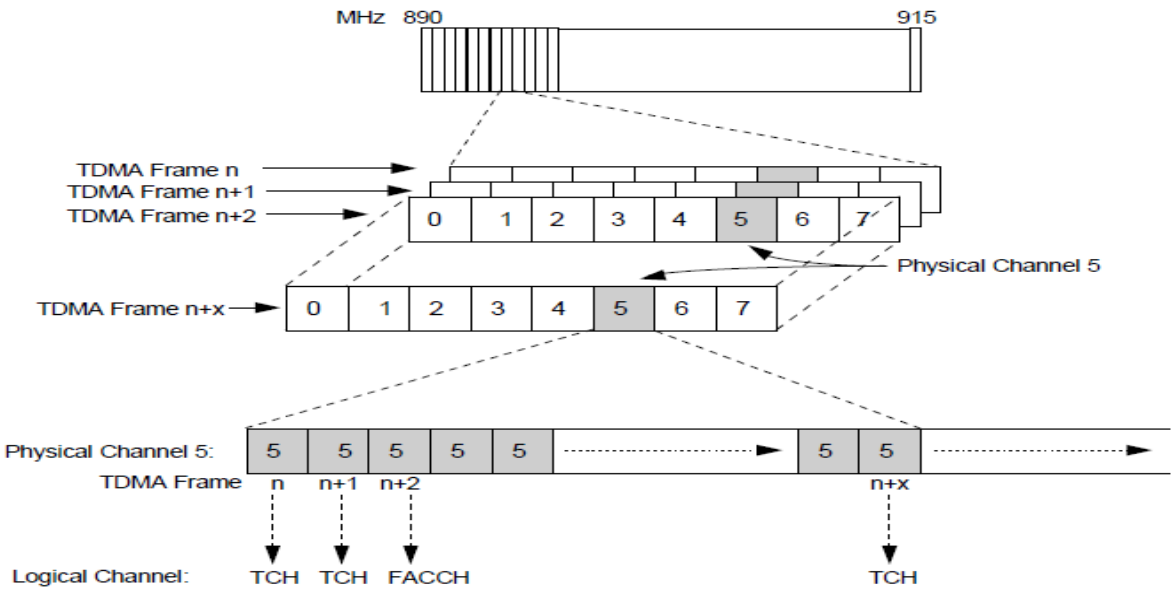
- ARFCN represents a pair of forward and reverse channels divided in frequency by 45MHz, and a single channel is time shared among eight users using TDMA.
- Each user uses the same ARFCN and holds a time slot per frame.

2.3.4 GSM Burst Structure

- **Time slot structure** is the **division** of a **time slot period into** different **fields** (information parts). Slot structure fields include a **preamble** for synchronization, **control** header, **user data**, **signaling data**, and **error detection**.
- A single time slot transmission is called a **radio burst**. Four **types** of radio bursts are defined in the GSM system; normal burst, shortened burst, frequency correction burst, and synchronization burst.
- The time period for a GSM time slot is 577 microseconds.
- Time slots include ramp up and ramp down periods to minimize rapid changes in radio transmitter power.
- The ramp up and ramp down time is used to reduce unwanted radio emissions that occur from rapidly changing signals.
- **Normal Burst** is used for normal communication between the mobile device and the base station. Each normal burst can transfer 114 bits of user information data (after error protection is removed).
- **Random Access Burst (Shortened Burst)** is a short 88 bit transmission burst that is used to request access to the GSM system. Mobile devices use a shortened burst.
- **Frequency Correction Burst** is a time slot of information that contains a 142 bit pattern of all "0" values. It allows the mobile device to adjust its timing so it can better receive and demodulate the radio channel.
- **Synchronization Burst** is a transmission burst that contains system timing information. It contains a 78 bit code to identify the hyperframe counter. The synchronization burst follows the frequency correction burst.

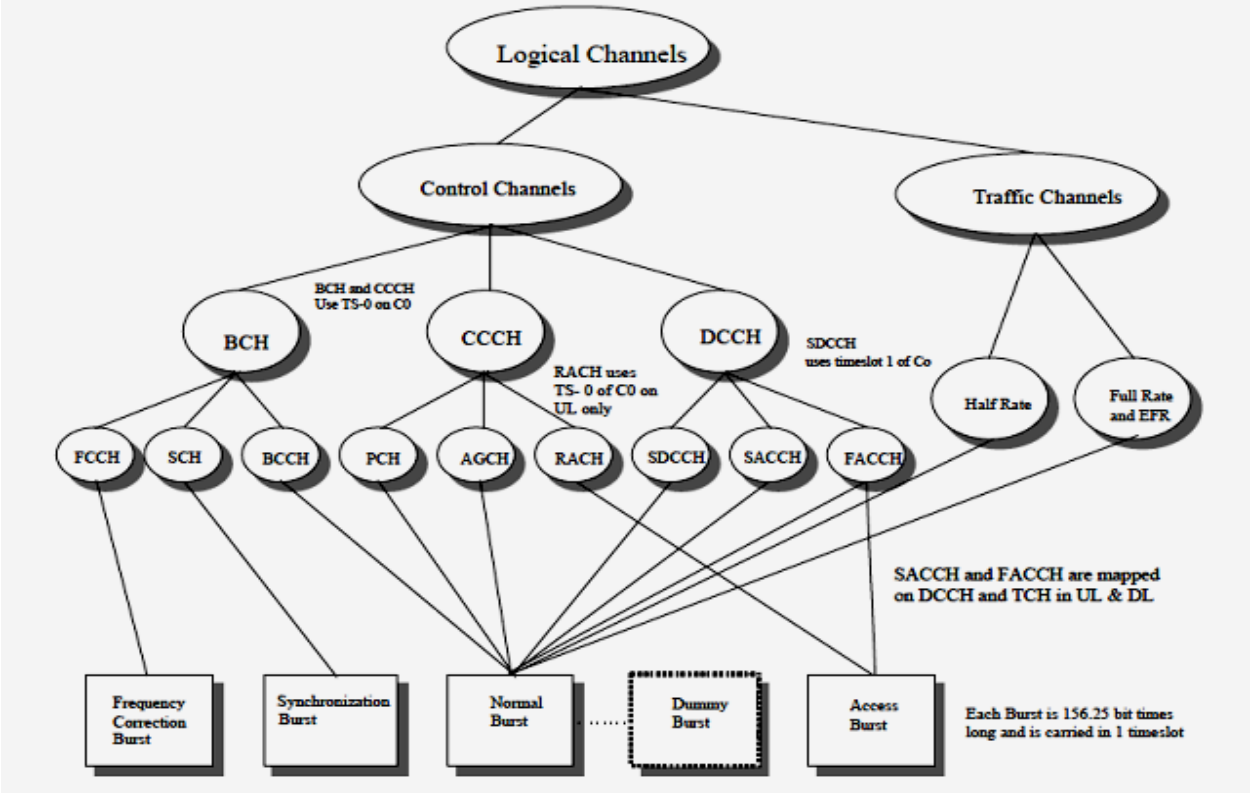
2.3.5GSM Channel Types

Each timeslot on a TDMA frame is called a **physical channel**. Therefore, there are 8 physical channels per carrier frequency in GSM. Physical channels can be used to transmit speech, data or signaling information. A physical channel may carry different messages, depending on the information that is to be sent. These messages are called **logical channels**. For example, on one of the physical channels used for traffic, the traffic itself is transmitted using a Traffic CHannel (TCH) message, while a handover instruction is transmitted using a Fast Associated Control Channel (FACCH) message.



Logical Channels

- Many types of logical channels exists, each designed to carry a different message to or from an MS.
- All information to and from an MS must be formatted correctly, so that the receiving device can understand the meaning of different bits in the message.
- For example, in the burst used to carry traffic, some bits may represent the speech or data itself, while others may be used as a training sequence.
- There are several types of burst.
- The relationship between bursts and logical channels is shown in the figure below.



CONTROL CHANNELS

- When an MS is switched on, it searches for a BTS to connect to.
- The MS scans the entire frequency band, or, optionally, uses a list containing the allocated carrier frequencies for this operator.
- When the MS finds the strongest carrier, it must then determine if it is a control channel.
- It does so by searching for a particular logical channel called Broadcast Control CHannel (BCCH).
- A frequency carrying BCCH contains important information for an MS, including e.g. the current LA identity, synchronization information and network identity.
- Without such information, an MS cannot work with a network.
- This information is broadcast at regular intervals, leading to the term Broadcast CHannel (BCH) information.

Broadcast CHannels (BCH's)			
Logical Channel	*Direction*	*BTS*	*MS*
Frequency Correction CHannel (FCCH)	Downlink, point to multipoint	Transmits a carrier frequency.	Identifies BCCH carrier by the carrier frequency and synchronizes with the frequency.
Synchronization CHannel (SCH)	Downlink, point to multipoint	Transmits information about the TDMA frame structure in a cell (e.g. frame number) and the BTS identity (Base Station Identity Code (BSIC)).	Synchronizes with the frame structure within a particular cell, and ensures that the chosen BTS is a GSM BTS - BSIC can only be decoded by an MS if the BTS belongs to a GSM network.
Broadcast Control CHannel (BCCH)	Downlink, point to multipoint	Broadcasts some general cell information such as Location Area Identity (LAI), maximum output power allowed in the cell and the identity of BCCH carriers for neighboring cells.	Receives LAI and will signal to the network as part of the Location Updating procedure if the LAI is different to the one already stored on its SIM. MS sets its output power level based on the information received on the BCCH. The MS stores the list of BCCH carrier frequencies on which Rx.lev.measurement is done for Handover decision.

Common Control Channels (CCCH)			
Logical Channel	*Direction*	*BTS*	*MS*
Paging CHannel (PCH)	Downlink, point to point	Transmits a paging message to indicate an incoming call or short message. The paging message contains the identity number of the mobile subscriber that the network wishes to contact.	At certain time intervals the MS listens to the PCH. If it identifies its own mobile subscriber identity number on the PCH, it will respond.
Random Access CHannel (RACH)	Uplink, point to point	Receives access-request from MS for call setup/ loc. updatate/ SMS	Answers paging message on the RACH by requesting a signaling channel.
Access Grant CHannel (AGCH)	Downlink, point to point	Assigns a signaling channel (SDCCH) to the MS.	Receives signaling channel assignment (SDCCH).

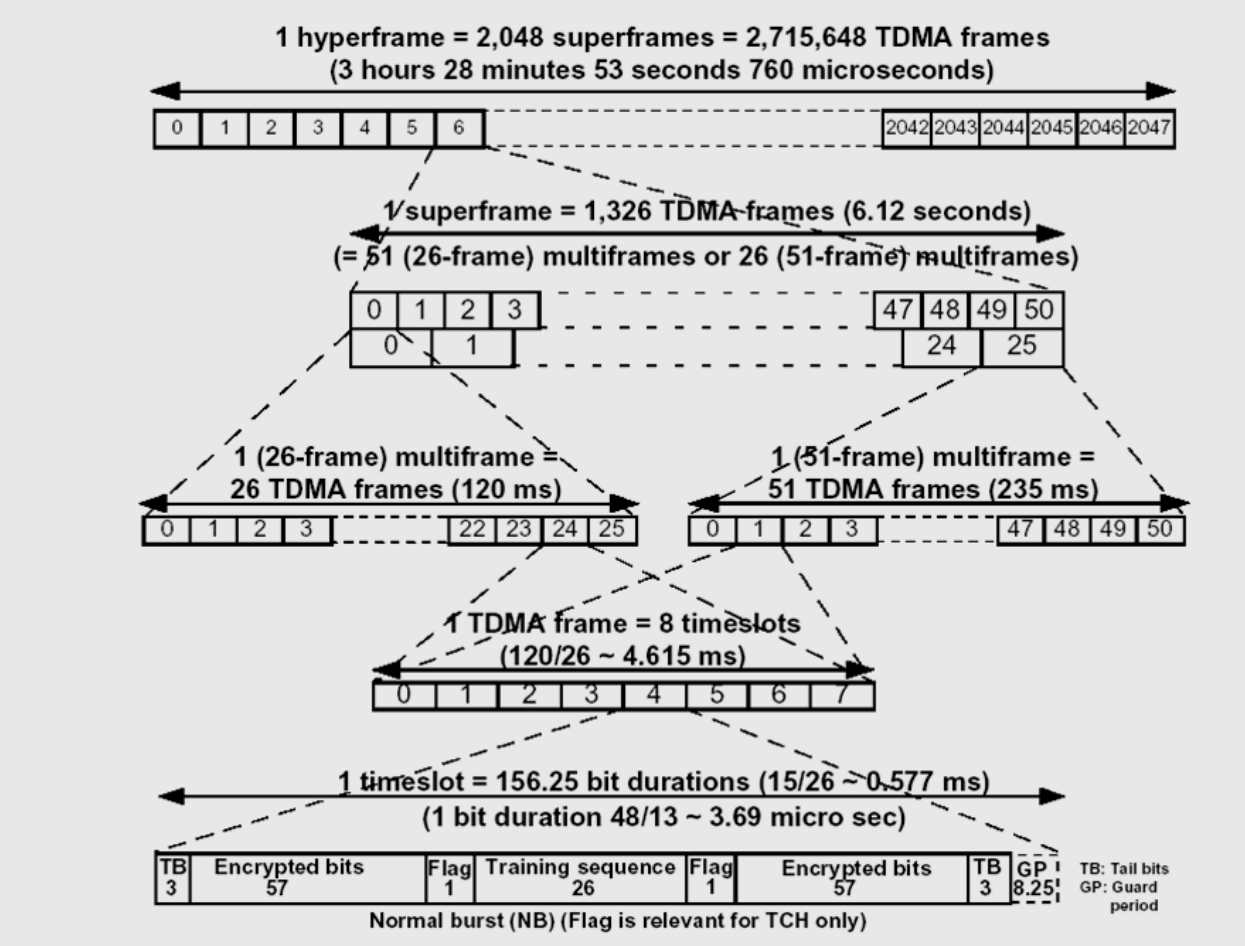
Dedicated Control Channels (DCCH)			
Logical Channel	*Direction*	*BTS*	*MS*
Stand alone Dedicated Control CHannel (SDCCH)	Uplink and downlink, point to point	The BTS switches to the assigned SDCCH, used for call set-up signaling. TCH is assigned on here. (SDCCH is also used for SMS messages to MS).	The MS switches to the assigned SDCCH. Call set-up is performed. The MS receives a TCH assignment information (carrier and time slot).
Cell Broadcast CHannel (CBCH)	DL,point to multi point, mapped on SDCCH	Uses this logical channel to transmit short message service cell broadcast.	MS receives cell broadcast messages.
Slow Associated Control CHannel (SACCH)	Uplink and downlink, point to point	Instructs the MS on the allowed transmitter power and parameters for time advance. SAACH is used for SMS during a call.	Sends averaged measurements on its own BTS (signal strength and quality) and neighboring BTS's (signal strength). The MS continues to use SACCH for this purpose during a call.
Fast Associated Control CHannel (FACCH)	Uplink and downlink, point to point	Transmits handover information.	Transmits necessary handover information in access burst

TRAFFIC CHANNELS

- Once call set-up procedures have been completed on the control physical channel, the MS tunes to a traffic physical channel.
- It uses the Traffic CHannel (TCH) logical channel. There are two types of TCH:
  - **Full rate (TCH):** transmits full rate speech (13 kbits/s). A full rate TCH occupies one physical channel.
  - **Half rate (TCH/2):** transmits half rate speech (6.5 kbits/s). Two half rate TCH's can share one physical channel, thus doubling the capacity of a cell.

2.3.6 GSM Frame Structure

- The **GSM frame structure** is designated as hyperframe, superframe, multiframe and frame. The minimum unit being frame (or TDMA frame) is made of 8 time slots.
- One GSM hyperframe is composed of 2048 superframes.
- Each GSM superframe is composed of multiframes (either 26 or 51 as described below).
- Each GSM multiframe is composed of frames (either 51 or 26 based on multiframe type).
- Each frame is composed of 8 time slots.
- Hence there will be total of 2715648 TDMA frames available in GSM and the same cycle continues.
- As shown in the figure, there are two variants to multiframe structure.
  - 26 frame multiframe - Called traffic multiframe, composed of 26 bursts in a duration of 120ms, out of these 24 are used for traffic, one for SACCH and one is not used.
  - 51 frame multiframe- Called control multiframe, composed of 51 bursts in a duration of 235.4 ms.
- This type of multiframe is divided into logical channels.
- These logical channels are time sheduled by BTS. Always occur at beacon frequency in time slot 0, it may also take up other time slots if required by system for example 2,4,6.



2.4 GPRS

General Packet Radio System also known as **GPRS** is a third-generation step toward internet access. GPRS is also known as GSM-IP that is a Global-System Mobile Communications Internet Protocol as it keeps the users of this system online, allows to make voice calls, and access internet on-the-go. Even Time-Division Multiple Access (TDMA) users benefit from this system as it provides packet radio access.

GPRS also permits the network operators to execute an Internet Protocol (IP) based core architecture for integrated voice and data applications that will continue to be used and expanded for 3G services.

GPRS supersedes the wired connections, as this system has simplified access to the packet data networks like the internet. The packet radio principle is employed by GPRS to transport user data packets in a structure way between GSM mobile stations and external packet data networks. These packets can be directly routed to the packet switched networks from the GPRS mobile stations.

In the current versions of GPRS, networks based on the Internet Protocol (IP) like the global internet or private/corporate intranets and X.25 networks are supported.

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

Key Features

Following three key features describe wireless packet data:

- **The always online feature -** Removes the dial-up process, making applications only one click away.
- **An upgrade to existing systems -** Operators do not have to replace their equipment; rather, GPRS is added on top of the existing infrastructure.
- **An integral part of future 3G systems -** GPRS is the packet data core network for 3G systems EDGE and WCDMA.

Goals of GPRS

GPRS is the first step toward an end-to-end wireless infrastructure and has the following goals:

- Open architecture
- Consistent IP services
- Same infrastructure for different air interfaces
- Integrated telephony and Internet infrastructure
- Leverage industry investment in IP
- Service innovation independent of infrastructure

Benefits of GPRS

- ***Higher Data Rate***
  GPRS benefits the users in many ways, one of which is higher data rates in turn of shorter access times. In the typical GSM mobile, setup alone is a lengthy process and equally, rates for data permission are restrained to 9.6 kbit/s. The session establishment time offered while GPRS is in practice is lower than one second and ISDN-line data rates are up to many 10 kbit/s.
- ***Easy Billing***
  GPRS packet transmission offers a more user-friendly billing than that offered by circuit switched services. In circuit switched services, billing is based on the duration of the connection. This is unsuitable for applications with bursty traffic. The user must pay for the entire airtime, even for idle periods when no packets are sent (e.g., when the user reads a Web page).

In contrast to this, with packet switched services, billing can be based on the amount of transmitted data. The advantage for the user is that he or she can be "online" over a long period of time but will be billed based on the transmitted data volume.

GPRS has opened a wide range of unique services to the mobile wireless subscriber. Some of the characteristics that have opened a market full of enhanced value services to the users. Below are some of the characteristics:

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

- **Immediacy** - Allows subscribers to obtain connectivity when needed, regardless of location and without a lengthy login session.
- **Localization** - Allows subscribers to obtain information relevant to their current location.

Using the above three characteristics varied possible applications are being developed to offer to the mobile subscribers. These applications, in general, can be divided into two high-level categories:

- Corporation
- Consumer

These two levels further include:

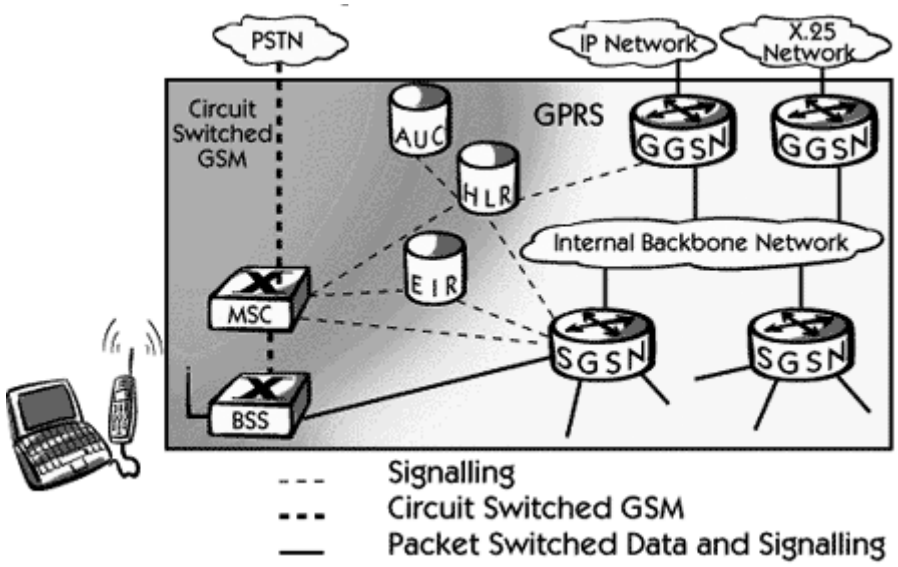
- **Communications** - E-mail, fax, unified messaging and intranet/internet access, etc.
- **Value-added services** - Information services and games, etc.
- **E-commerce** - Retail, ticket purchasing, banking and financial trading, etc.
- **Location-based applications** - Navigation, traffic conditions, airline/rail schedules and location finder, etc.
- **Vertical applications** - Freight delivery, fleet management and sales-force automation.
- **Advertising** - Advertising may be location sensitive. For example, a user entering a mall can receive advertisements specific to the stores in that mall.

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

2.4.1 GPRS Architecture

GPRS architecture works on the same procedure like GSM network, but, has additional entities that allow packet data transmission. This data network overlaps a second-generation GSM network providing packet data transport at the rates from 9.6 to 171 kbps. Along with the packet data transport the GSM network accommodates multiple users to share the same air interface resources concurrently.

GPRS attempts to reuse the existing GSM network elements as much as possible, but to effectively build a packet-based mobile cellular network, some new network elements, interfaces, and protocols for handling packet traffic are required.Following is the GPRS Architecture diagram:



GPRS Mobile Stations

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

GPRS Base Station Subsystem

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

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

GPRS Support Nodes

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

Gateway GPRS Support Node (GGSN)

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

Serving GPRS Support Node (SGSN)

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

Internal Backbone

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

Routing Area

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

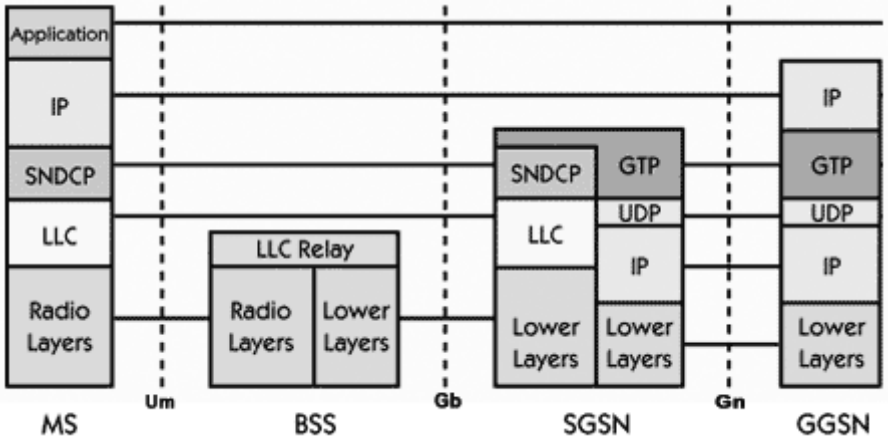
2.4.2 GPRS Terminals

GPRS defines three classes of terminals: A, B, and C.

- A class A terminal supports simultaneous circuit-switched and packet-switched traffic. Thus a user of such a terminal can simultaneously talk and browse the Internet.
- A class B terminal can be attached to the network as both a circuit-switched and packet-switched client but can only support traffic from one service at a time. Thus, when a user of such a terminal receives a call, his Internet connection is suspended.
- Finally, a class C terminal uses only packet-switched services. Thus, when a user of such a terminal receives a call, his Internet connection is dropped.

2.4.2 GPRS Protocol Stack

The flow of GPRS protocol stack and end-to-end message from MS to the GGSN is displayed in the below diagram. GTP is the protocol used between the SGSN and GGSN using the Gn interface. This is a Layer 3 tunneling protocol.



The process that takes place in the application looks like a normal IP sub-network for the users both inside and outside the network. The vital thing that needs attention is, the

application communicates via standard IP, that is carried through the GPRS network and out through the gateway GPRS. The packets that are mobile between the GGSN and the SGSN use the GPRS tunneling protocol, this way the IP addresses located on the external side of the GPRS network do not have deal with the internal backbone. UDP and IP are run by GTP.
SubNetwork Dependent Convergence Protocol (SNDCP) and Logical Link Control (LLC) combination used in between the SGSN and the MS. The SNDCP flattens data to reduce the load on the radio channel. A safe logical link by encrypting packets is provided by LLC and the same LLC link is used as long as a mobile is under a single SGSN.
In case, the mobile moves to a new routing area that lies under a different SGSN; then, the old LLC link is removed and a new link is established with the new Serving GSN X.25. Services are provided by running X.25 on top of TCP/IP in the internal backbone.

Comparison of GSM & GPRS

	GSM	**GPRS**
Data Rates	9.6 Kbps	9.6 to 171Kbps
Modulation Technique	GMSK	GMSK
Billing	Duration of connection	Amount of data transferred
Type of Connection	Circuit – Switched Technology	Packet - Switched Technology

2.5 EDGE

- Stands for Enhanced Data rates for GSM Evolution.
- It is a 2.5G telecommunication network.
- Channel bandwidth is 200 kHz.
- Data rate of 384Kbps is supported.
- Uses 8-PSK (octal phase shift keying).
- Can handle data subscribers 3 times more than in GPRS.
- Sometimes called as Enhanced GPRS.

2.5.1 EDGE Architecture

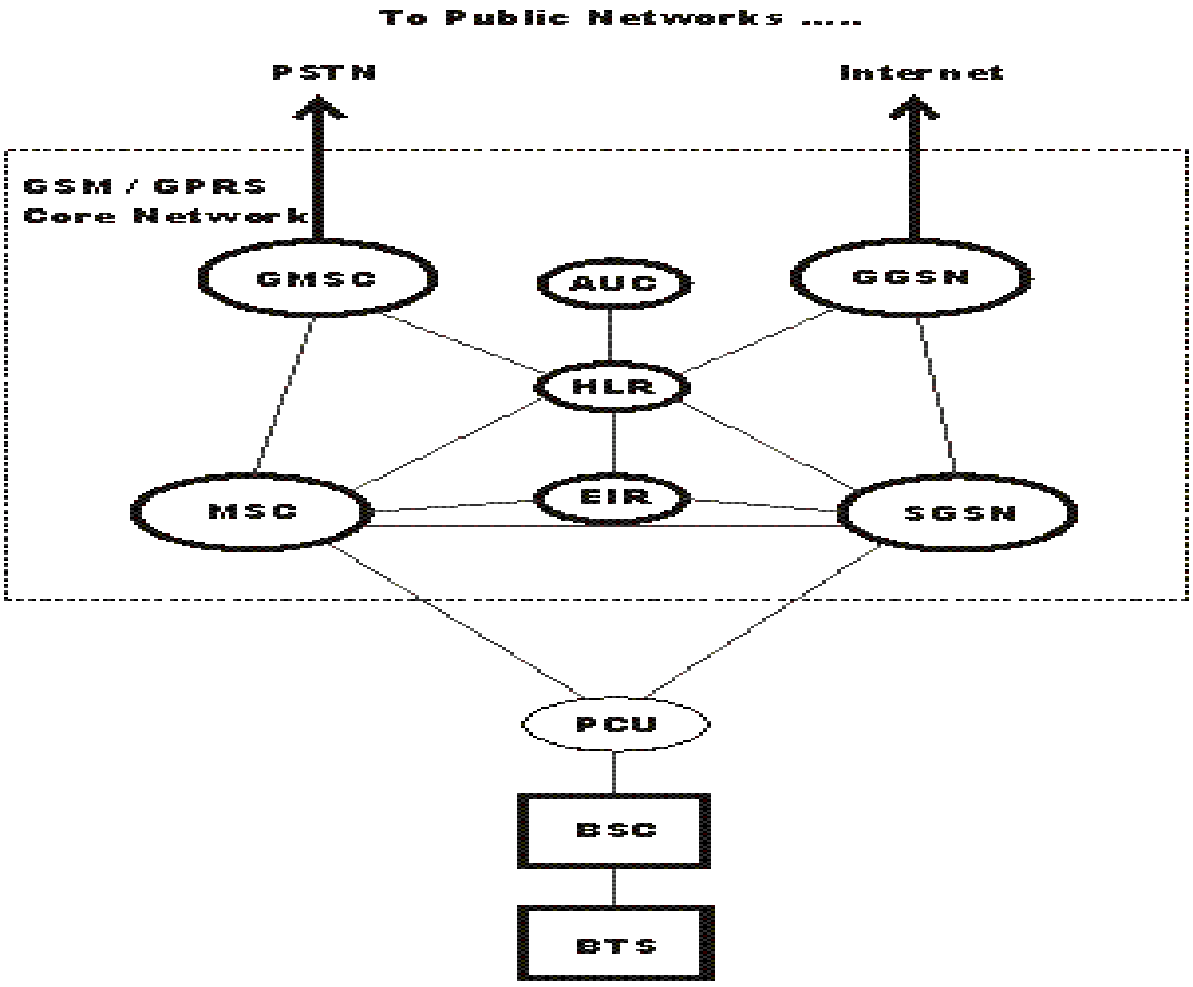
The EDGE architecture consists of three main components:

1. GGSN (Gateway GPRS Support Node)
2. SGSN(Serving GPRS Support Node)
3. PCU(Packet Control Unit)

GGSN (Gateway GPRS Support Node)

- Acts as a gateway to the world outside the network.
- Manages the working between EDGE network and external packet switched networks to which mobile devices are connected.
- A gateway, router, and firewall together form GGSN.

- It first verifies whether a user is active or not, then only it forwards the packets outside or inside the GGSN network.



SGSN (Serving GPRS Support Node)

- Acts as a gateway to the services found within the network.
- Focuses on IP elements of the network.
- Maintains location information such as current cell and VLR
- Also contains information related to user profiles, such as packet address used.
- Offers to mobiles, the services like
  - Packet routing and transmission
  - Authentication
  - Logical link management
  - Mobility management
  - Data charging

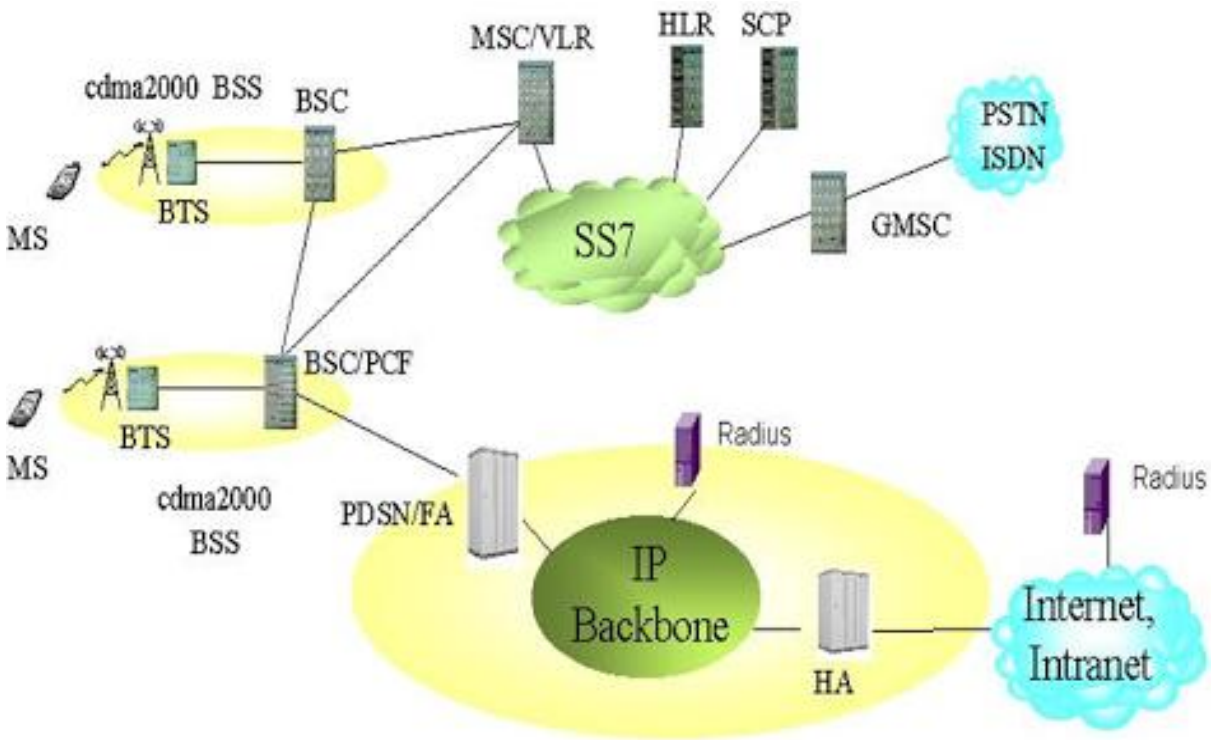
PCU (Packet Control Unit)

- Determines whether the data has to be routed to circuit switched networks or packet switched networks.
- Refers to the hardware router added with a BSC.

2.6 CDMA

- Multiple transmitters can transmit information at the same time using single communication channel.
- This enables mobile users to share the same band of frequencies.
- Uses the spread spectrum technology.
- Used as a channel access method on CDMA One, CDMA 2000 and W-CDMA.
- Used in satellite systems and military applications.

2.6.1 CDMA Architecture



Mobile Station (MS)

- Is the mobile subscriber equipment that can originate and receive calls and communicate with the BTS.

Base Transceiver Station (BTS)

- Transmits and receives radio signals, realizing the communication between the radio system and the mobile station.

Base Station Controller (BSC)

Implements the following functions

- Controlling and managing the BTS
- Call connection and disconnection
- Mobility management
- Stable and reliable link provision for the upper-layer services by soft/hard handoff
- Power control
- Radio resource management

Packet Control Function (PCF)

- Implements the R-P (radio access network to PDSN) connection management.
- Because of the shortage of radio resources, some radio channels should be released when subscribers do not send or receive data, but PPP connection is maintained continuously.
- The PCF can shield radio mobility for the upper-layer services via handoff.

Packet Data Service Node (PDSN)

- Implements switching of packet data services of mobile subscribers.
- One PDSN can be connected to multiple PCFs.
- It provides the interface between the radio network and the packet data network.

Home Agent (HA)

- Locates the place where the Mobile Node opens its account.
- Receive the registration information from the MN.
- Similar to HLR in mobile network.
- Broadcast the accessible information of mobile network.
- Setup the tunnel between FA (Foreign Agent) and HA.
- Transfer the data from other computer to the MN via the tunnel.

Mobile Switching Center (MSC)

- Manages communication between GSM and other networks
- Call setup function and basic switching
- Call routing
- Billing information and collection
- Mobility management
  - Registration
  - Location Updating
  - Inter BSS and inter MSC call handoff
- MSC does gateway function while its customer roams to other network by using HLR/VLR.

Home Location Registers (HLR)

- It is a permanent database about mobile subscribers in a large service area(generally one per GSM network operator)
- Database contains IMSI,MSISDN,prepaid/postpaid,roaming restrictions,supplementary services.

Visitor Location Registers (VLR)

- Temporary database which updates whenever new MS enters its area, by HLR database
- Controls those mobiles roaming in its area and reduces number of queries to HLR
- Database contains IMSI,TMSI,MSISDN,MSRN,Location Area,authentication key

2.6.2 Channels in CDMA

- **Forward Channels**
  - The Forward CDMA channel is the **cell-to-mobile** direction of communication or the **downlink path**.
- **Reverse Channels**
  - The Reverse CDMA channel is the **mobile-to-cell** direction of communication or the **uplink path**.

Forward Channels

- **Pilot Channel**
  - It is a reference channel which the mobile station uses for acquisition, timing and as a phase reference for demodulation.
  - It is transmitted at all times by each base station on each active CDMA frequency. Each mobile station tracks this signal continuously.
- **Synchronization Channel**
  - It carries a single, repeating message that conveys the timing and system configuration information to the mobile station in the CDMA system.
  - Works at 1200bps.
- **Paging Channel**
  - Its primary purpose is to send out pages, that is, notifications of incoming calls, to the mobile stations.
  - The base station uses them to transmit system overhead information and mobile station- specific messages.
  - Works at 9600,4800, and 2400bps.
- **Forward Traffic Channels**
  - They are code channels used to assign call (usually voice) and signaling traffic to individual users.

Reverse Channels

- **Access Channels**
  - They are used by mobile stations to initiate communication with the base station or to respond to Paging Channel messages.
  - The Access Channel is used for short signaling message exchanges such as call origination's, responses to pages, and registrations.
- **Reverse Traffic Channels**
  - They are used by individual users during their actual calls to transmit traffic from a single mobile station to one or more base stations.

CDMA Vs GSM

Feature	CDMA	GSM
Stands for	Code Division Multiple Access	Global System for Mobile communication
Storage Type	Internal Memory	SIM (subscriber identity module) Card
Global market share	25%	75%
Dominance	Dominant standard in the U.S.	Dominant standard worldwide except the U.S.
Data transfer	EVDO/3G/4G/LTE	GPRS/E/3G/4G/LTE
Network	There is one physical channel and a special code for every device in the coverage network. Using this code, the signal of the device is multiplexed, and the same physical channel is used to send the signal.	Every cell has a corresponding network tower, which serves the mobile phones in that cellular area.
International roaming	Less Accessible	Most Accessible
Frequency band	Single (850 MHz)	Multiple (850/900/1800/1900 MHz)
Network service	Handset specific	SIM specific. User has option to select handset of his choice.

CHAPTER 3

WIRELESS IN LOCAL LOOP

3.1 Introduction

- Wireless Local Loop (WLL) is a system that connects subscribers to the public switched telephone network (PSTN) using radio signals as a substitute for copper for all or part of the connection between the subscriber and the switch.
- Sometimes called radio in the loop (RITL) or fixed-radio access (FRA).
- This includes cordless access systems, proprietary fixed radio access, and fixed cellular systems.
- Using a wireless link shortens the construction period and also reduces installation and operating costs.
- WLL will be implemented across five categories of wireless technology.
- They are digital cellular, analog cellular, PCN/PCS, CT-2/DECT, and proprietary implementations.
- Each of these technologies has a mix of strengths and weaknesses for WLL applications.

3.1.1 Analog Cellular

- There are currently three main analog cellular system types operating in the world: advanced mobile phone system (AMPS), nordic mobile telephone (NMT), and total access communications systems (TACS).
- As a WLL platform, analog cellular has some limitations in regards to capacity and functionality.
- Given its characteristics, analog cellular is best suited to serve low-density to medium-density markets that don't require landline-type features.

3.1.2 Digital Cellular

- Major worldwide digital cellular standards include global system for mobile communications (GSM), time division multiple access (TDMA), Hughes enhanced TDMA (E-TDMA), and code division multiple access (CDMA).
- Like analog cellular, digital cellular has the benefit of wide availability.
- Digital cellular can support higher capacity subscribers than analog cellular, and it offers functionality that is better suited to emulate capabilities of advanced wireline networks.
- Its disadvantage is that it is not as scalable as analog cellular.

3.1.3 Personal Communications Services (PCS)/Personal Communications Network (PCN)

- PCS/PCN incorporates elements of digital cellular and cordless standards as well as newly developed RF protocols.
- Its purpose is to offer low-mobility wireless service using low-power antennas and lightweight, inexpensive handsets.

- PCN is primarily seen as a city communications system with far less range than cellular.
- PCS let people or devices communicate regardless of where they are.
- Some of the services include personal numbers assigned to individuals rather than telephones, call completion regardless of locations ("find me"), calls to the PCS customer that can be paid by either the caller or the receiver, and call management services that give the called party greater control over incoming calls.
- PCS/PCN has the advantage of being designed specifically to provide WLL by public wireless operators.
- The main weakness of PCS/PCN is that it is not yet commercially available.

3.1.4 Cordless Telephones 2nd Generation/Digital European Cordless Telephone (CT-2/DECT)

- Cordless telephony was originally developed to provide wireless access within a residence or business between a base station and a handset.
- DECT is considered WLL when a public network operator provides wireless service directly to the user via this technology.
- Although DECT does not appear to be ideally suited for rural or low-density applications, it has some significant advantages in medium-density to high-density areas.
- Cordless telephony has advantages in terms of scalability and functionality.
- As compared to cellular technology, DECT is capable of carrying higher levels of traffic, provides better voice quality, and can transmit data at higher rates.

3.1.5 Proprietary Implementations

- Proprietary WLL systems encompass a variety of technologies and configurations.
- These systems are considered proprietary because they are not available on public wireless networks and are typically customized for a specific application.
- They generally do not provide mobility. This makes proprietary technology most effective for applications that cannot cost effectively or time effectively be reached by landline alternatives.
- Proprietary systems are, therefore, positioned to provide basic fixed wireless telephony in low-demand and medium-demand density applications.

3.2 Technical requirements of WLL systems

The following conditions are required of WLL systems which are looked to as a replacement for existing copper subscriber lines.

1) Communications quality

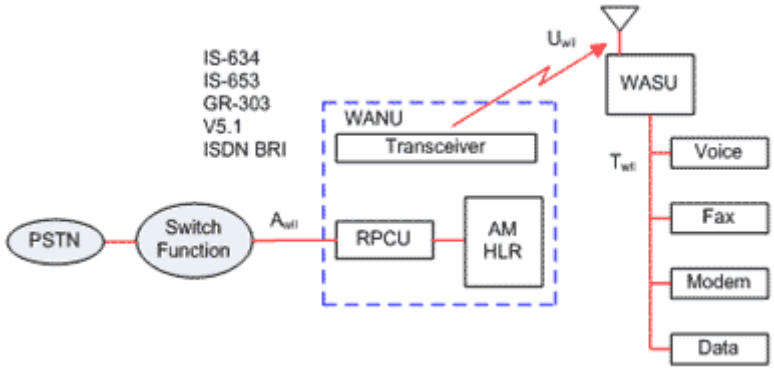
- Since a WLL system serves as the access line for fixed telephone sets, it must provide the same level of quality as conventional telephone systems with respect to such aspects as speech quality, grade of service (GOS), connection delay and speech delay.

- In addition, since radio waves are used, careful consideration must be given to protection of confidentiality and terminal authentication.

2) **Short construction period**
3) **Low cost**
   - The overall cost must be low, including equipment, construction and maintenance costs.
4) **Absence of interference with other wireless systems**
   - A WLL system must not cause any interference with the operation of existing systems, such as microwave communications and broadcasting systems.
5) **High traffic volume**
   - One characteristic of a WLL system is that it must support a larger traffic volume per subscriber than mobile communications systems.

3.3 WLL Reference Model

WLL refers to a system that is used to link subscribers to the PSTN with the help of radio signals.



WLL architecture contains the following major components:

Wireless Access Network Unit (WANU)

- It is an interface between underlying telephone network and wireless link that consists of Base Station Transceivers (BTS) or Radio Ports (RP) , Radio Port Controller Unit (RPCU) or BSC Access Manager (AM), Home Location Register (HLR)
- RP is a base station of WLL system.

RPCU - Radio Port Control Unit

- It connects a number of cell site based station transceivers and associated antennas.
- The RPCU provides the interface between the base stations and a telephone switch.
- It provides control and signaling functions for implementing the air interface to wireless handsets through the base stations Access Manager (AM).
- The access manager/home location register (AM/HLR) handles authentication and privacy**.**

Wireless Access Subscriber Unit (WASU)

- It is located at the subscriber.
- It translates wireless link into a traditional telephone connection.
- It provides an air interface toward the network and another interface to the subscriber.
- This interface includes protocol conversion and transcoding, authentication functions.

Switching Function

- It can be a digital switch.
- All the SF include ISDN algorithms.
- It is the transmission link between WANU & SF can be microwave or cable.

Advantages of WLL

1. **Cost**: Wireless systems are less expensive than wired systems.
2. **Installation Time**: WLL systems can be installed rapidly. Only problem is selection of frequency band and authorization to use it. Once it is obtained, it can be easily installed.
3. **Mobile Cellular Technology**: Current cellular systems are too expensive and do not provide sufficient facilities to act as a realistic alternative to WLL systems. A major advantage of WLL over mobile cellular is that, since the subscriber unit is fixed, the subscriber can use a directional antenna pointed at the base station antenna, providing improved signal quality in both the directions.

Limitations of WLL

1. Spectrum
    - Management of spectrum is the main issue in WLL system because WLL can be deployed only in licensed bands.
2. Service Quality
    - Reliability and fraud immunity must be fulfilled to provide good quality service.
3. Network Planning
    - Since subscriber units are fixed, antenna height and where to place this unit is the question in installation of WLL.
4. Economics
    - The major cost in wire-line is physical aspects and installation, whereas in WLL, it is electronics.

3.4 The Public Switched Telephone Network (PSTN)

- The term Public Switched Telephone Network (PSTN) describes the various equipment and interconnecting facilities that provide phone service to the public.
- The PSTN began in the United States in 1878 with a manual mechanical switchboard that connected different parties and allowed them to carry on a conversation.
- Today, the PSTN is a network of computers and other electronic equipment that converts speech into digital data and provides a multitude of sophisticated phone features, data services, and mobile wireless access.
- At the core of the PSTN are digital switches. The term "switch" describes the ability to cross-connect a phone line with many other phone lines and switching from one connection to another.
- The PSTN is well known for providing reliable communications to its subscribers.

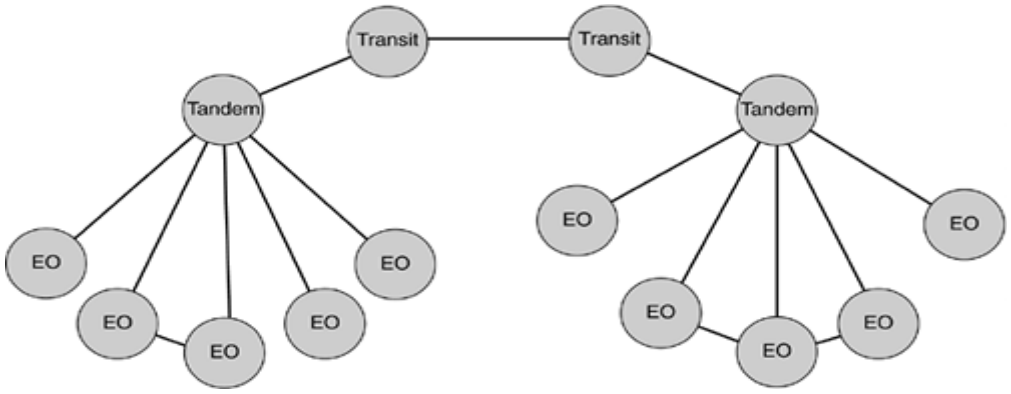
3.4.1General PSTN Hierarchies

Depending on geographical region, PSTN nodes are sometimes referred to by different names. The three node types we discuss in this chapter include:

End Office (EO): Also called a Local Exchange. The End Office provides network access for the subscriber. It is located at the bottom of the network hierarchy.

Tandem: Connects EOs together, providing an aggregation point for traffic between them. In some cases, the Tandem node provides the EO access to the next hierarchical level of the network.

Transit: Provides an interface to another hierarchical network level. Transit switches are generally used to aggregate traffic that is carried across long geographical distances.



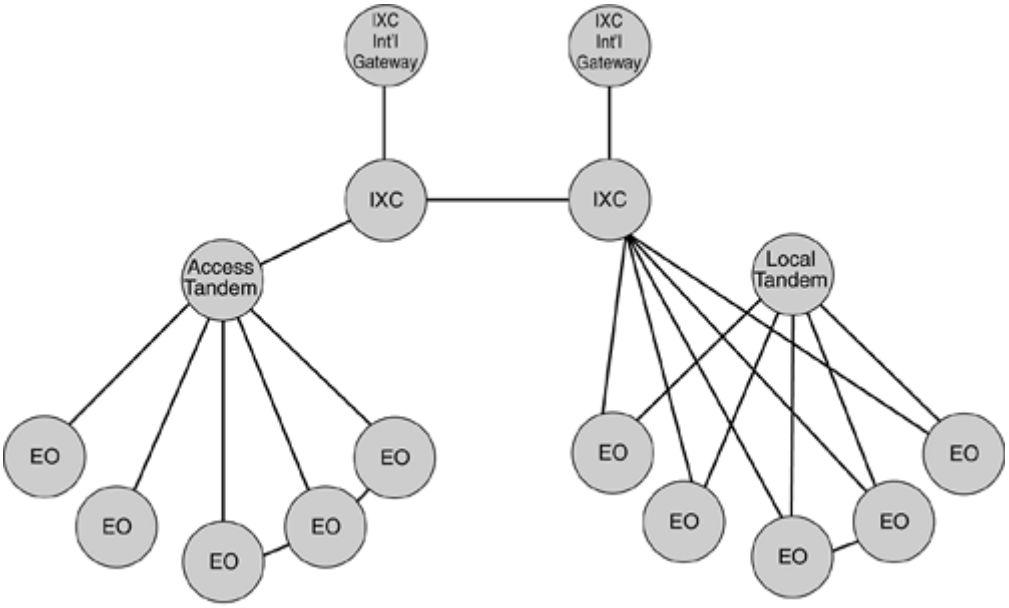
- There are two primary methods of connecting switching nodes.
- The first approach is a **mesh topology**, in which all nodes are interconnected. This approach does not scale well when you must connect a large number of nodes. You must connect each new node to every existing node. This approach does have its merits, however; it simplifies routing traffic between nodes and avoids bottlenecks by involving only those switches that are in direct communication with each other.
- The second approach is a **hierarchical tree** in which nodes are aggregated as the hierarchy traverses from the subscriber access points to the top of the tree.
- PSTN networks use a combination of these two methods, which are largely driven by cost and the traffic patterns between exchanges.
- In a generic PSTN hierarchy, End Offices are connected locally and through tandem switches.
- Transit switches provide further aggregation points for connecting multiple tandems between different networks.
- While actual network topologies vary, most follow some variation of this basic pattern.
- The PSTN hierarchy is implemented differently in the United States and the United Kingdom.

3.4.2 PSTN Hierarchy in the United States

- In the United States, the PSTN is generally divided into three categories:
  - Local Exchange Networks

- InterExchange Networks
- International Networks

- Local Exchange Carriers (LECs) operate Local Exchange networks, while InterExchange Carriers (IXCs) operate InterExchange and International networks.



- **Local Exchange Network**

- The Local Exchange network consists of the digital switching nodes (EOs) that provide network access to the subscriber.
- The Local Exchange terminates both lines and trunks, providing the subscriber access to the PSTN.
- A Tandem Office often connects End Offices within a local area, but they can also be connected directly. In the United States, Tandem Offices are usually designated as either Local Tandem (LT) or Access Tandem (AT).
- The primary purpose of a Local Tandem is to provide interconnection between End Offices in a localized geographic region.
- An Access Tandem provides interconnection between local End Offices and serves as a primary point of access for IXCs.
- Trunks are the facilities that connect all of the offices, thereby transporting inter-nodal traffic.

- **InterExchange Network**

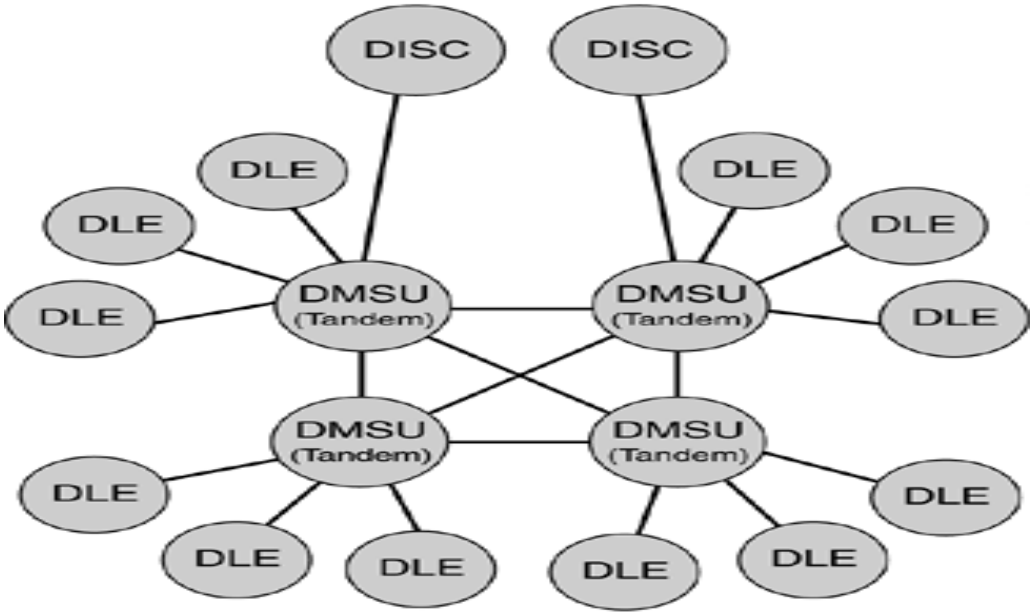
- The InterExchange network is comprised of digital switching nodes that provide the connection between Local Exchange networks. Because they are points of high traffic aggregation and they cover larger geographical distances, high-speed transports are typically used between transit switches.
- In the deregulated U.S. market, transit switches are usually referred to as *carrier switches*.
- In the U.S., IXCs access the Local Exchange network at designated points, referred to as a Point of Presence (POP). POPs can be connections at the Access Tandem, or direct connections to the End Office.

- **International Network**

- The International network consists of digital switching nodes, which are located in each country and act as international gateways to destinations outside of their respective countries.
- These gateways adhere to the ITU international standards to ensure interoperability between national networks.
- The international switch also performs the protocol conversions between national and international signaling

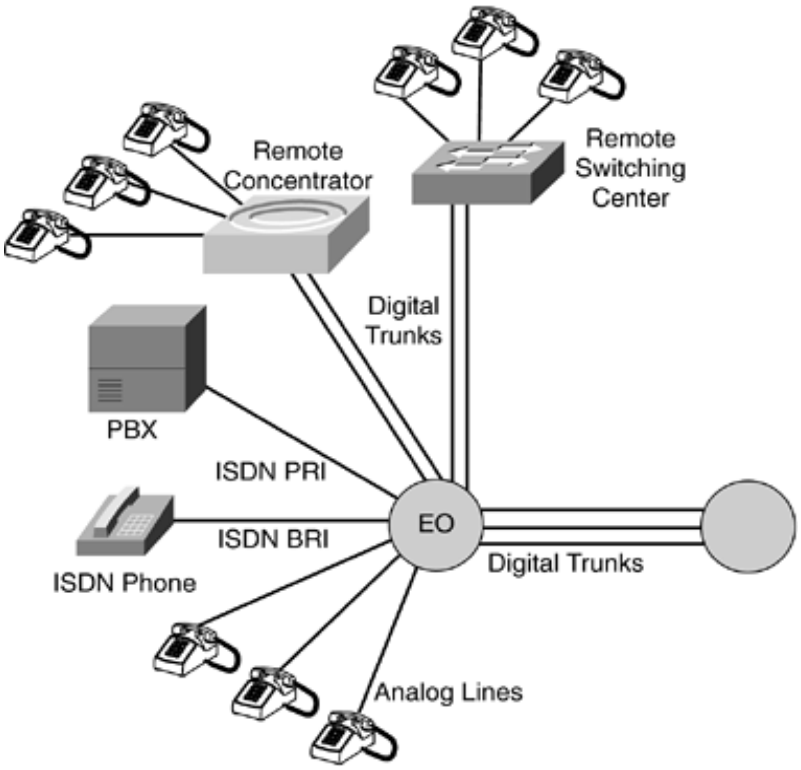
3.4.3 PSTN Hierarchy in the United Kingdom

End Offices are referred to as Digital Local Exchanges (DLE). A fully meshed tandem network of Digital Main Switching Units (DMSU) connects the DLEs. Digital International Switching Centers (DISC) connect the DMSU tandem switches for international call connections.



3.5 Access and Transmission Facilities

- Connections to PSTN switches can be divided into two basic categories: lines and trunks.
- Individual telephone lines connect subscribers to the Central Office (CO) by wire pairs, while trunks are used to interconnect PSTN switches.
- Trunks also provide access to corporate phone environments, which often use a Private Branch eXchange (PBX) or their own digital switch.



3.6 Lines

- Lines are used to connect the subscriber to the CO, providing the subscriber access into the PSTN. The following sections describe the facilities used for lines, and the access signaling between the subscriber and the CO.

3.6.1 The Local Loop

- The local loop consists of a pair of copper wires extending from the CO to a residence or business that connects to the phone, fax, modem, or other telephony device.
- The local loop allows a subscriber to access the PSTN through its connection to the CO.

3.6.2 Analog Line Signaling

- Currently, most phone lines are analog phone lines.
- They are referred to as analog lines because they use an analog signal over the local loop, between the phone and the CO.
- The analog signal carries two components that comprise the communication between the phone and the CO: the voice component, and the signaling component.

3.6.3 Dialing

- When a subscriber dials a number, the number is signaled to the CO as either a series of pulses based on the number dialed, or by Dual Tone Multi-Frequency (DTMF) signals.

- The DTMF signal is a combination of two tones that are generated at different frequencies.

3.6.4 Ringing and Answer

- To notify the called party of an incoming call, the CO sends AC ringing voltage over the local loop to the terminating line.
- The incoming voltage activates the ringing circuit within the phone to generate an audible ring signal.
- The CO also sends an audible ring-back tone over the originating local loop to indicate that the call is proceeding and the destination phone is ringing.
- When the destination phone is taken off-hook, the CO detects the change in loop current and stops generating the ringing voltage.
- This procedure is commonly referred to as *ring trip*.
- The off-hook signals the CO that the call has been answered; the conversation path is then completed between the two parties and other actions, such as billing, can be initiated, if necessary.

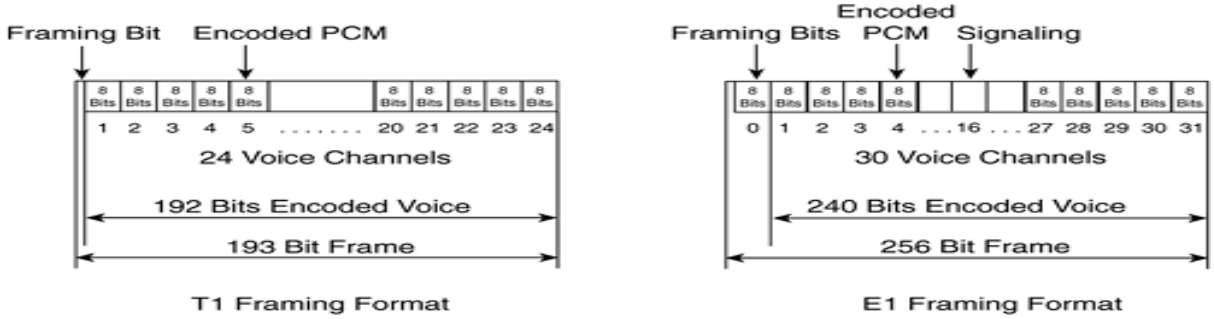
3.6.5 Voice Encoding

- An analog voice signal must be encoded into digital information for transmission over the digital switching network.
- The conversion is completed using a codec (coder/decoder), which converts between analog and digital data.

3.6.6 ISDN BRI

- There are two ISDN interface types: Basic Rate Interface (BRI) for lines, and Primary Rate Interface (PRI) for trunks.
- BRI multiplexes two bearer (2B) channels and one signaling (D) channel over the local loop between the subscriber and the CO; this is commonly referred to as 2B+D.
- The two B channels each operate at 64 kb/s and can be used for voice or data communication.
- The D channel operates at 16 kb/s and is used for call control signaling for the two B channels.
- The D channel can also be used for very low speed data transmission.

3.7 Trunks



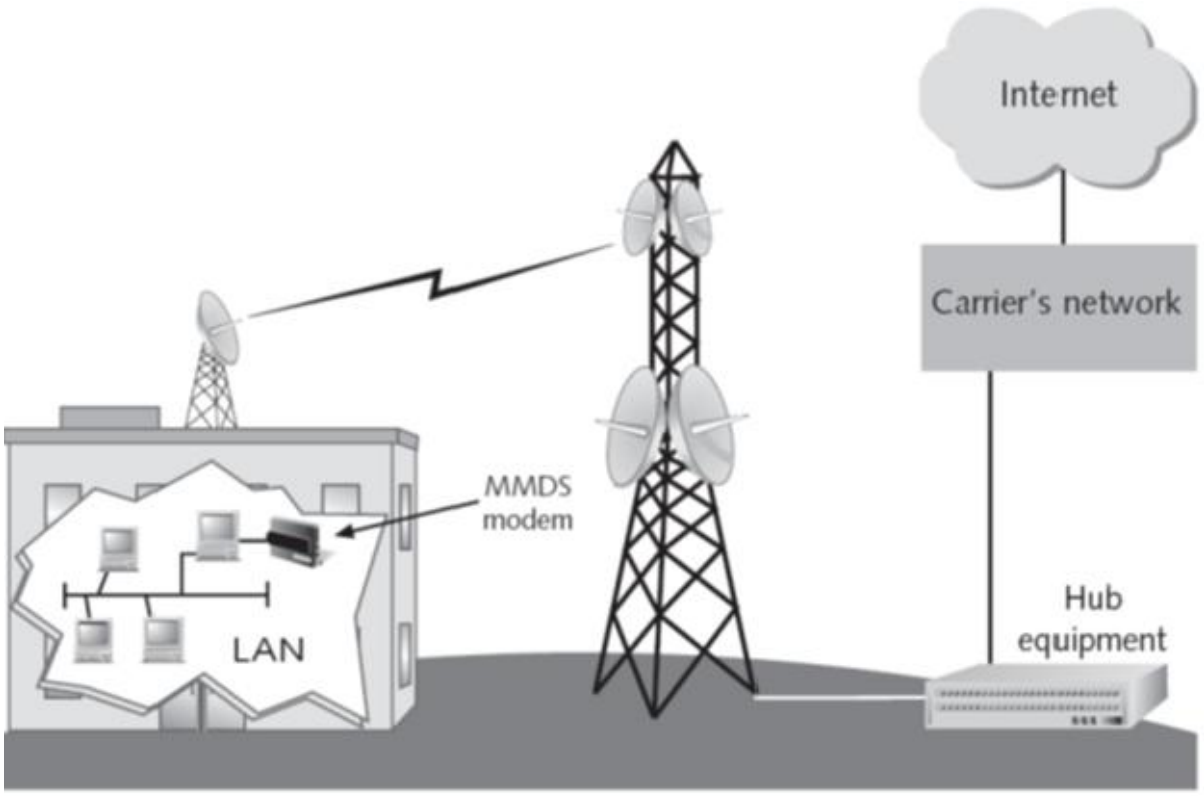
- Trunks carry traffic between telephony switching nodes.
- While analog trunks still exist, most trunks in use today are digital trunks.
- Digital trunks may be either four-wire (twisted pairs) or fiber optic medium for higher capacity.
- T1 and E1 are the most common trunk types for connecting to End Offices. North American networks use T1, and European networks use E1.
- On the T1/E1 facility, voice channels are multiplexed into digital bit streams using Time Division Multiplexing (TDM).
- TDM allocates one timeslot from each digital data stream's frame to transmit a voice sample from a conversation.
- Each frame carries a total of 24 multiplexed voice channels for T1 and 31 channels for E1.
- The T1 frame uses a single bit for framing, while E1 uses a byte.

3.8 Multichannel multipoint distribution service (MMDS)

- MMDS is a broadcasting and communications service that operates in the ultra−high−frequency(UHF) portion of the radio spectrum between 2.1 and 2.7 GHz.
- MMDS is also known as wireless cable.
- In MMDS, a medium−power transmitter is located with an omni−directional broadcast antenna at or near the highest topographical point in the intended coverage area.
- The workable radius can reach up to 70 miles in flat terrain (significantly less in hilly or mountainous areas).

Key Elements of MMDS system

1. **The Headend**
   - Equipment such as signal processors, demodulators and Satellite Receivers to generate input baseband video and audio signals.
2. **The Transmitter**
   - The Transmitter converts the broadband signal provided by the modulators to the transmit microwave frequency (2500 to 2586 MHz) and amplifies the resulting microwave signal to the power level desired for transmission.
3. **The Transmitting Antenna**
   - The Transmitting Antenna system includes the cables or waveguide connecting the transmitter to the antenna, as well as the antenna itself.
4. **The Subscriber Equipment**
   - The Subscriber Equipment consists of an outdoor unit which converts the received microwave signal to frequencies in the 220 to 408 MHz range, which is suitable for feeding standard TV sets. The outdoor unit is connected through a coaxial cable to the subscriber’s home wiring or directly to the TV set.



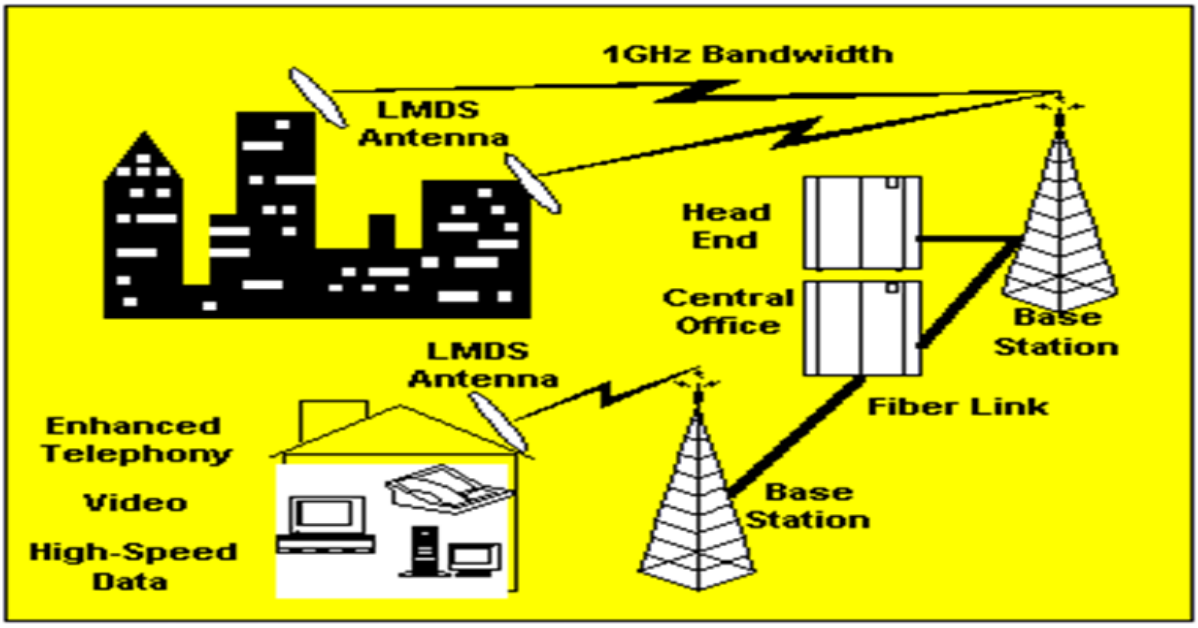
Advantages and disadvantages of MMDS

- Propagation over long distances up to 100 km with single tower
- Less attenuation due to rain, foliage
- RF component costs lower at 2.5 GHz
- Equipment readily available today
- Limited capacity without sectorization, cellularization which adds complexity and cost
- Interference issues with other MMDS and ITFS licensees
- Large upstream bandwidth in MMDS band requires careful planning, filtering etc.
- Cellularization later on may require retuning the entire network.

3.9 Local Multipoint Distribution Service (LMDS)

- Local Multipoint Distribution Service (LMDS) is an ideal solution for bringing high-bandwidth services to homes and offices within the last-mile—an area where cable or optical fiber may not be convenient or economical.
- Having architectural similarities with cellular networks, LMDS is a fixed (non-mobile) point-to-multipoint wireless access technology that typically operates in the 28 GHz band and offers Line-of-Sight (LoS) coverage up to 3-5 km.
- Depending on the local licensing regulations in a country, such broadband wireless systems may operate anywhere from 2 to 42 GHz.

- Though data transfer rates for LMDS can reach 1.5 to 2 Gbps, in reality it is designed to deliver data at speeds between 64 Kbps to 155 Mbps a more realistic downstream average being around 38 Mbps.
- At such speeds, LMDS may be the key to bringing multimedia data, supporting voice connections, the Internet, videoconferencing, interactive gaming, video streaming and other high-speed data applications to millions of customers worldwide over the air.
- As with other wireless networks, LMDS technology offers the advantage that it can be deployed quickly and relatively inexpensively. New market entrants who do not have an existing network like incumbent's copper wires or fibers - can rapidly build an advanced wireless network and start competing. LMDS is also attractive to incumbent operators who need to complement or expand existing networks.



Advantages and disadvantages of LMDS

- Very large bandwidth available for data, IP telephony, video conferencing services
- Large capacity
- Higher RF component costs
- Small cell size, 2-8 Km.
- Does not cover entire metropolitan area of a large city without adding many cells at high cost

3.9 Satellite System

- Satellite is a system that supports mobile communications
- It offers global coverage without wiring costs for base stations and is almost independent of varying population densities
- Two or more stations on Earth are called ‘Earth Stations’
  - One or more stations in Earth Orbit called ‘Satellites’
- Uplink frequency is used for transmission to satellite.

- Downlink is used for transmission to earth station.
- The satellite converts uplink transmissions into downlink transmission via a transponder'

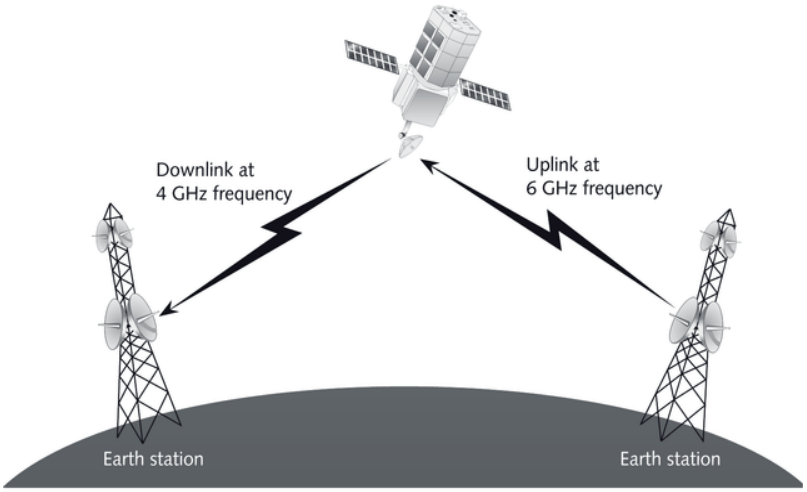
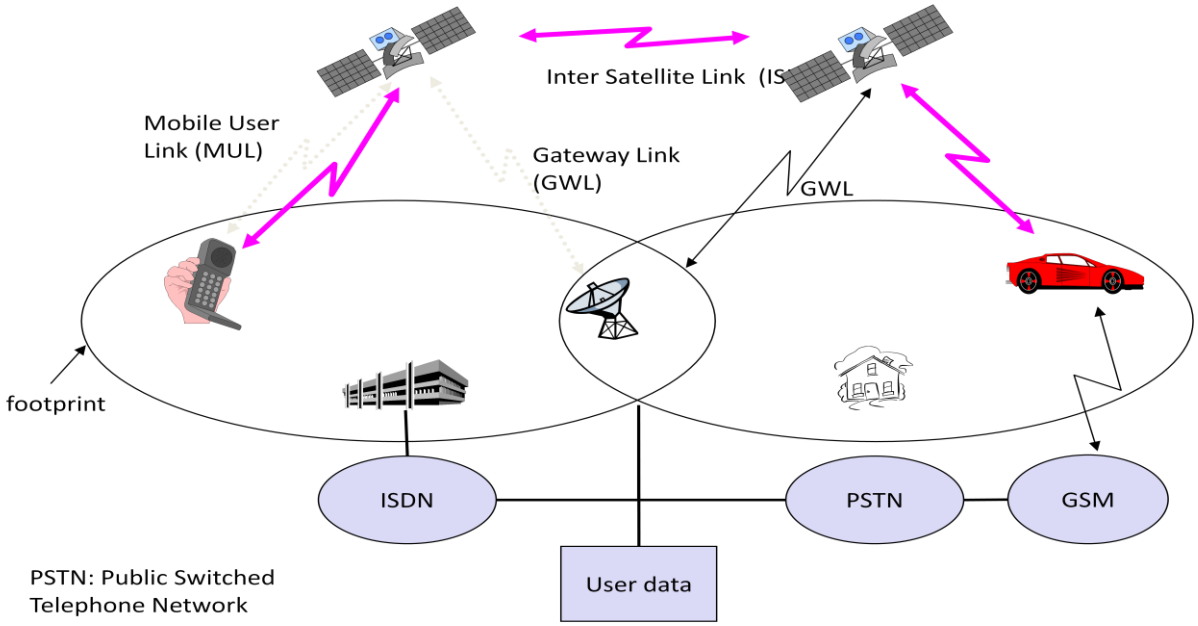


Figure 1-4 Satellite frequency transmission

Applications

- Weather forecasting: several satellites deliver pictures of the earth.
- Radio and TV broadcast satellites: hundreds of radio and TV programs are available via satellite. This technology competes with cable in many places as it is cheap
- Military satellites
- Satellites for navigation and localization (e.g., GPS). Almost all ships and aircraft rely on GPS in addition to traditional navigation systems.



- A communication satellite functions as an overhead wireless repeater station that provides a microwave communication link between two geographically remote sites.
- Due to its high altitude, satellite transmissions can cover a wide area over the surface of the earth.
- Each satellite is equipped with various "transponders" consisting of a transceiver and an antenna tuned to a certain part of the allocated spectrum.
- The incoming signal is amplified and then rebroadcast on a different frequency.
- Most satellites simply broadcast whatever they receive, and are often referred to as "bent pipes".
- These were traditionally used to support applications such as TV broadcasts and voice telephony.
- In recent times, the use of satellites in packet data transmission has been on the rise. They are typically used in WAN networks where they provide backbone links to geographically dispersed LAN's and MAN's.
- Figure above shows a classical scenario for satellite systems supporting global mobile communication. Depending on its type, each satellite can cover a certain area on the earth with its beam (the so-called ‘footprint’.
- Within the footprint, communication with the satellite is possible for mobile users via a mobile user link (MUL) and for the base station controlling the satellite and acting as gateway to other networks via the gateway link (GWL).
- Satellites may be able to communicate directly with each other via inter-satellite links (ISL).
- This facilitates direct communication between users within different footprints without using base stations or other networks on earth.
- Saving extra links from satellite to earth can reduce latency for data packets and voice data.
- Some satellites have special antennas to create smaller cells using spot beams

CHAPTER 4

WIRELESS LOCAL AREA NETWORKS (WLAN)

4.1 Introduction

- A WLAN is a wireless computer network that connects two or more devices using a wireless distribution within a limited area, such as in a school or an office building.
- It provides the facility of mobility to its users within the coverage area.
- IEEE and ETSI support wireless networks.
- IEEE gives 802.11 standards for WLAN for both 2.4GHz and 5GHz bands.
- ETSI gives HiperLAN Types 1 and 2 standards for 5GHz band only.
- Mainly used for LAN extension, cross-building interconnect, ad hoc networking and nomadic access.

4.2 Advantages of WLAN

- **Flexibility:** Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.).
- **Planning:** Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans.
- **Design:** Wireless networks allow for the design of small, independent devices which can (for example) be put into a pocket. Cables not only restrict users but also designers of small PDAs, notepads etc. Wireless senders and receivers can be hidden in historic buildings.
- **Robustness:** Wireless networks can survive disasters, e.g., earthquakes or users pulling a plug. If the wireless devices survive, people can still communicate. Networks requiring a wired infrastructure will usually breakdown completely.
- **Cost**: Setting up a wireless network can be much more cost effective than buying and installing cables.
- **Expandability**: Adding new computers to a wireless network is as easy as turning the computer on (as long as you do not exceed the maximum number of devices).

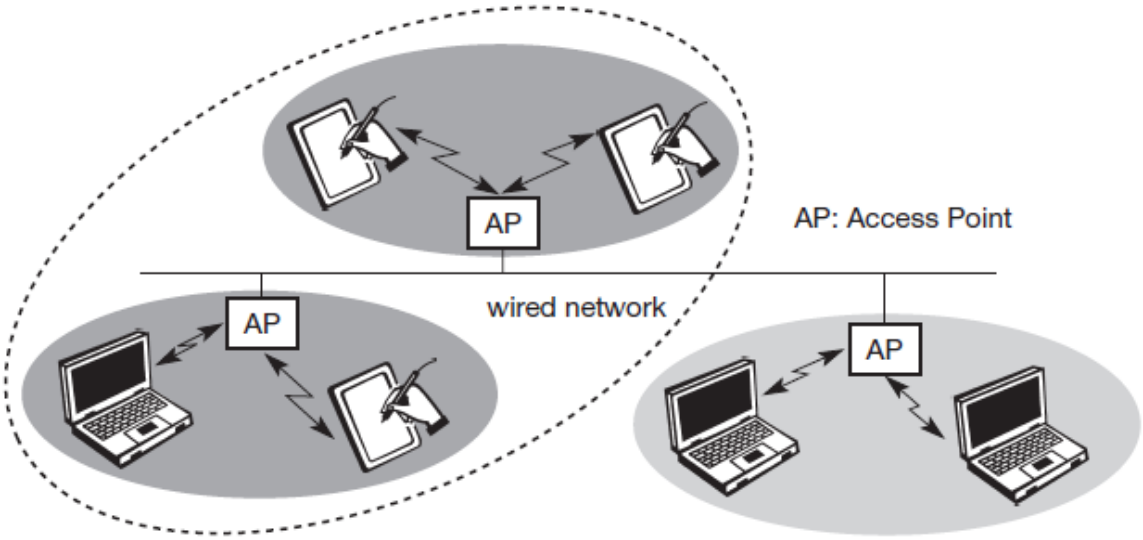
4.3 Disadvantages

- **Quality of service:** WLAN provides lower transmission quality compared to the wired LANs.
- **Proprietary solutions:** The cost of wireless equipment used in WLAN is much higher than that of the equivalent equipment used in wired LAN.
- **Restrictions:** All wireless products have to comply with national regulations. Several government and non-government institutions worldwide regulate the operation and restrict frequencies to minimize interference.
- **Safety and security:** WLAN provides less safety and security as information transmitted on the radio channel can be intercepted much easily than in the wired LAN.

4.4 Types of Wireless LAN

1. Infrastructure Based Wireless Network

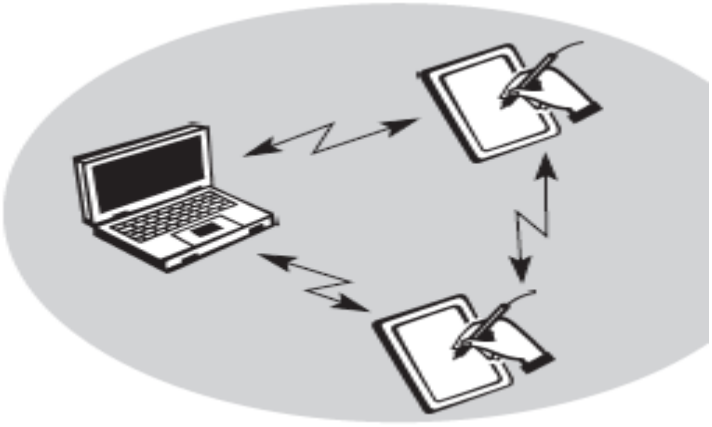
- This type of network allows users to move in a building while they are connected to computer resources.
- In an infrastructure network, a cell is also known as a Basic Service Area (BSA). It contains a number of wireless stations.
- The size of a BSA depends on the power of the transmitter and receiver units; it also depends on the environment.
- A number of BSAs are connected to each other and to a distribution system by Access Points (APs).
- A group of stations belonging to an AP is called a Basic Service Set (BSS).



2. Ad Hoc Wireless Network

- This network can be set up by a number of mobile users meeting in a small room. It does not need any support from a wired/wireless backbone. There are two ways to implement this network.
- **Broadcasting/Flooding**
  Suppose that a mobile user A wants to send data to another user B in the same area. When the packets containing the data are ready, user A broadcasts the packets. On receiving the packets, the receiver checks the identification on the packet. If that receiver was not the correct destination, then it rebroadcasts the packets. This process is repeated until user B gets the data.

- **Temporary Infrastructure**
  In this method, the mobile users set up a temporary infrastructure. But this method is complicated and it introduces overheads. It is useful only when there is a small number of a mobile user.



4.5 Wireless Equipments

Equipment	Description
Wireless Network Adapter	Used to connect Laptop or computer to WLAN. Provides connectivity to the device with LAN network. Can be internal or external.
Wireless Switch	Connect multiple computers, laptops or other devices to a WLAN.
Wireless Router	Connect multiple computers, laptops to a shared Internet connection within a wireless LAN. Wireless router works as a shared gateway to the Internet.

Wireless Repeaters	It is a wireless signal amplifier that receives signals as input and generates amplified signals as output. It can also extend the size of WLAN.
Wireless Bridge	Connects multiple LANs (wired or wireless) at the MAC layer level. It can also be used to pass Internet connection to the devices connected to its LAN jacks.

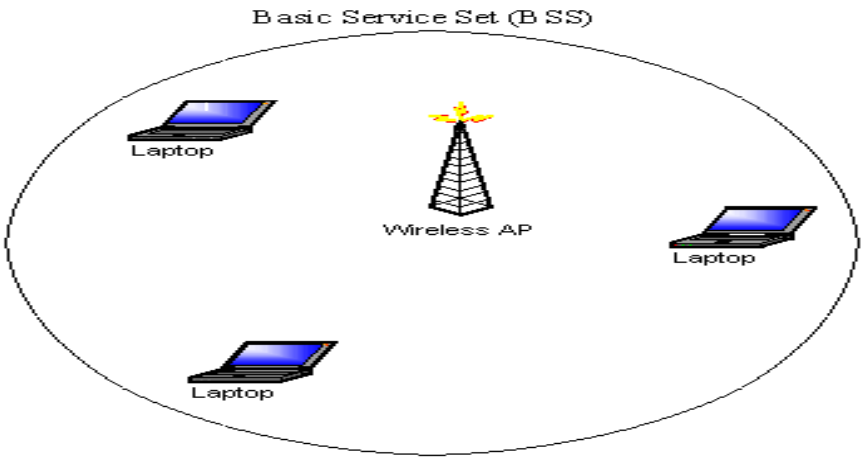
4.6 WLAN Topologies

- A topology refers to the arrangement of devices such as computer, laptop, smart phone, bridge, and router in a network.
- The topology structure of a network represents the physical or logical placement of network components so that they can connect to each other and share resources like the Internet.
- It is not concerned with the logical factors like transmission rates, distances among the devices and signal types.
- The different types of WLAN topologies are as follows:

1. Basic Service Set (BSS)
    a) Independent BSS
    b) Infrastructure BSS
2. Extended Service Set (ESS)

1. Basic Service Set

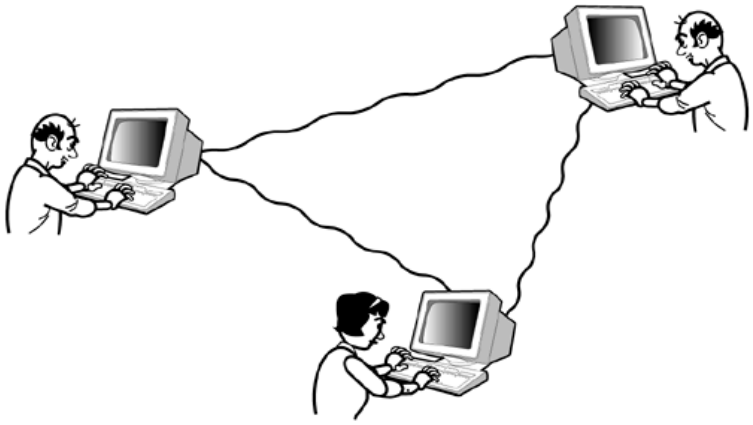
- A BSS consists of a group of computers and one AP, which links to a wired LAN.
- The **basic service set** (BSS) provides the **basic** building-block of an 802.11 wireless LAN.



(a) Independent Basic Service Set (IBSS)

- It is the simplest form of WLAN topology.
- Logically, this configuration is analogous to a peer-to-peer office network in which no single node is required to function as a server.
- Also called Ad-hoc network.

- Ad hoc WLANs include a number of nodes or wireless stations that communicate directly with one another on a peer-to-peer basis, without using an access point (AP) or any connection to a wired network.

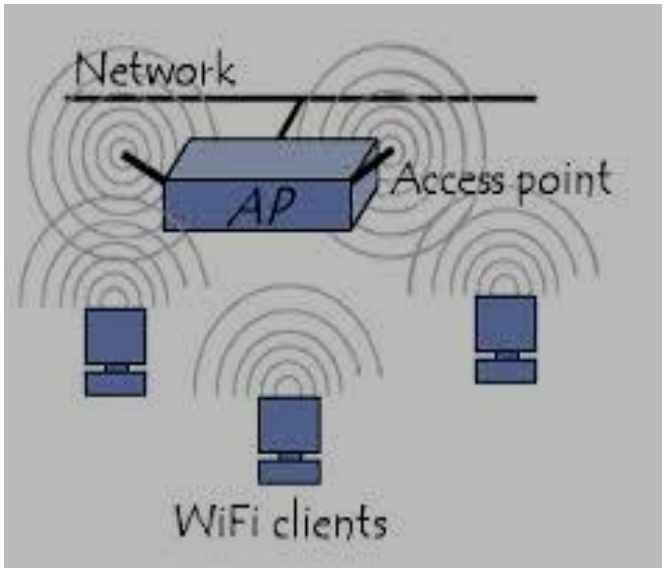


Limitations:

1. Only few devices can be connected to each other.
2. It works in a small compact area.
3. There is no way to manage connections.
4. There is no way to connect with bigger networks like LAN or Internet

(b) Infrastructure BSS

- An infrastructure BSS depends on a fixed device called an AP.
- It consists of a group of client devices and a single AP.
- AP is linked to the wired LAN and provides services to the client devices wirelessly.
- The area covered by an AP is known as BSS.



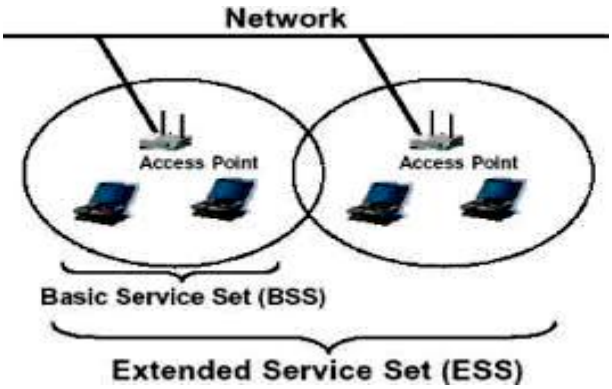
Service Set Identifier (SSID)

- A network may have many BSS that can be identified by SSID.
- SSID is code that must be attached with every packet on a wireless network.

- It is also used to identify a group of devices used in a service set.
- For example, in a college, various service sets may exist, like group of teachers or group of students.

2. Extended Service Set (ESS)

- Interconnected collection of BSSs is known as an ESS.
- It extends the services of wireless LANs by connecting BSSs.
- An ESS can be identified through SSID, which is 1 to 32 byte character string.



4.7 WLAN Technologies

The available technologies for implementing WLANs are as follows:

1. Infrared (IR)
2. Ultra High Frequency (UHF) (narrowband) radios
3. Spread Spectrum radios

1. Infrared (IR)

- IR is an invisible radiant energy having longer bandwidth than that of visible light.
- WLAN uses IR as a medium to transfer signal, but requires communicating devices in the line-of-sight.
- IR is a short-range technology.
- They do not penetrate through solid objects like building.
- Can be used only in indoor applications.
- Sunlight, fog, ice, and snow may affect the performance of IR-based system, thereby making IR unpopular for WLANs.

Advantages and Disadvantages of IR

Advantages

1. No license is required from government regulations.
2. Resistive to electro-magnetic and RF interference.

Disadvantages

1. It is a short-range technology (30-50 ft).
2. It has no penetration power
3. Affected by sunlight, fog, ice, snow and dirt.
4. Communicating device must be in line-of-sight(LoS).

2. Ultra High Frequency (UHF) (narrowband) radios

- The frequency range for UHF (narrowband) is 430-470MHz.
- 430-450MHz is the lower portion of the band and it is unprotected, unlicensed.
- 450-470MHz is the upper portion of the band and it is protected, licensed.
- Narrowband RF systems require power level in the range of 1 -2 watts.

Advantages and Disadvantages of UHF

Advantages

1. Offers longest frequency range.
2. Provides a low-cost solution.
3. Low to medium data throughput is required.

Disadvantages

1. Often, the throughput is low.
2. Large antenna is required.
3. License is required for protected bands.

3. Spread Spectrum Radios

- In this technique, signal generated with a particular bandwidth is purposely spread in a signal with wider bandwidth.
- In other words, this is a technique in which transmission of a signal takes place on a bandwidth significantly larger than the original bandwidth.
- Spread spectrum devices can be used in one of the following transmission procedures:
    1. **Direct Sequence Spread Spectrum (DSSS):** In this technique, digital radio transmission is done on multiple radio channels through a coding technique. For spreading the signal across a carrier frequency, the frequency spectrum is altered using this coding technique so as to increase its bandwidth.
    2. **Frequency Hopping Spread Spectrum (FHSS):** For synchronizing with the receiver, a hopping sequence is utilized in this technique. The signal is extended across a wider bandwidth because of the haphazard quality of the hopping sequence across the allocated frequency band of operation. As at any one time there is concentration of the RF power on one radio channel, the average output power is reduced.

Advantages and Disadvantages

Advantages

1. Bands are free.
2. Low data rates.
3. Reliable, secure and robust.
4. Low installation and maintenance cost.
5. Highly resistant to interference like noise.

Disadvantages

1. Limited communication distance upto 5 miles.

2. 2.4GHz band can be affected by microwave radiation.
3. Signals may heavily pollute the environment.

4.8 IEEE 802.11 WLAN

IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6, 5, and 60 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802).

The fundamental block of the IEEE 802.11 architecture is BSS. It is a collection of stations that are controlled by a single function, either Distributed Coordination Function (DCF) or Point Coordination Function (PCF). BSS covers a geographical area called Basic Service Area (BSA). A single BSS can be used to set an ad hoc network, which is a group of stations that communicate without adding an infrastructure network.

4.8.1 IEEE 802.11 WLAN Protocol Architecture

<table>
<tr><td rowspan="2">ISO/OSI
Data Link Layer</td><td colspan="3">802.2 Logical Link Control (LLC)</td></tr>
<tr><td colspan="3">802.11 Media Access Control (MAC)</td></tr>
<tr><td rowspan="2">ISO/OSI
Physical Layer
(PHY)</td><td colspan="3">802.11 Physical Layer Convergence Protocol (PLCP)</td></tr>
<tr><td>PMD 802.11
Infrared</td><td>PMD 802.11 FHSS
Frequency Hopping
Spread Spectrum</td><td>PMD 802.11 DSSS
Direct Sequence
Spread Spectrum</td></tr>
</table>

Fig. 4 IEEE 802.11 protocol architecture

- Figure above shows that the physical layer of 802.11 is divided into two different layers: PMD (Physical Medium Dependent) and PLCP (Physical Layer Convergence Protocol).
- The PMD layer offers physical medium-dependent access for infrared, FHSS (Frequency Hopping Spread Spectrum) and DSSS (Direct Sequence Spread Spectrum) communication.
- PLCP provides a medium-independent interface for the MAC (Medium Access Control) layer, which manages the package transport from one network interface to another through a shared transmission channel.
- **FHSS** uses the frequency hopping mechanism to avoid collisions with other WLAN devices. The baseband is divided into 79 channels, which are changed in a random order.

- **DSSS** uses the CDMA (Code Division Multiple Access) mechanism, which enables multiple transmissions on the same frequency channel for more than one transmitting device. The different signals are multiplexed with the help of device-unique codes and are de-multiplexed at the receiver's side.

4.8.2 IEEE 802.11 Physical Layer

IEEE 802.11 supports three different physical layers: one layer based on infra redand two layers based on radio transmission (primarily in the ISM band at 2.4GHz, which is available worldwide). All PHY variants include the provision ofthe **clear channel assessment** signal **(CCA)**. This is needed for the MAC mechanismscontrolling medium access and indicates if the medium is currently idle.The PHY layer offers a service access point (SAP) with 1 or 2 Mbit/s transferrate to the MAC layer (basic version of the standard).

(a) FHSS PHY Layer

Frequency hopping spread spectrum (FHSS) is a spread spectrum techniquewhich allows for the coexistence of multiple networks in the same area by separatingdifferent networks using different hopping sequences.

The standard specifies Gaussian shaped FSK (frequency shift keying), GFSK,as modulation for the FHSS PHY. For 1 Mbit/s a 2 level GFSK is used (i.e., 1 bit ismapped to one frequency, see chapter 2), a 4 level GFSK for 2 Mbit/s (i.e., 2 bitsare mapped to one frequency). While sending and receiving at 1 Mbit/s ismandatory for all devices, operation at 2 Mbit/s is optional.

Format of an IEEE 802.11 PHY frame using FHSS

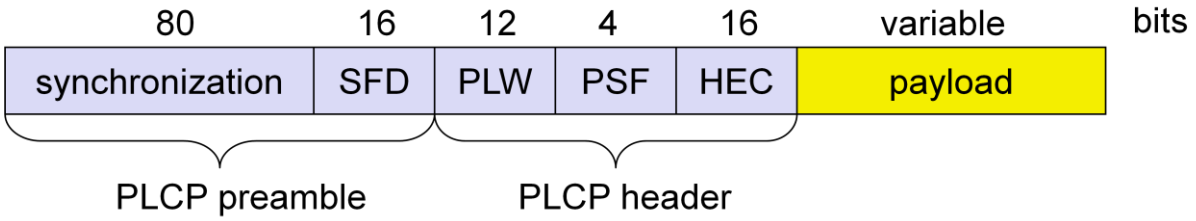


Figure shows a frame of the physical layer used with FHSS. The frameconsists of two basic parts, the PLCP part (preamble and header) and the payloadpart. While the PLCP part is always transmitted at 1 Mbit/s, payload, i.e.MAC data, can use 1 or 2 Mbit/s.

The fields of the frame fulfill the following functions:

Synchronization: The PLCP preamble starts with 80 bit synchronization,which is a 010101... bit pattern. This pattern is used for synchronization ofpotential receivers and signal detection by the CCA.

Start frame delimiter (SFD): The following 16 bits indicate the start of theframe and provide frame synchronization. The SFD pattern is0000110010111101.

PLCP_PDU length word (PLW): This first field of the PLCP header indicatesthe length of the payload in bytes including the 32 bit CRC at the endof the payload. PLW can range between 0 and 4,095.

PLCP signalling field (PSF): This 4 bit field indicates the data rate of the payload either 1 or 2 Mbit/s.
Header error check (HEC): Finally, the PLCP header is protected by a16 bit checksum.

(b) DSSS PHY Layer
Direct sequence spread spectrum (DSSS) is the alternative spread spectrummethod separating by code and not by frequency. In the case of IEEE 802.11DSSS, spreading is achieved using the 11-chip Barker sequence (+1, –1, +1, +1, –1,+1, +1, +1, –1, –1, –1). The key characteristics of this method are its robustnessagainst interference and its insensitivity to multipath propagation (time delayspread). However, the implementation is more complex compared to FHSS.
IEEE 802.11 DSSS PHY also uses the 2.4 GHz ISM band and offers both 1 and2 Mbit/s data rates. The system uses differential binary phase shift keying (DBPSK)for 1 Mbit/s transmission and differential quadrature phase shift keying (DQPSK)for 2 Mbit/s as modulation schemes.

Format of an IEEE 802.11 PHY frame using DSSS

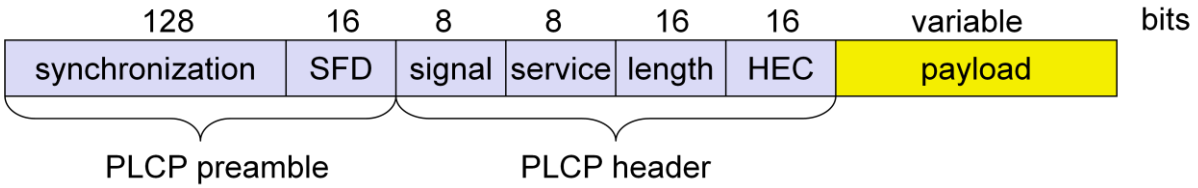


Figure shows a frame of the physical layer using DSSS. The frame consistsof two basic parts, the PLCP part (preamble and header) and the payloadpart. While the PLCP part is always transmitted at 1 Mbit/s, payload, i.e., MACdata, can use 1 or 2 Mbit/s.

The fields of the frame have the following functions:
Synchronization: The first 128 bits are not only used for synchronization,but also gain setting, energy detection (for the CCA), and frequency offsetcompensation.
Start frame delimiter (SFD): This 16 bit field is used for synchronization atthe beginning of a frame and consists of the pattern 1111001110100000.
Signal: Originally, only two values have been defined for this field to indicatethe data rate of the payloadeither 1 or 2 Mbit/s.
Service: This field is reserved for future use.
Length: 16 bits are used in this case for length indication of the payloadin microseconds.
Header error check (HEC): Signal, service, and length fields are protectedby this checksum.

(c) IR PHY Layer
The IEEE 802.11 physical layer specification uses Pulse Position Modulation (PPM) totransmit data using IR radiation. PPM varies the position of a pulse in order to transmitdifferent binary symbols. Extensions 802.11a and 802.11b address only microwave transmissionissues. Thus, the IR physical layer can be used to transmit information either at 1

or 2Mbps. For transmission at 1 Mbps, 16 symbols are used to transmit 4 bits of information,whereas in the case of 2 Mbps transmission, 2 data bits are transmitted using four pulses.

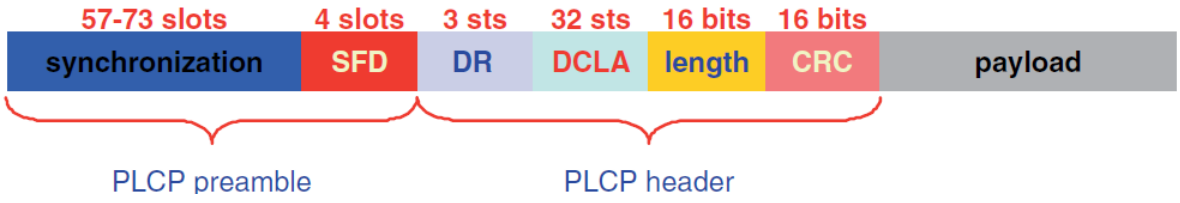


Figure shows a frame of the physical layer using IR.The fields of the frame have the following functions:

SYNC: Contains alternating pulses in consecutive time slots. It is used for receiversynchronization. The size of this field is between 57 and 73 bits.

Start frame delimiter (SFD): A 4-bit field that defines the beginning of a frame. It takes the value1001.

Data rate: A 3-bit field that takes the values 000 and 001 for 1 and 2 Mbps, respectively.

DC level adjustment: Consists of a 32-bit pattern that stabilizes the signal at the receiver.

Length: A 16-bit field containing the length of the MPDU in milliseconds.

CRC: A 16-bit frame check sequence (FCS) used for error detection.

MPDU(Payload): The 802.11 MAC protocol data unit to be sent. The size of this field ranges from 0to 4096 octets.

4.8.3 IEEE 802.11 MACLayer

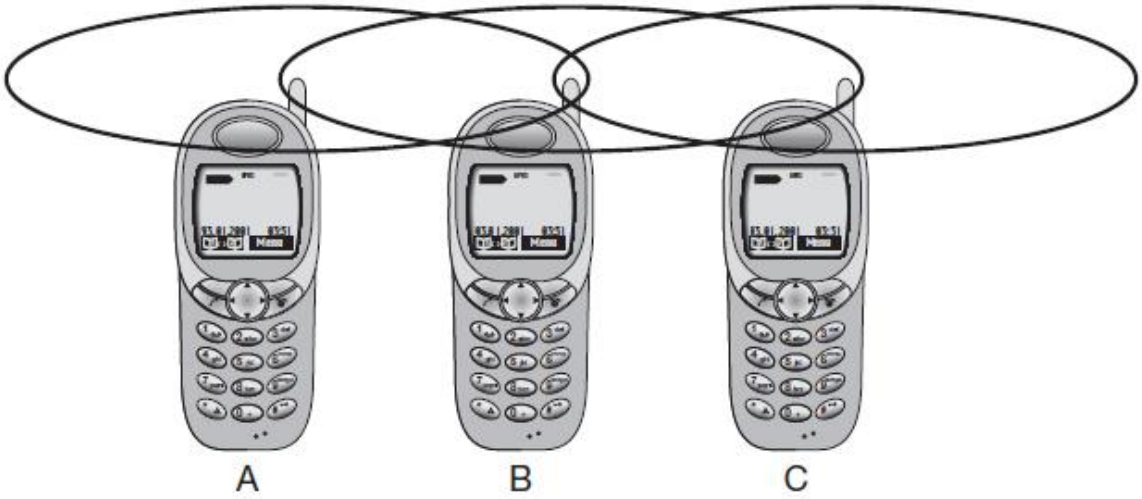
The data link layer within 802.11 consists of two sublayers: logical link control(LLC) and media access control (MAC). 802.11 uses the same 802.2 LLCand 48-bit addressing as the other 802 LAN, allowing for simple bridging fromwireless to IEEE wired networks, but the MAC is unique to WLAN. The sublayerabove MAC is the LLC, where the framing takes place. The LLC inserts certainfields in the frame such as the source address and destination address at the headend of the frame and error handling bits at the end of the frame.

The 802.11 MAC is similar in concept to 802.3, in that it is designed tosupport multiple users on a shared medium by having the sender sense the mediumbefore accessing it. For the 802.3 Ethernet LAN, the carrier sense multiple accesswith collision detection (CSMA/CD) protocol regulates how Ethernet stationsestablish access to the network and how they detect and handle collisions thatoccur when two or more devices try to simultaneously communicate over theLAN. In an 802.11 WLAN, collision detection is not possible due to the *near/far*problem. To detect a collision, a station must be able to transmitand listen at the same time, but in radio systems the transmission drowns out theability of a station to hear a collision.

Hidden and exposed terminals

Consider the scenario with three mobile phones as shown in Figure 3.1. Thetransmission range of A reaches B, but not C (the detection range does notreach C either). The transmission range of C reaches B, but not A. Finally, thetransmission range of B reaches A and C, i.e., A cannot detect C and vice versa.

A starts sending to B, C does not receive this transmission. C also wants tosend something to B and senses the medium. The medium appears to be free,the carrier sense fails. C also starts sending causing a collision at B. But A cannotdetect this collision at B and continues with its transmission. A is **hidden** for Cand vice versa.

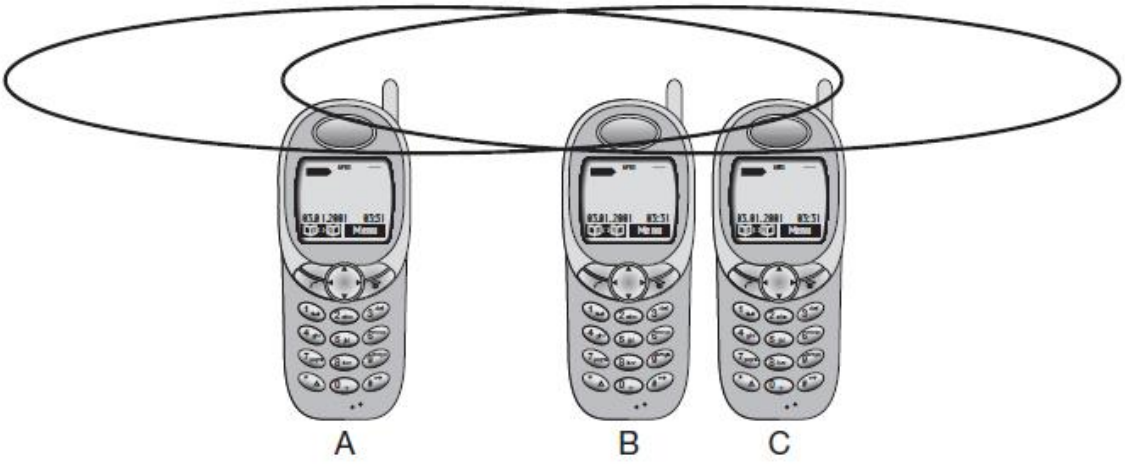


While hidden terminals may cause collisions, the next effect only causesunnecessary delay. Now consider the situation that B sends something to A andC wants to transmit data to some other mobile phone outside the interferenceranges of A and B. C senses the carrier and detects that the carrier is busy (B'ssignal). C postpones its transmission until it detects the medium as being idleagain. But as A is outside the interference range of C, waiting is not necessary.Causing a 'collision' at B does not matter because the collision is too weak topropagate to A. In this situation, C is **exposed** to B.

Near and far terminals scenario

- A and B are both sending with the same transmission power.
- As the signal strength decreases proportionally to the square of the distance, B's signal drowns out A's signal.
- As a result, C cannot receive A's transmission.
- Now think of C acts as a base station coordinating media access.
- In this case, terminal B would already drown out terminal A on the physical layer.
- C in return would have no chance of applying a fair scheme as it would only hear B.
- The **near/far effect is a severe problem.**
- **All** signals should arrive at the receiver with more or less the same strength.

- Otherwise a person standing closer to somebody could always speak louder than a person further away.
- Precise power control is needed to receive all senders with the same strength at a receiver.



CSMA/CA

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) is the *channel access* mechanism used by most wireless LANs in the ISM bands. A channel access mechanism is the part of the *protocol*which specifies how the node uses the medium : when to listen, when to transmit...

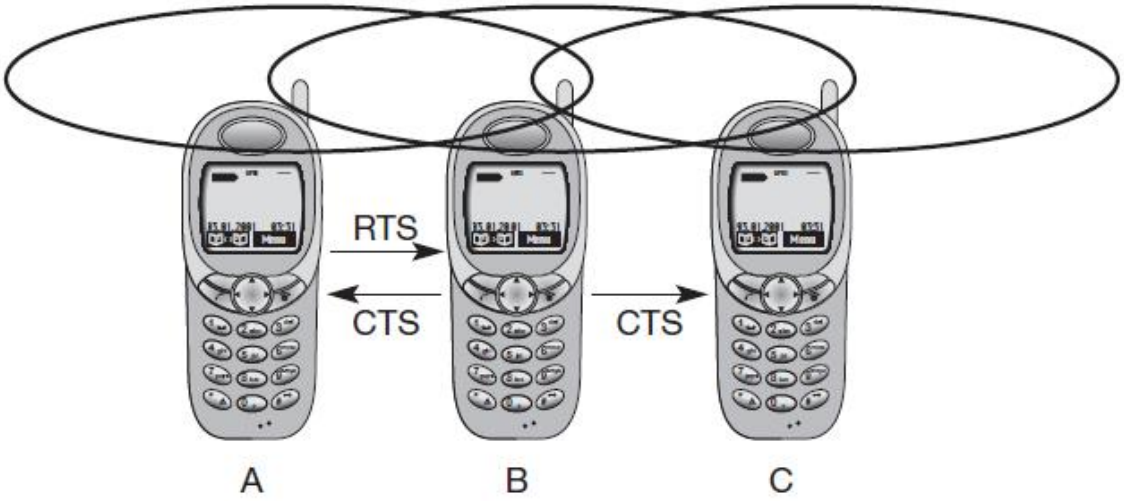
The basic principles of CSMA/CA are *listen before talk* and *contention*. This is an *asynchronous* message passing mechanism (connectionless), delivering a best effort service, but no bandwidth and latency guarantee. It's main advantages are that it is suited for network protocols such as TCP/IP, adapts quite well with the variable condition of traffic and is quite robust against interferences.

CSMA/CA is fundamentally different from the channel access mechanism used by cellular phone systems.

CSMA/CA is derived from CSMA/CD (Collision Detection), which is the base of *Ethernet*. The main difference is the *collision avoidance*: on a wire, the transceiver has the ability to listen while transmitting and so to detect collisions (with a wire all transmissions have approximately the same strength). But, even if a radio node could listen on the channel while transmitting, the strength of its own transmissions would mask all other signals on the air. So, the protocol can't directly detect collisions like with *Ethernet* and only tries to avoid them.

Multiple access with collision avoidance

Multiple access with collision avoidance (MACA) presents a simplescheme that solves the hidden terminal problem, does not need a base station.



MACA to Avoid Hidden Terminal Problem

With MACA, A does not start its transmission at once, but sends a **requestto send (RTS)** first. B receives the RTS that contains the name of sender andreceiver, as well as the length of the future transmission. This RTS is not heardby C, but triggers an acknowledgement from B, called **clear to send (CTS)**. TheCTS again contains the names of sender (A) and receiver (B) of the user data,and the length of the future transmission. This CTS is now heard by C and themedium for future use by A is now reserved for the duration of the transmission.After receiving a CTS, C is not allowed to send anything for the durationindicated in the CTS toward B. A collision cannot occur at B during data transmission,and the hidden terminal problem is solved – provided that thetransmission conditions remain the same. (Another station could move into thetransmission range of B after the transmission of CTS.)

Still, collisions can occur during the sending of an RTS. Both A and C couldsend an RTS that collides at B. RTS is very small compared to the data transmission,so the probability of a collision is much lower. B resolves this contentionand acknowledges only one station in the CTS (if it was able to recover the RTSat all). No transmission is allowed without an appropriate CTS. This is one ofthe medium access schemes that is optionally used in the standard IEEE 802.11.

MACA also help to solve the 'exposed terminal' problem

- With MACA, B has to transmit an RTS first containing the name of the receiver (A) and the sender (B).
- C does not react to this message as it is not the receiver, but A acknowledges using a CTS which identifiesB as the sender and A as the receiver of the following data transmission.
- C does not receive this CTS and concludes that A is outside the detection range.
- C can start its transmission assuming it will not cause a collision at A.
- The problem with exposed terminals is solved without fixed access patterns or a base station.

802.11MAC Frame Types

- The IEEE 802.11 WLAN specification defines various frame types than Ethernet for wireless communications, as well as managing and controlling wireless connections.
- The types of frames in the IEEE 802.11 specification are **management, control, and data frames.**

Management Frame

- Used for station association and disassociation with the AP.
- Used for timing and synchronization.
- Used for authentication and de-authentication.

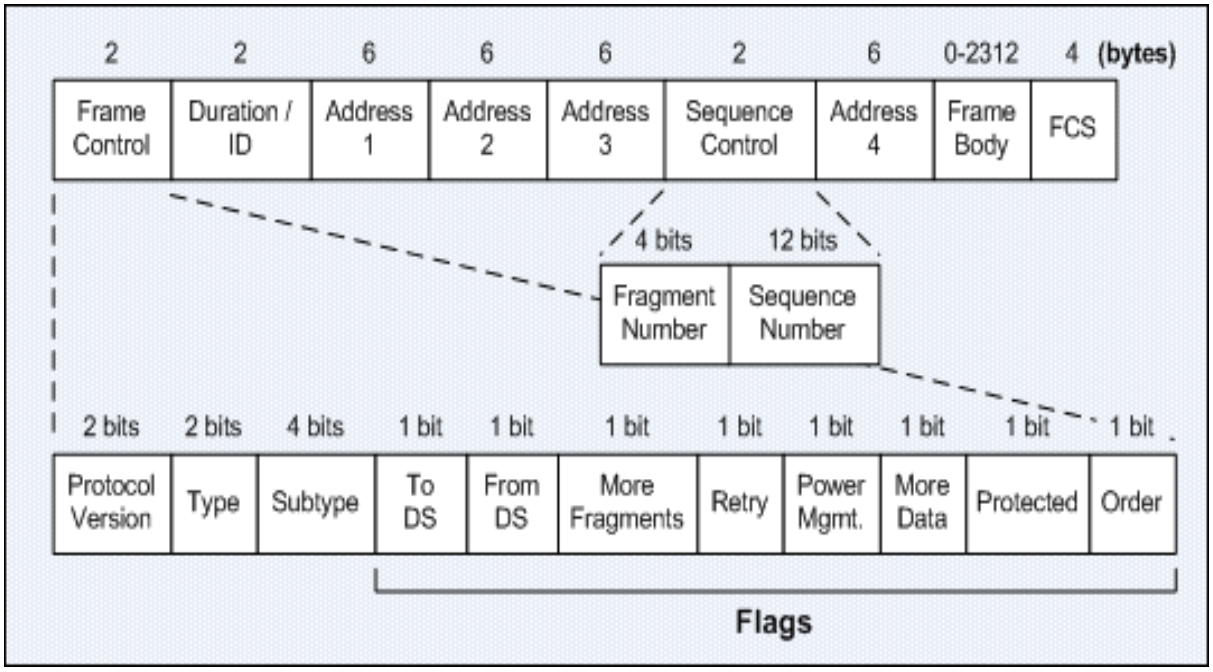
Control Frame

- Used for handshaking during contention period (CP).
- Used for the positive acknowledgement during the CP.
- Used for contention free period (CFP).

Data Frame

- Used for the transmission of data during the CP and CFP.
- Can be combined with polling and acknowledgements during the CFP.

802.11 MAC Frame



- **Protocol Version:** Indicates the version of the 802.11 protocol. A receiving station uses this value to determine whether it supports the version of the protocol of the received frame.
- **Type and Subtype:** Determine the function of the frame – management, control, or data. The type and subtype fields for each frame type determine the specific function to perform.

- **To DS** and **From DS:** Indicates whether the frame is destined to or exiting from the distributed system (DS). All frames of wireless stations that are associated with an access point (infrastructure mode) will have one of the DS bits set. The interpretation of the Address fields depends on the setting of these bits.
- **More Fragments:** Indicates whether there are more subsequent fragments for a particular management or data frame are to follow. Control frames are not fragmented, hence this bit is always set to 0 for control frames.
- **Retry:** Indicates whether the management or data frame is being retransmitted.
- **Power Management:** Indicates whether the sending wireless station is in active or power-saving mode.
- **More Data:** Used to inform a wireless station which is in power-saving mode that the access point has more frames to send to it. Also used by an access points to indicate that additional broadcast or multicast frames are to follow. This bit is only being used in management and data frames; hence this bit is always set to 0 for control frames.
- **Protected:** Indicates whether encryption and authentication are used for the frame. Control frames may not be encrypted; hence this bit is always set to 0 for control frames.
- **Order:** Indicates that all received data frames must be processed in sequence.
- The **Duration/ID** field is used in all control frames to indicate the remaining duration needed to receive the next frame transmission.
- An 802.11 frame may contain up to 4 Address fields.
- **BSS Identifier (BSSID):** Used to uniquely identify each BSS (WLAN). When the frame is from a wireless station in an infrastructure BSS, the BSSID is the MAC address of the access point; when the frame is from a wireless station in an IBSS (ad-hoc) mode, the BSSID is a locally administered MAC address generated with a 46-bit random number, and is generated by the wireless station that initiated the IBSS.
- **Source Address (SA):** Indicates the 48-bit MAC address of the source station that created and transmitted the frame (source of the transmission). Only 1 station can be the source of a frame.
- **Destination Address (DA):** Indicates the 48-bit MAC address of the destination station to receive the frame (recipient).
- **Transmitter Address (TA):** Indicates the 48-bit MAC address of the wireless interface that transmitted the frame onto the wireless medium. The TA is only being used in **wireless bridging**.
- **Receiver Address (RA):** Indicates the 48-bit MAC address of the (immediate) wireless station which should receive and process the frame. If it is a wireless station, the RA is the DA. For frames destined to a node on an Ethernet network connected to an access point, the RA is the wireless interface of the access point, and the DA may be a node attached to the Ethernet.
- The Sequence Control field contains the following 2 subfields:
  Fragment Number: Indicates the number of each frame of a fragmented upper-layer packet. The 1st fragment will have a fragment number of 0, and each subsequent

fragment of a fragmented packet increments the fragment number incremented by one.

Sequence Number: Indicates the sequence number of each frame. It begins at 0 and incremented by 1 until 4095 and rollovers to zero and begins again (**modulo-4096**). All fragments of a fragmented packet as well as retransmitted frames will have the same sequence number.

- **Data Field**: Holds the actual data to be transmitted.
- **FCS**: CRC code to determine the occurrence of errors in the frame while transmitting the data.

4.9 *Robustness features provided in 802.11 MAC*

The 802.11 MAC layer provides the following robustness features:

- **CRC checksum:** Each packet has a CRC checksum calculated and attached to ensure that the data was not corrupted in transit.
- **Packet fragmentation:** Allows large packets to be broken into smaller units when sent over the air. This technique reduces the need for retransmission in many cases and thus improves overall wireless network performance.
- **Roaming Provisions:** 802.11 allow a client to roam among multiple APs that can be operating on the same or separate channels.
- **Support for Time-Bounded Data:** Time-bounded data such as voice and video is supported in the 802.11 MAC specifications through the Point Coordination Function (PCF). In PCF mode a single access point controls access to the media. During the periods when the system is in PCF mode, the access point will poll each station for data, and after a given time move on to the next station. No station is allowed to transmit unless it is polled, and stations receive data from the access point only when they are polled. Since PCF gives every station a turn to transmit in a predetermined fashion, a maximum latency is guaranteed.
- **Synchronization:** The 802.11 MAC layer helps in finding a wireless LAN and synchronizes internal clocks.
- **Power Management:** To extend the battery life of portable devices, 802.11 supports two power- utilization modes, called ***Continuous Aware Mode and Power Save Polling Mode***. In the former, the radio is always on and drawing power, whereas in the later, the radio is "dozing" with the AP queueing any data for it.

4.10 Wireless Security Offered by IEEE 802.11

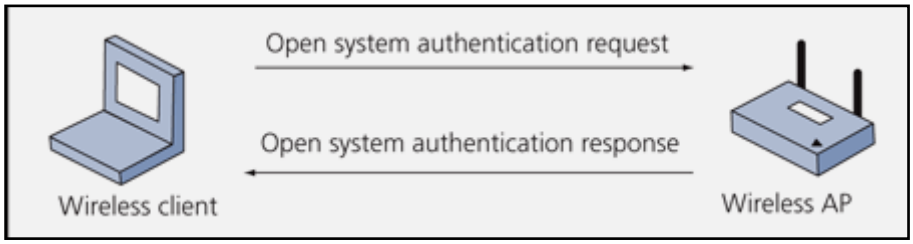
IEEE 802.11 provides for security via two methods: authentication and encryption.

4.10.1 Authentication

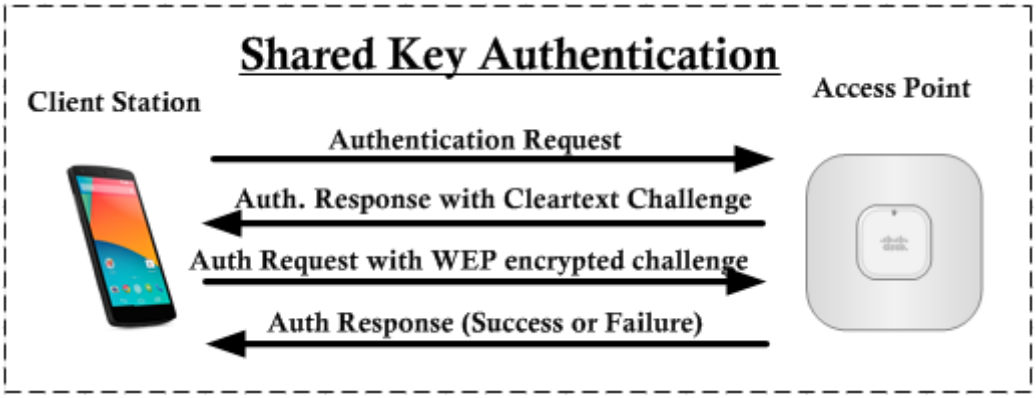
Authentication is the means by which one station is verified to have authorization to communicate with a second station in a given coverage area. In the infrastructure mode, authentication is established between an AP and each station.

802.11 provides two methods of authentication: open system or shared key.

- An **open system** allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption.



- **Shared key authentication**, on the other hand, requires **Wired Equivalent Privacy (**WEP) be enabled, and identical WEP keys on the client and AP (for more information on WEP keys, see below). The initiating endpoint requests a shared key authentication, which returns unencrypted challenge text (128 bytes of randomly generated text) from the other endpoint. The initiator encrypts the text and returns the data.



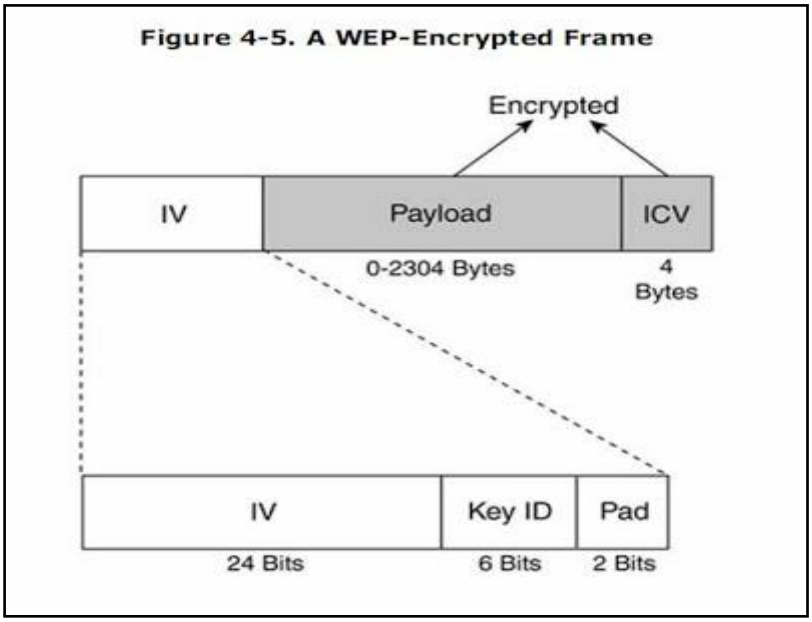
4.10.2 Encryption

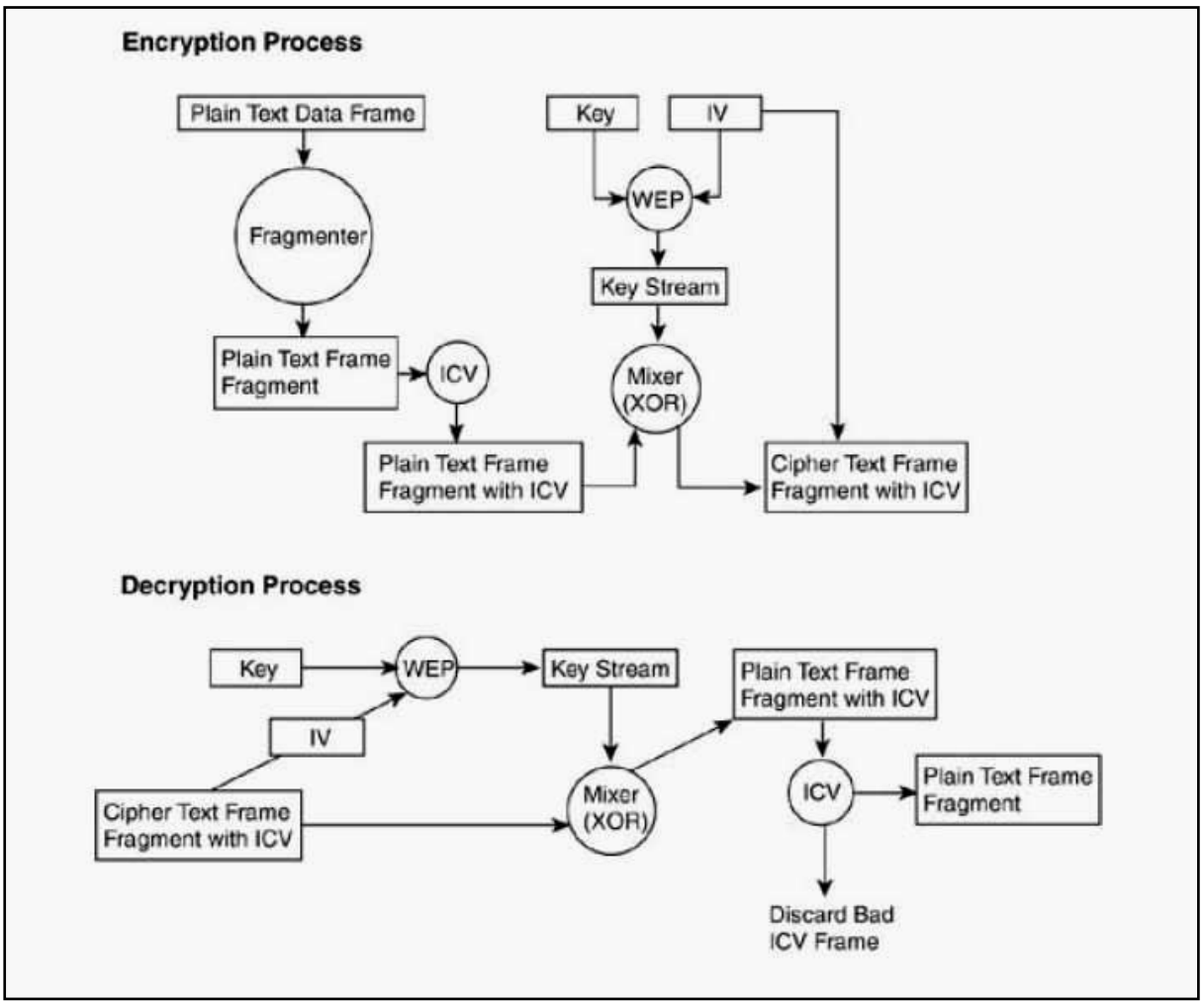
The 802.11 specification provides data privacy with the WEP algorithm. WEP is based on theRC4 symmetric stream cipher. The symmetric nature of RC4 requires that matching WEP keys, either 40 or 104 bits in length, must be statically configured on client devices and access points (APs). WEP was chosen primarily because of its low computational overhead. Although 802.11-enabled PCs are common today, this situation was not the case back in 1997. The majority of WLAN devices were application-specific devices (ASDs). Examples of ASDs include barcode scanners, tablet PCs, and 802.11-based phones.

To avoid the Electronic Code Book (ECB) mode of encryption, WEP uses a 24-bit IV, which is concatenated to the keybefore being processed by the RC4 cipher. Figure below shows a WEP-encrypted frame, including the IV.

The IV must change on a per-frame basis to avoid IV collisions. IV collisions occur when the same IV and WEP key are used, resulting in the same key stream being used to encrypt aframe. This collision gives attackers a better opportunity to guess the plaintext data byseeing similarities in the ciphertext. The point of using an IV is to prevent this scenario, so it is important to change the IV often. Most vendors offer per-frame IVs on

their WLAN devices.The 802.11 specification requires that matching WEP keys bestatically configured on bothclient and infrastructure devices.





In addition to data encryption, the 802.11 specification provides for a 32-bit value that functions as an integrity check for the frame. This check tells the receiver that the frame

has arrived without being corrupted during transmission. It augments the Layer 1 and Layer 2 frame check sequences (FCSs), which are designed to check for transmission-related errors.

The ICV is calculated against all fields in the frame using a cyclic redundancy check (CRC)-32 polynomial function. The sender calculates the values and places the result in the ICV field. The ICV is included in the WEP-encrypted portion of the frame, so it is not plainly visible to eavesdroppers. The frame receiver decrypts the frame, calculates an ICV value, and compares what it calculates against what has arrived in the ICV field. If the values match, the frame is considered to be genuine and un-tampered with. If they don't match, the frame is discarded.

4.11 Latest Developments in IEEE 802.11 Standards

- **802.11a:**
  - Operates in the 5.15GHz to 5.35GHz radio spectrum.
  - Speed: Up to 54Mbps (actual throughput is closer to 22Mbps)
  - Range: 50 feet
  - Less prone to interference.
  - More expensive.
  - Because 802.11b and 802.11a use different radio technologies and portions of the spectrum, they are incompatible with one another.

- **802.11b:**
  - Operates in the 2.4GHz radio spectrum.
  - Speed: Up to 11Mbps
  - Range: 100 feet
  - Prone to interference (it shares airspace with cell phones, Bluetooth, security radios, and other devices).
  - Least expensive wireless LAN specification.
  - The Wireless Ethernet Compatibility Alliance (WECA) has done its part by certifying hundreds of products to make sure they work together.

- **802.11g:**
  - Operates in the 2.4GHz radio spectrum.
  - Speed: Up to 54Mbps
  - Range: 100 feet
  - Prone to interference (it shares airspace with cell phones, Bluetooth, security radios, and other devices).

- **802.11n (Draft):**
  - Operates in the 2.4 or 5GHz radio spectrum
  - Speed: Up to 700Mbs
  - Range: 50 feet

- Because 802.11b and 802.11g use the same radio technologies and portions of the spectrum, they are compatible with one another. But because the 802.11n standard has yet to be ratified by WECA, it may not be completely compatible with 802.11b and 802.11g.

- **IEEE 802.11ad**
  The IEEE 802.11ad also referred to as WiGig is really a relatively new standard published in December 2012. It specification adds a "fast session transfer" feature. To provide for optimal performance and range criteria, the IEEE 802.11ad provides the capability to move in between the bands ensuring that computing devices are usually "best connected."

Parameter	Details
Operating frequency range	60 GHz ISM band
Maximum data rate	7 Gbps
Typical distances	1 - 10 m
Antenna technology	Uses beamforming
Modulation formats	Various: single carrier and OFDM

- **IEEE 802.11ae**
  The IEEE 802.11ae aims to introduce a mechanism for prioritization of management frames. A protocol to communicate management frame prioritization policy is specified in this standard.

- **IEEE 802.11ac**
  Among the important standards currently under development is IEEE 802.11ac. This standard is anticipated to be published by the end of 2014. It's expected to supply a multi-station WLAN throughput of around 7 Gbps and an individual link throughput of at the least 500 Mbps. That is accomplished by extending the air interface concepts which are embraced by 802.11n like wider RF bandwidth (up to 160 MHz), more MIMO spatial streams (up to 8), multi-user MIMO, and high-density modulation.

Parameter	Details
Frequency band	5.8 GHz ISM (unlicensed) band
Max data rate	6.93 Gbps
Transmission bandwidth	20, 40, & 80 MHz 160 & 80 + 80 MHz optional
Modulation formats	BPSK, QPSK, 16-QAM, 64-QAM 256-QAM optional
FEC coding	Convolutional or LPDC (optional) with coding rates of 1/2, 2/3, 3/4, or 5/6
MIMO	Both single and multi-user MIMO with up to 8 spatial streams
Beam-forming	Optional

- **IEEE 802.11af**

The IEEE 802.11af, also known as White-fi is meant to operate in the TV White Spaces, that will be the spectrum already allocated to the TV broadcasters however, not used at a certain location and time frame. It uses cognitive radio technology to spot white spaces it could use. However, this cognitive technology will soon be predicated on an officialgeolocation database. This database can provide information on which frequency, at what time and under what conditions networks may operate.

Parameter	Details
Operating frequency range	470-510 MHz
Channel bandwidth	6 MHz
Transmission Power	20 dBm
Modulation format	BPSK
Antenna Gain	0dBi

- **IEEE 802.11ah**

The IEEE 802.11ah is directed at developing an international WLAN network which will allow user to gain access to sub carrier frequencies below 1GHz in the ISM band. One of the goals of this standard is to ensure that the transmission, ranges up to 1 km. It will even enable devices on the basis of the IEEE 802.11 standards to access short burst data transmissions like meter data. Additionally it can provide improve coverage range that will allow new applications such as, for example wide area based sensor networks, sensor backhaul systems and potential Wi-Fi off-loading functions to emerge. This standard is under development and is predicted to be finalized by 2016.

- **IEEE 802.11ai**

The IEEE 802.11ai is a forthcoming standard predicted to be finalized by 2015. It'll add a fast initial link setup (FILS) that might enable an STA to reach a protected link setup that will be significantly less than 100 ms.An effective link setup process will then permit the STA to send IP traffic with a valid IP address through the AP.

- **IEEE 802.11mc**

The IEEE 802.11mc resembles the IEEE 802.11m and is also scheduled to appoint an operating group with the job of maintenance of the standard around 2015.

- **IEEE 802.11aj**

The IEEE 802.11aj is intended provide modifications to the IEEE 802.11ad Physical (PHY) layer and the Medium Access Control (MAC) layer for operation in the Chinese Milli-Meter Wave (CMMW) frequency bands like the 59-64 GHz frequency band. The amendment can also be meant to maintain backward compatibility with 802.11ad when it operates in the 59-64 GHz frequency band. The amendment shall

also define modifications to the PHY and MAC layers allowing the operation in the Chinese 45 GHz frequency band. This standard is scheduled to be finalized by the end of 2016.

- **IEEE 802.11aq**

  The WLAN is fast evolving and is no more one, where stations are merely looking for just usage of internet service. This creates opportunities to supply new services, because the IEEE 802.11 standard must be enhanced to advertise and describe these new services.

  The IEEE 802.11aq can provide mechanisms that will assist in pre-association discovery of services by addressing the methods to advertise their existence and enable delivery of information that describes them. These records about services will be made available ahead of association by stations operating on IEEE 802.11 wireless networks. This standard is scheduled to be published by 2015.

IEEE 802.11	Release Date	Frequency (GHz)	Max Data Rate (Mbps)	Range (m)		Status and Comments
				Indoor	Outdoor	
-1997	1997	2.4	2	20	100	Obsolete
a	1999	5/3.7	54	35/-	120/5k	Legacy systems
b	1999	2.4	11	35	140	Legacy systems
g	2003	2.4	54	38	140	Legacy systems
n	2009	2.4/5	600	70	250	Current systems
ac	2013	2.4/5	450/7,000	35		Next generation – just starting to be deployed.
ad	2012	60	7,000	10		Known as WiGig. Short-reach high data rate data transfers.
af	Est. 2016	0.470-0.710	568		6,000	Being called White-Fi because it uses unused TV spectrum.
ah		0.9	40			In development.
aj		45/60	7,000	10		Modification of 802.11ad for 45GHz band for use in China
ax	Est. 2019	2.4/5	450/10,000	35		Revision to 802.11ac to increase efficiency.

CHAPTER 5

WIRELESS PERSONAL AREA NETWORKS (WPAN)

5. 1 Introduction

- A **WPAN** is a personal, short distance area wireless network for interconnecting devices centered around an individual's workspace.
- WPAN address wireless networking of mobile computing devices like PCs, PDAs, Pagers, Cell phones and consumer electronics.
- Also called "short wireless distance networks".
- WPAN typically extends to 33 ft (10 m) or less.
- WPAN technology is mainly used as replacement for cables; thus reduces the overall cost associated with cabled network setup, maintenance and planning.
- Provides high-speed data transfer that ranges from 1 and 3 Mbps.

5.2 Technologies used for implementing WPAN

1. **Insteon**: Refers to home automation technology using which devices such as thermostats, switches and so on can interoperate using RF communications or power lines or both.
2. **Infrared**: Refers to an invisible electromagnetic radiation having long wavelength as compared to the visible light. Infrared radiation is usually used in industries and in scientific and medical applications.
3. **Wireless Universal Serial Bus (WUSB):** Refers to a low-range wireless radio communication protocol. WUSB is mainly used in digital cameras, printers, USB flash drives, and so on.
4. **Z-wave**: Refers to wireless communications protocol used specially in remote control applications.
5. **Body Area Network**: Refers to wireless network of devices that can be worn. These devices are embedded within the body or can be carried in clothes pockets or in hand bags.

5.3 WPAN Architecture

- The WPAN architecture is defined into a number of structural blocks called layers.
- Each layer implements a subset of the WPAN standard and offers services to its upper layers and gets services from its lower layers.

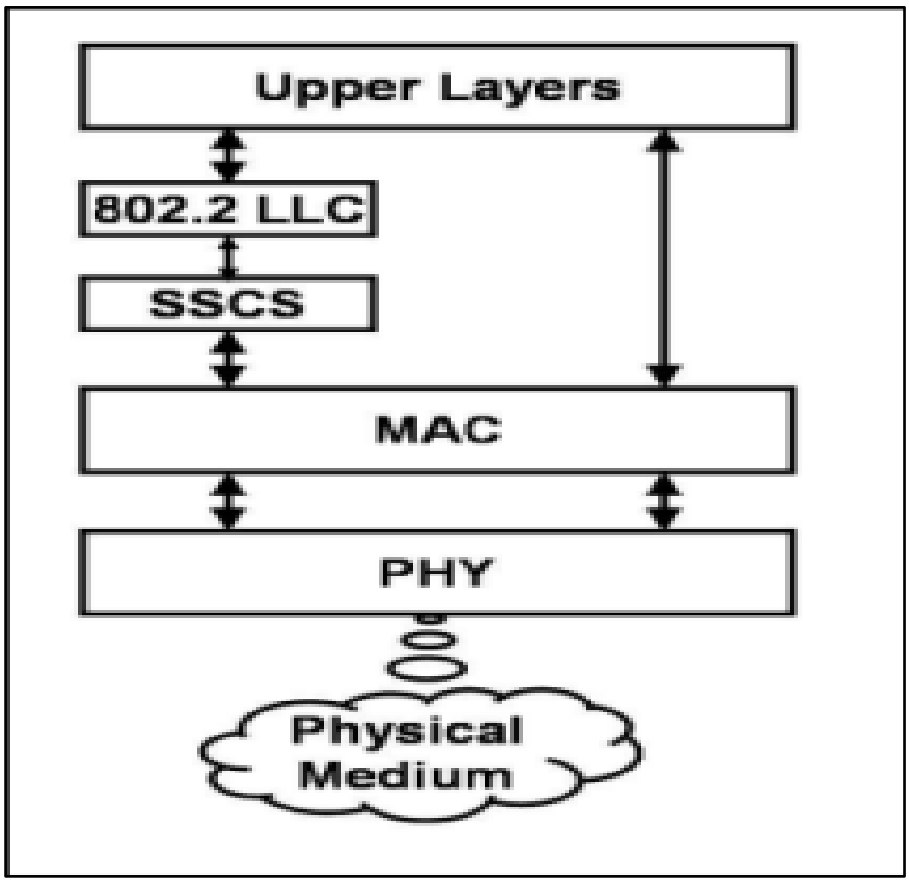
1. Upper Layer

- The upper layer consists of two layers which are as follows:
- A network layer which gives network configuration, manipulation and routing. It is also responsible for all TCP/IP and FTP protocols so that the message is protected during transmission.
- An application layer also called as service layer which provides services like checking the protocol, and data syntax, authentication of message, sender and receiver.

2. 802.2 LLC

- LLC stands for logical link control.
- It is the interface between the MAC sub layer and the network layer.

- Facilitates multiplexing mechanism, flow control and Automatic Repeat Request (ARQ) error management mechanism.



3. Service Specific Convergence Sublayer (SSCS)

- SSCS interfaces the MAC sublayer to the logical link control sublayer and other upper layers such as the networking layer, application layer, etc.

4. MAC Layer

- The MAC data service enables the transmission and reception of MAC Protocol Data Units (MPDU) across the PHY data service.
- The features of MAC sub layer are
  - beacon management,
  - channel access control through the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) scheme,
  - collision-free time slots management,
  - frame validation
  - acknowledged frame delivery and
  - Node association and disassociation

5. PHY Layer

- The PHY data service enables the transmission and reception of PHY Protocol Data Units (PPDU) across the physical radio channel.

- The main tasks of the PHY layer are
  - the activation and deactivation of the radio transceiver,
  - channel Energy Detection (ED),
  - Link Quality Indication (LQI),
  - Clear Channel Assessment (CCA), and
  - transmitting as well as receiving data packets over the physical medium.
  - The ED measurement estimates the received signal power.

5.4 Bluetooth

Bluetooth technology is a short-range wireless communications technology to:

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

5.4.1 Bluetooth Specifications

- Bluetooth-Wireless technology providing link between mobile and electronic devices.
- It operates on 2.45 GHz radio signals using frequency hopping spread spectrum.
- Technology of Bluetooth concentrates on short range of communication
- Standard: IEEE 802.15
- ISM Band Frequency: 2.4 GHz
- Range: 10 – 100 meters
- Channel Bandwidth: 1 Mbps
- Maximum Asymmetric Data Transfer Rate: 721 Kbps

5.4.2 Bluetooth Applications

Nowadays, Bluetooth technology is used for severalcomputer and non computer application:

1. It is used for providing communication between peripheral devices like wireless mouse orkeyboard with the computer.
2. It is used by modern healthcare devices to send signals to monitors.
3. It is used by modern communicating devices like mobile phone, PDAs, palmtops etc to transfer data rapidly.
4. It is used for dial up networking. Thus, allowing a notebook computer to call via a mobile phone.
5. It is used for cordless telephoning to connect a handset and its local base station.
6. It also allows hands-free voice comml1nication with headset.
7. It also enables a mobile computer to connect to a fixed LAN.
8. It can also be used for file transfer operations from one mobile phone to another.
9. Bluetooth uses omni-directional radio waves that can through walls or other non-metal barriers.

5.4.3 Bluetooth Architecture

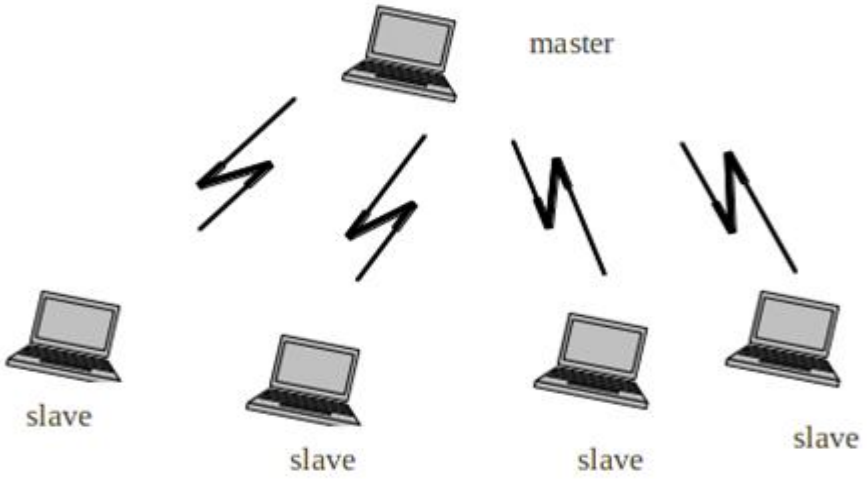
Bluetooth architecture defines two types of networks:

1. Piconet
2. Scatternet

1. Piconet

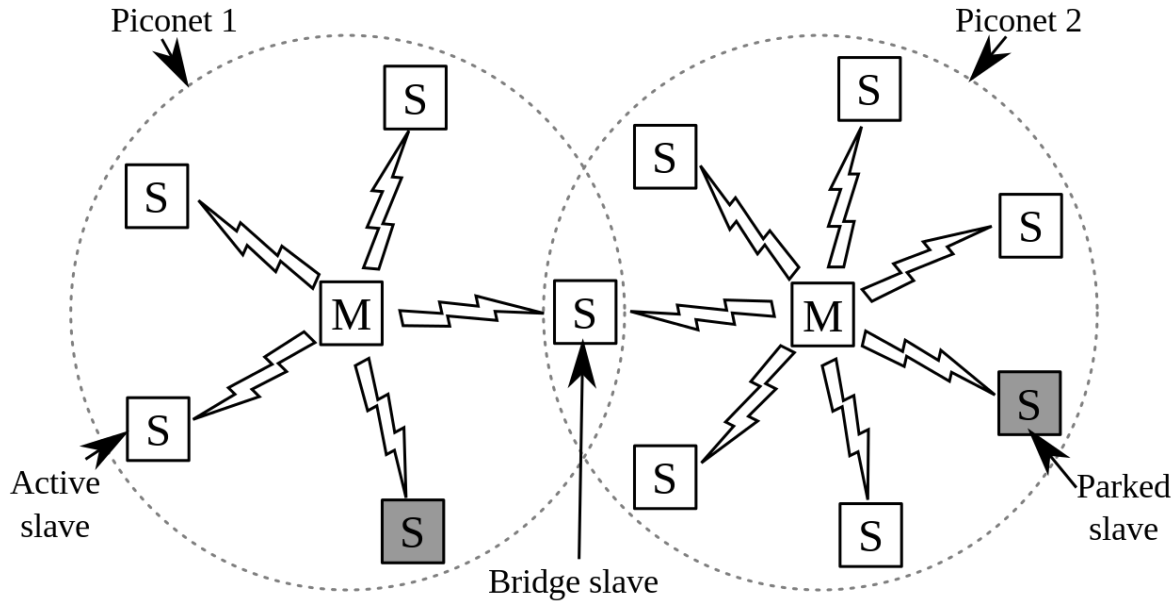
- Piconet is a Bluetooth network that consists of one primary (master) node and seven active secondary (slave) nodes.

- Thus, piconet can have upto eight active nodes (1 master and 7 slaves) or stations within the distance of 10 meters.
- There can be only one primary or master station in each piconet.
- The communication between the primary and the secondary can be one-to-one or one-to-many.
- All communication is between master and a slave. Salve-slave communication is not possible.
- In addition to seven active slave station, a piconet can have upto 255 parked nodes. These parked nodes are secondary or slave stations and cannot take part in communication until it is moved from parked state to active state.



2. Scatternet

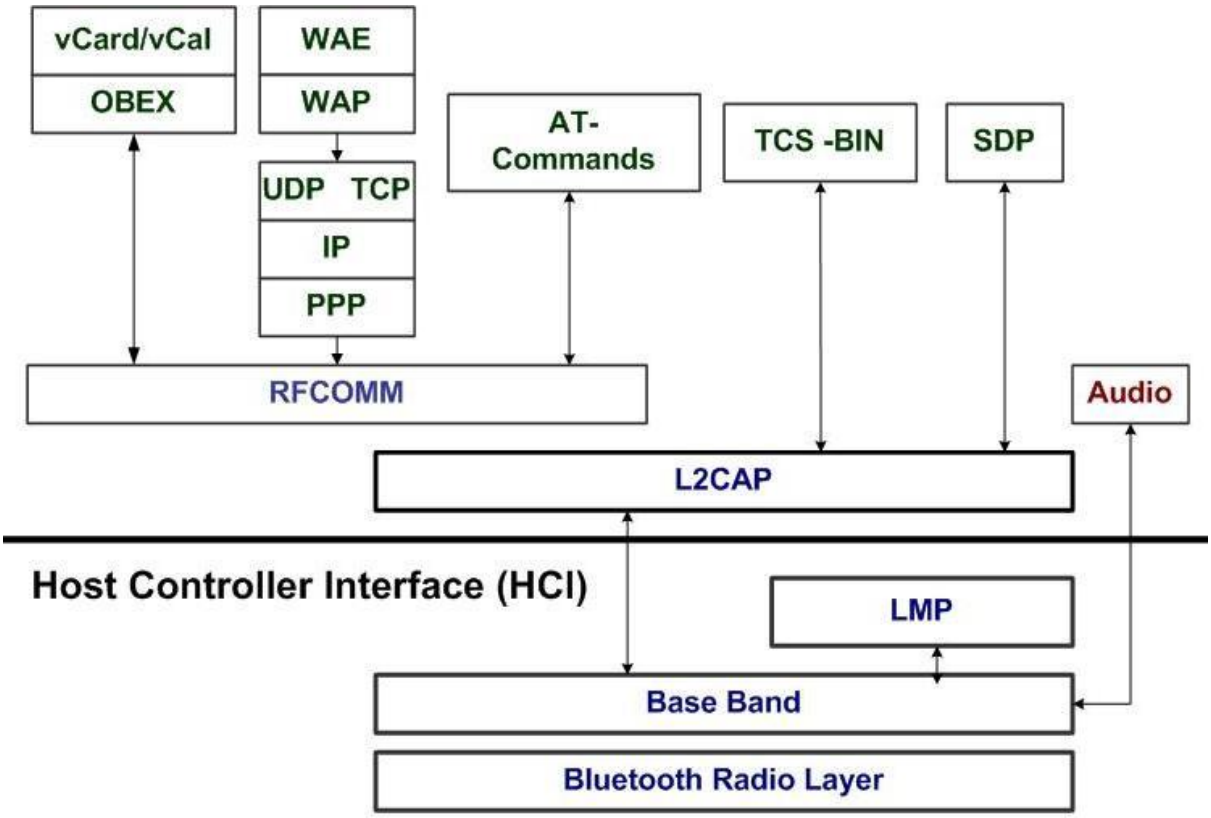
- Scatternet is formed by combining various piconets.
- A slave in one piconet can act as a master or primary in other piconet.
- Such a station or node can receive messages from the master in the first piconet and deliver the message to its slaves in other piconet where it is acting as master. This node is also called bridge slave.
- Thus a station can be a member of two piconets.
- A station cannot be a master in two piconets.



5.4.4 Bluetooth Protocol Stack

The protocol architecture of the bluetooth consists of following in a**bluetooth protocol stack**:

- Core protocols consisting 5 layer protocols stack viz. radio,baseband,link manager protocol,logical link control and adaptation protocol, service discovery protocol.
- Cable replacement protocol,RFCOMM.
- Telephony Control Protocols.
- Adopted protocols viz. PPP,TCP/UDP/IP,OBEX and WAE/WAP.



The Bluetooth Protocol Stack

Bluetooth Core Layer Protocols

1. **Radio**: This protocol specification defines air interface, frequency bands, frequency hopping specifications, modulation technique used and transmit power classes.

2. **Baseband**: Addressing scheme, packet frame format, timing and power control algorithms required for establishing connection between bluetooth devices within piconetare defined in this part of protocol specification.

3. **Link Manager protocol**: It is responsible to establish link between bluetooth devices and to maintain the link between them. This protocol also includes authentication and encryption specifications. Negotiation of packet sizes between devices can be taken care by this.

4. **Logical link control and adaptation protocol**: This L2CAP protocol adapts upper layer frame to baseband layer frame format and vice versa. L2CAP take care of both connection-oriented and connectionless services.

5. **Service discovery protocol**: Service related queries including device information can be taken care at this protocol so that connection can be established between bluetooth devices.

Cable replacement protocol

1. **RFCOMM**
   The RFCOMM protocol is a serial port emulation protocol. The protocol covers applications that make use of the serial ports of the unit. RFCOMM emulates RS-232 control and data signals over the Bluetooth baseband. It provides transport capabilities for upper level services, e.g. OBEX that use a serial line as the transport mechanism.

Telephony control protocol

1. **Telephony Control – Binary**
   The Telephony Control protocol – Binary, TCS Binary or TCS BIN, is a bit-oriented protocol, which defines the call control signalling for the establishment of speech and data calls between Bluetooth units. The protocol defines the signalling for establishment and release of calls between Bluetooth units. As well as signalling to ease the handling of groups of Bluetooth units. Furthermore, TCS Binary provides functionality to exchange signalling information unrelated to ongoing calls. Establishment of a voice or data call in a point-to-point configuration as well as in a point-to-multipoint configuration is covered in this protocol (note, after establishment, the transmission is from point to point). The TCS Binary is based on the ITU-T Recommendation.

2. **Telephony Control – AT Commands**
   A number of Attention Sequence (AT) -commands are supported for transmitting control signals for telephony control. These use the serial port emulation, RFCOMM, for transmission.

Adopted protocols

This section describes a number of protocols that are defined to be adopted to the Bluetooth protocol stack.

1. **PPP**
   The IETF Point-to-Point Protocol (PPP) in the Bluetooth technology is designed to run over RFCOMM to accomplish point-to-point connections. PPP is a packet-oriented protocol and must therefore use its serial mechanisms to convert the packet data stream into a serial data streams.

2. **TCP/UDP/IP**
   The TCP/UDP/IP standards are defined to operate in Bluetooth units allowing them to communicate with other units connected, for instance, to the Internet. Hence, the Bluetooth unit can act as a bridge to the Internet. The TCP/IP/PPP protocol configuration is used for all Internet Bridge usage scenarios in Bluetooth 1.0 and for OBEX in future versions. The UDP/IP/PPP configuration is available as transport for WAP.

3. **OBEX Protocol**
   Object Exchange Protocol (OBEX), is an optional application layer protocol designed to enable units supporting infrared communication to exchange a wide variety of data and commands in a resource-sensitive standardized fashion. OBEX uses a client-server model and is independent of the transport mechanism and transport API. The OBEX protocol also defines a folder-listing object, which is used to browse the contents of folders on remote device. RFCOMM is used as the main transport layer for OBEX.

4. **Content formats**
   The formats for transmitting vCard and vCalendar information are also defined in the Bluetooth specification. The formats do not define transport mechanisms but the format in which electronic business cards and personal calendar entries and scheduling information are transported. vCard and vCalendar is transferred by OBEX.

5. **Wireless Application Protocol, WAP**
   The Wireless Application Protocol (WAP) is a wireless protocol specification that works across a variety of wide-area wireless network technologies bringing the Internet to mobile devices. Bluetooth can be used like other wireless networks with regard to WAP, it can be used to provide a bearer for transporting data between the WAP Client and its adjacent WAP Server. Furthermore, Bluetooth's ad hoc networking capability gives a WAP client unique possibilities regarding mobility compared with other WAP bearers.
   The traditional form of WAP communications involves a client device that communicates with a Server/Proxy device using the WAP protocols. Bluetooth is expected to provide a bearer service as specified by the WAP architecture. The WAP technology supports server push. If this is used over Bluetooth, it opens new possibilities for distributing information to handheld devices on location basis. For example, shops can push special price offers to a WAP client when it comes within Bluetooth range.

5.4.5 Advantages and Disadvantages of Bluetooth Technology

The advantages and disadvantages of Bluetooth technology are well-known to anyone who extensively uses Bluetooth for transferring data or sharing information. IEEE

standards govern its networks and have standardized it for use with a vast range of compatible devices.

The Advantages of Bluetooth

- Bluetooth does not require a clear line of sight between the synced devices. This means that the devices need not be facing each other, and it is also possible to carry out transfers when both the devices are in separate rooms.
- The fact that this technology requires no cables and wires is something that has made it so popular. With so many devices engulfing our lives today, the need for clutter-free technology is becoming more intense.
- The maximum range that it offers is 100 meters, but this range is not the same for all similar connections. It depends on the nature of the devices and the version that they operate upon.
- The processing power and battery power that it requires in order to operate is very low. This makes it an ideal tool for so many electronic devices, as the technology can be implemented pretty much anywhere.
- One major advantage is its simplicity of use. Anyone can figure out how to set up a connection and sync two devices with ease. Moreover, the technology is completely free to use and requires no charges to be paid to any service provider.
- The chances of other wireless networks interfering with yours are very low. This is because of the low-powered wireless signals that the technology adopts, and also because of something known as frequency hopping.

The Disadvantages of Bluetooth

- Though the transfer speeds are impressive at around 25 Mbps, certain other technologies like Wi-Fi Direct can offer speeds up to 250 Mbps. This is an area that can be improved upon in the near future.
- Even though the security is good, it is even better on Wi-Fi Direct. This can be accounted to the (comparatively) larger range of Bluetooth and also to the lack of a line of sight. Someone who knows how to hack such networks can do so eventually.
- The battery usage during a single transfer is negligible, but there are some people who leave the device switched on in their devices. This inevitably eats into the battery of these devices, and lowers the battery life considerably.

5.5 HR-WPAN (High Rate- WPAN)

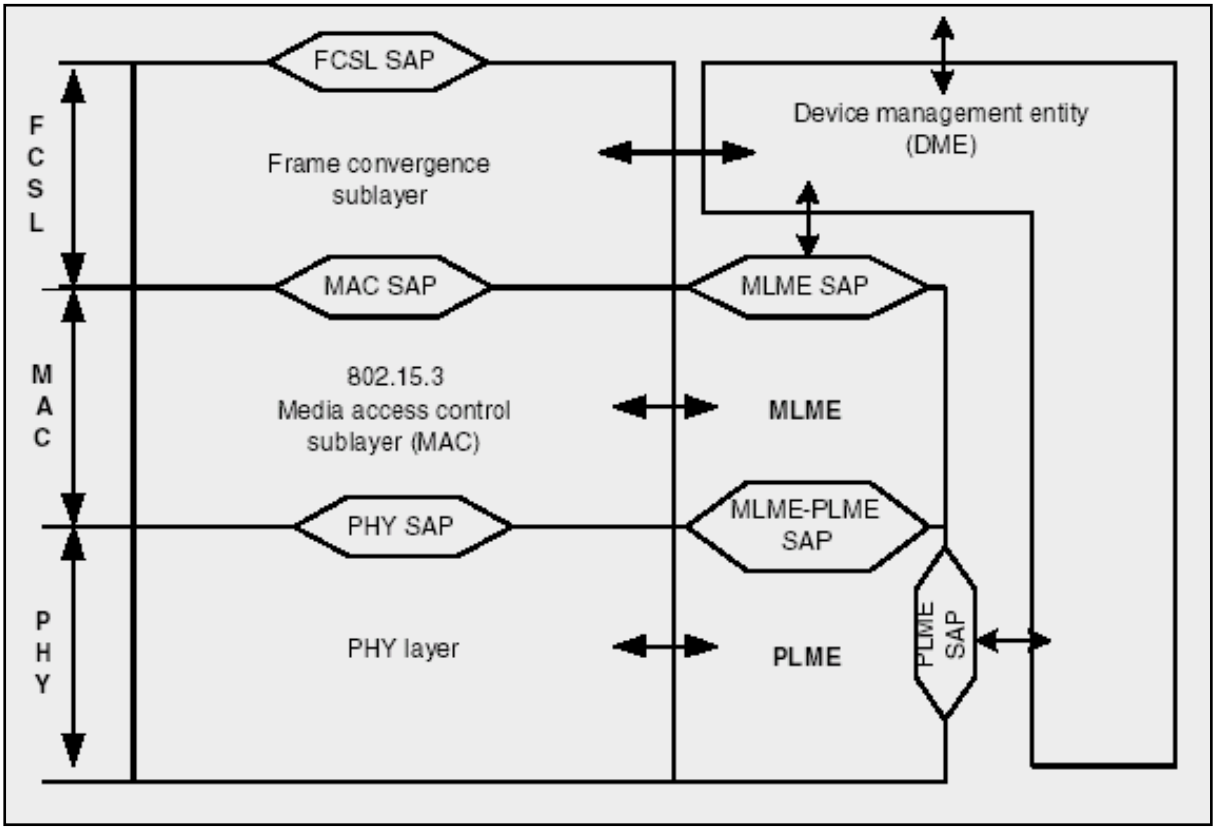
IEEE 802.15.3 standard defines the specifications for HR WPANs supporting speeds of 11, 22, 33, and up to 55 Mbps in the 2.4 GHz ISM band

5.5.1 Application characteristics of HR-WPAN

- Require high throughput
- Transceiver should be low-power
- Cost should be low

- Require quality-of-service (QOS) capabilities
- Connections should be simple and automatic
- Devices should be able to connect to multiple other devices
- Security features should be included

5.5.2 HR WPAN Architecture



- This model defines the architecture into two parts; namely: node structural blocks part and node management part.
- The node structural blocks part is mainly composed of three layers; Frame Convergence sublayer (FCSL), MAC sublayer, and Physical (PHY) layer.
- The HR - WPANs standard is defined only for the MAC and PHY layers where each layer implements a subset of the standard and offers services to its upper layers and gets services from its lower layers.
- The FCSL interfaces the MAC sublayer to the upper layers such as the networking layer, application layer, etc.
- The management part of a HR - WPAN node consists of the Device Management Entity (DME).
- The DME facilitates the functionalities of the MAC and PHY layers and other upper layers.
- Gathering layer-dependent status from the management entities of different layers and setting the values of layer- specific parameters are examples of DME duties.

PHY Layer

- The physical layer contains two functional entities; namely: PHY function and PLME function.
- The PHY layer services are provided to the MAC sublayer through the PHY's SAP.
- The main tasks of the PHY layer are the activation and deactivation of the radio transceiver, Link Quality Indication (LQI), Clear Channel Assessment (CCA), and transmitting as well as receiving data packets over the physical medium.
- The DME is interfaced to the MAC sublayer and the PHY layer through designated Service Access Points (SAPs) of the MAC subLayer Management Entity (MLME) and the PHY Layer Management Entity (PLME) respectively.

MAC Layer

- The MAC sublayer of the HRWPANs is designed to achieve a set of goals. These goals are: Supporting fast connection time, Ad hoc networks topology, QoS support, dynamic node membership, efficient data transfer, and secure data communication.
- The MAC sublayer achieves these goals through two services: the MAC data service and the MAC management service.
- For data communication, the MAC sublayer communicates with the FCSL through the MAC SAP and being serviced by the PHY layer through the PHY SAP. The management entity of the MAC sublayer; MAC sublayer Management Entity (MLME) communicates with the DME through the MLME Service Access Point (SAP) (MLME-SAP).
- The features of the MAC sublayer are beacon management, channel access control through the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) scheme, collision – free channel time allocation for management information and data communication, frame validation, acknowledged frame delivery and node association and disassociation.

5.6 LR-WPAN (ZigBee) – IEEE 802.15.4 Standard

ZigBee technology is a low data rate, low power consumption, low cost, wireless networking protocol targeted towards automation and remote control applications. ZigBee is expected to provide low cost and low power connectivity for equipment that needs battery life as long as several months to several years but does not require data transfer rates as high as those enabled by Bluetooth. In addition, ZigBee can be implemented in mesh networks largerthan is possible with Bluetooth. ZigBee compliant wireless devices are expected to transmit 10-75 meters, depending on the RF environment and the power output consumption required for a given application, and will operate in the unlicensed RF worldwide(2.4GHz global, 915MHz Americas or 868 MHz Europe). The data rate is 250kbps at 2.4GHz, 40kbps at 915MHz and 20kbps at 868MHz.

The main features of this standard are network flexibility, low cost, very low power consumption, and low data rate in an adhoc self-organizing network among inexpensive

fixed, portable and moving devices. It is developed for applications with relaxed throughput requirements which cannot handle the power consumption of heavy protocol stacks.

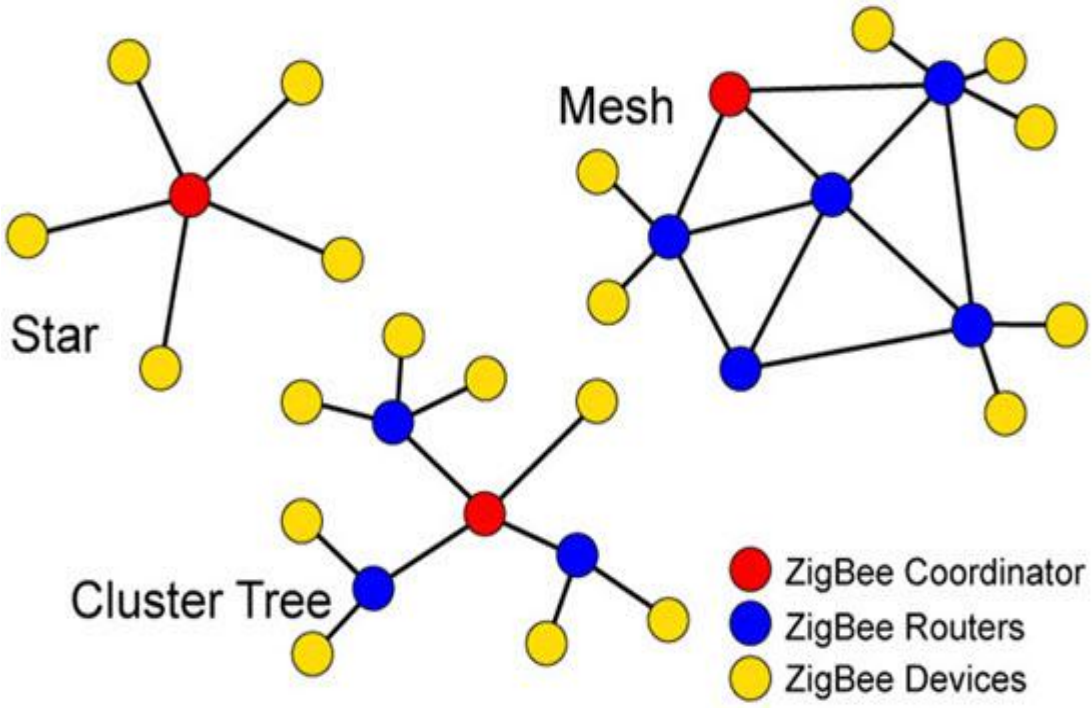
5.6.1 Components of LR-WPAN

- A ZigBee system consists of several components.
- The most basic is the device. A device can be a full-function device (FFD) or reduced-function device (RFD).
- A network shall include at least one FFD, operating as the PAN coordinator.
- The FFD can operate in three modes: a personal area network (PAN) coordinator, a coordinator or a device.
- An RFD is intended for applications that are extremely simple and do not need to send large amounts of data.
- An FFD can talk to RFDs or FFDs while an RFD can only talk to an FFD.

5.6.2 ZigBee Topologies

Zigbee supports several network topologies; however, the most commonly used configurations are star, mesh and cluster-tree topologies. Any topology consists of one or more coordinators.

In a **star topology**, the network consists of one coordinator which is responsible for initiating and managing the devices over the network. All the other devices are called end devices that directly communicate with the coordinator. This is used in industries where all the end point devices are needed to communicate with the central controller, and this topology is simple and easy to deploy.



In **mesh and tree** topologies, the Zigbee network is extended with several routers wherein the coordinator is responsible for staring them. These structures allow any device to communicate with any other adjacent node for providing redundancy to the data. If any node fails, the information is routed automatically to otherdevice by these topologies. As the redundancy is the main factor in industries, hence mesh topology is mostly used.

In a **cluster-tree** network, each cluster consists of a coordinator with leaf nodes, and these coordinators are connected to the parent coordinator that initiates the entire network.

5.6.3Applications of Zigbee Technology

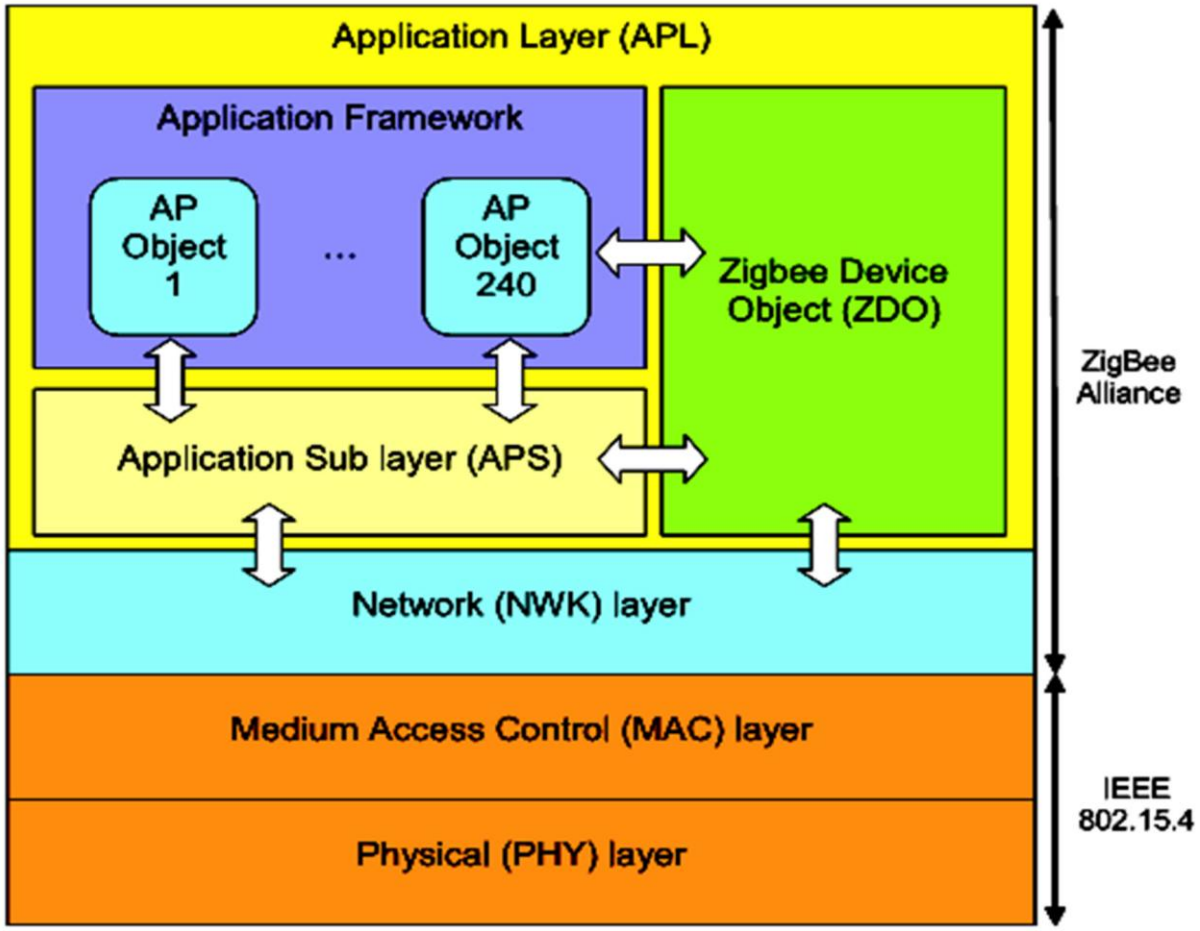
- **Industrial Automation:** In manufacturing and production industries, a communication link continually monitors various parameters and critical equipment. Hence, Zigbee considerably reduces this communication cost as well as optimizes the control process for greater reliability.
- **Home Automation:** Zigbee is perfectly suited for controlling home appliances remotely as a lighting system control, appliance control, heating and cooling system control, safety equipment operations and control unit, surveillance unit, and so on.
- **Smart Metering:** Zigbee remote operations in smart metering include energy consumption response,pricing support, security over power theft, etc.
- **Smart Grid monitoring:** Zigbee operations in this smart grid involve remote temperature monitoring, fault locating, reactive-power management, and so on.

5.6.4 ZigBee Protocol Stack Architecture

The proposed system uses the IEEE 802.15.4 standard as the communication protocol. The IEEE 802.15.4 standard define the characteristics of the physical and MAC layers for Low-Rate Wireless Personal Area Networks (LR-WPAN) including wireless sensor networks (WSNs). IEEE 802.15.4 focuses mainly on low-cost, low-power communication between devices and therefore it presents a low transfer rate with a maximum of 250 kbits/s.

Physical (PHY) Layer

The IEEE 802.15.4 standard defines the physical layer (PHY) in all ZigBee devices. The PHY is responsible for data transmission and reception by using a defined radio channel and specific modulation and spreading technique. The IEEE 802.15.4 standard specifies two physical layers that represent three operational frequency bands. These three bands include: 868 MHz (used in Europe), 915 MHz (used in America), and 2.4 GHz (used worldwide). The 868 and 915 MHz bands are in one PHY using the Binary Phase Shift Keying (BPSK) for modulation, while the 2.4 GHz band is in the second PHY and employs Offset Quadrature Phase Shift Keying (O-QPSK) for modulation. There is a single channel between 868 and 868.8 MHz, 10 channels between 902 and 928 MHz, and 16 Channels between 2.4 and 2.4835 GHz, all using the Direct Sequence Spread Spectrum (DSSS) access mode.



Medium Access Control (MAC) Layer

In addition to the physical layer, the IEEE 802.15.4 standard defines the medium access control layer for all ZigBee devices. The MAC layer protocol serves as the interface between the PHY and the higher layer protocols. The functions of the MAC include synchronization, frame validation, acknowledged frame delivery, association, and disassociation.

The MAC layer defines two types of devices; Full Function Device (FFD) and Reduced Function Device (RFD).

ZigBee Layers

Based on the IEEE 802.15.4, the ZigBee standard defines the higher layer namely; the network layer and the application layer.

The **network layer** is responsible for joining/leaving a network, security, routing, discovering 1-hop neighbors and storing neighbor information. The ZigBee network layer supports three topologies; the star topology where end devices (RFD) are attached to a central point playing the role of PAN coordinator (FFD), the tree topology where end devices can be attached also to FFD nodes with routing capabilities playing the role of ZigBee routers in a hierarchical manner (with parent-child relationship), the mesh topology where ZigBee routers can be fully connected.

As shown in figure, the **application layer** includes the Application Framework, the ZigBee Device Objects (ZDO), and the Application Sub Layer (APS). The Application Framework

can have up to 240 Application Objects (APOs), that is, user defined application modules which are part of a ZigBee application. The ZDO defines the role of the device, initiates and responds to binding requests and establishes a secure relationship between devices. The APS offers an interface to data and security services to the APO sand ZDO.

5.7 Wireless Sensor Networks (WSN)

- A **wireless sensor network (WSN)** (sometimes called a wireless sensor and actor network (WSAN)) are spatially distributed autonomoussensors to *monitor* physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location.

5.7.1 Components of WSN

- Sensor: It is a transducer that converts physical phenomenon e.g. heat, light, motion, vibration, and sound into electrical signals.
- Sensor node: It is the basic unit in sensor network that contains on-board sensors, processor, memory, transceiver, and power supply.
- Sensor network: It consists of a large number of sensor nodes deployed either inside or very close to the sensed phenomenon.

5.7.2 WSN Vs Ad hoc Networks

WSN	Ad Hoc Networks
Mainly used to collect information .	Designed for distributed computing.
Mainly use broadcast communication paradigm.	Based on point-to-point communications.
The number of nodes in sensor networks can be several orders of magnitude higher than that in ad hoc networks.	The number of nodes are less compared to WSN.
Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors.	Each node have global identification (ID).
Sensor nodes are much cheaper than nodes in ad hoc and are usually deployed in thousands.	Nodes are costlier than nodes in WSN.
Sensor nodes are limited in power, computational capacities, and memory.	Nodes in ad hoc networks can be recharged somehow.
Sensor nodes are much more limited in their computation and communication capabilities.	Nodes in ad hoc networks have good computation and communication capabilities.

5.7.3 Characteristics of WSN

- **Dense sensor node deployment**: Sensor nodes are usually densely deployed and can be several orders of magnitude higher than that in a MANET.
- **Battery-powered sensor nodes**: Sensor nodes are usually powered by battery and are deployed in a harsh environment where it is very difficult to change or recharge the batteries.
- **Severe energy, computation, and storage constraints**: Sensors nodes are having highly limited energy, computation, and storage capabilities.
- **Self-configurable**: Sensor nodes are usually randomly deployed and autonomously configure themselves into a communication network.
- **Unreliable sensor nodes:** Since sensor nodes are prone to physical damages or failures due to its deployment in harsh or hostile environment.
- **Data redundancy:** In most sensor network application, sensor nodes are densely deployed in a region of interest and collaborate to accomplish a common sensing task. Thus, the data sensed by multiple sensor nodes typically have a certain level of correlation or redundancy.
- **Application specific**: A sensor network is usually designed and deployed for a specific application. The design requirements of a sensor network change with its application.
- **Many-to-one traffic pattern**: In most sensor network applications, the data sensed by sensor nodes flow from multiple source sensor nodes to a particular sink, exhibiting a many-to-one traffic pattern.
- **Frequent topology change**: Network topology changes frequently due to the node failures, damage, addition, energy depletion, or channel fading.

5.7.4 Wireless Sensor Networks Applications

1. Military Applications

- Monitoring friendly forces, equipment, and ammunition
- Battlefield surveillance
- Reconnaissance of opposing forces and terrain
- Targeting
- Battle damage assessment
- Nuclear, biological, and chemical attack detection

2. Environmental Applications

- Forest fire detection
- Bio-complexity mapping of environment
- Flood detection
- Precision Agriculture
- Air and water pollution

3. Health Applications

- Tele-monitoring of human physiological data
- Tracking and monitoring doctors and patients inside a hospital
- Drug administration in hospitals

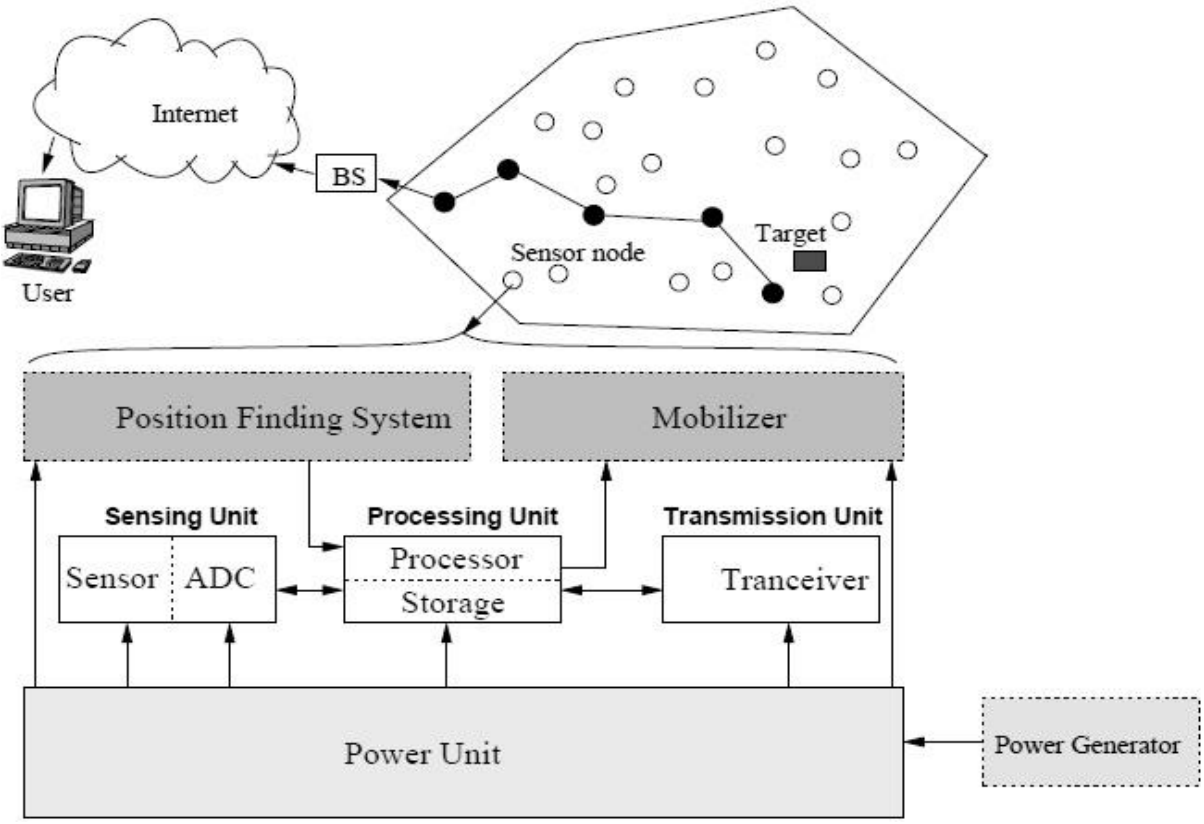
4. ***Home and Office Applications***
   - Home and office automation
   - Smart environment
5. ***Automotive Applications***
   - Reduces wiring effects
   - Measurements in chambers and rotating parts
   - Remote technical inspections
   - Conditions monitoring e.g. at a bearing

5.7.5 Design Challenges

- **Heterogeneity**
  - The devices deployed maybe of various types and need to collaborate with each other.
- **Distributed Processing**
  - The algorithms need to be centralized as the processing is carried out on different nodes.
- **Low Bandwidth Communication**
  - The data should be transferred efficiently between sensors
- **Large Scale Coordination**
  - The sensors need to coordinate with each other to produce required results.
- **Utilization of Sensors**
  - The sensors should be utilized in a ways that produce the maximum performance and use less energy.
- **Real Time Computation**
  - The computation should be done quickly as new data is always being generated.

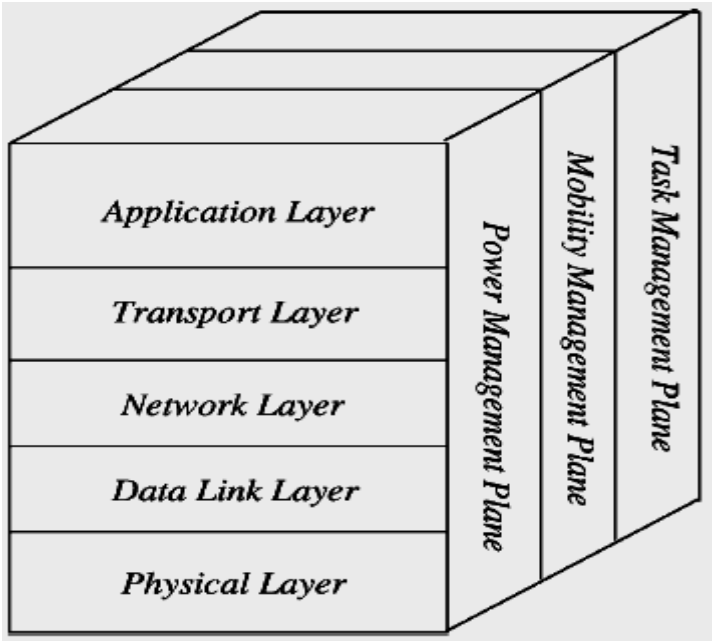
5.7.6 WSN Network Model

- The core of the wireless sensor node is the processing unit, usually a microprocessor with a limited amount of memory.
- The processing unit is connected to the sensors via one or more Analog to Digital Converters (ADCs).
- The sensors and the ADCs form the sensing unit.
- The data received by the sensing unit are processed and eventually transmitted by the transceiver unit.
- The transceiver unit is usually capable of bidirectional communications; nevertheless specific applications may require only transmission (TX) or reception (RX) capabilities.
- Specific nodes may integrate a location finding system that helps the node to discover its position, relative to its neighbors or global.
- This unit is often embedded on the transceiver module and requires the use of specific algorithms by the processing unit, depending on the adopted localization techniques.



- The power unit and the power generator are a key element in the sensor structure.
- The power unit is responsible to provide the electrical power needed by the other units in the system.
- Since the power generator usually consists of batteries, such devices have limited amount of energy available, thereby limiting the lifetime of the node.

5.7.7 WSN Protocol Stack



- This protocol stack combines power and routing awareness, integrates data with networking protocols, communicates power efficiently through the wireless medium and promotes cooperative efforts of sensor nodes.
- The protocol stack consists of the application layer, transport layer, network layer, data link layer, physical layer, power management plane, mobility management plane, and task management plane.
- Different types of application software can be built and used on the application layer depending on the sensing tasks. This layer makes hardware and software of the lowest layer transparent to the end-user.
- The transport layer helps to maintain the flow of data if the sensor networks application requires it.
- The network layer takes care of routing the data supplied by the transport layer, specific multi-hop wireless routing protocols between sensor nodes and sink.
- The data link layer is responsible for multiplexing of data streams, frame detection, Media Access Control (MAC) and error control. Since the environment is noisy and sensor nodes can be mobile, the MAC protocol must be power aware and able to minimize collision with neighbors' broadcast.
- The physical layer addresses the needs of a simple but robust modulation, frequency selection, data encryption, transmission and receiving techniques.
- In addition, the power, mobility, and task management planes monitor the power, movement, and task distribution among the sensor nodes. These planes help the sensor nodes coordinate the sensing task and lower the overall energy consumption.

5.7.8 Classification of Routing Protocols

- Routing techniques are required for sending data between sensor nodes and the base stations for communication. Different routing protocols are proposed for wireless sensor network. These protocols can be classified according to different parameters.
- Routing Protocols can be classified as Proactive, Reactive and Hybrid, based on their Mode of Functioning and Type of Target Applications.
- Routing protocols can be classified as Direct Communication, Flat and Clustering Protocols, according to the Participation style of the Nodes.
- Routing Protocols can be classified as Hierarchical, Data Centric and location based, depending on the Network Structure.

1. Based on Mode of Functioning and Type of Target Applications

- In a **Proactive Protocol** the nodes switch on their sensors and transmitters, sense the environment and transmit the data to a BS through the predefined route. e.g. The Low Energy Adaptive Clustering hierarchy protocol (LEACH) utilizes this type of protocol.
- **Reactive Protocols** are used if there are sudden changes in the sensed attribute beyond some pre-determined threshold value and the nodes immediately react. This type of protocol is used in time critical applications. e.g. The Threshold sensitive Energy Efficient sensor Network (TEEN) is an example of a reactive protocol.

- **Hybrid protocols** incorporate both proactive and reactive concepts. They first compute all routes and then improve the routes at the time of routing. e.g. Adaptive Periodic TEEN (APTEEN) is an example of a reactive protocol.

2. According to the Participation style of the Nodes

- **Direct Communication**: In this type of protocols, any node can send information to the Base Station(BS) directly. When this is applied in a very large network, the energy of sensor nodes may be drained quickly. Its scalability is very small. e.g. SPIN is an example of this type of protocol.
- **Flat**: In case of flat protocols, if any node needs to transmit data, it first searches for a valid route to the BS and then transmits the data. Nodes around the base station may drain their energy quickly. Its scalability is average. e.g. Rumor Routing is an example of this type of protocol.
- **Clustering Protocols**: According to the clustering protocol, the total area is divided into numbers of clusters. Each and every cluster has a cluster head (CH) and this cluster head directly communicates with the BS. All nodes in a cluster send their data to their corresponding CH. e.g. TEEN is an example of this type of protocol.

3. Depending on the Network Structure

- **Data Centric**:
  - Data centric protocols are query based and they depend on the naming of the desired data, thus it eliminates much redundant transmissions.
  - The BS sends queries to a certain area for information and waits for reply from the nodes of that particular region.
  - Since data is requested through queries, attribute based naming is required to specify the properties of the data.
  - Depending on the query, sensors collect a particular data from the area of interest and this particular information is only required to transmit to the BS and thus reducing the number of transmissions.
  - e.g. SPIN was the first data centric protocol.
- **Hierarchical:**

  Hierarchical routing is used to perform energy efficient routing, i.e., higher energy nodes can be used to process and send the information; low energy nodes are used to perform the sensing in the area of interest. Examples: LEACH, TEEN, APTEEN.
- **Location Based**:
  - Location based routing protocols need some location information of the sensor nodes.
  - Location information can be obtained from GPS (Global Positioning System) signals, received radio signal strength, etc.
  - Using location information, an optimal path can be formed without using flooding techniques.
  - e.g. Geographic and Energy-Aware Routing(GEAR)

DSDV routing protocol

Destination-Sequenced Distance Vector routing protocol (DSDV) is atypical routing protocol is based on the Distributed Bellman-Fordalgorithm. In DSDV, each route is tagged with a sequence number whichis originated by the destination, indicating how old the route is. Eachnode manages its own sequence number by assigning it two greater thanthe old one (call an even sequence number) every time. When a routeupdate with a higher sequence number is received, the old route isreplaced. In case of different routes with the same sequence number, theroute with better metric is used. Updates are transmitted periodically orimmediately when any significant topology change is detected. There aretwo ways of performing routing update: "full dump", in which a nodetransmits the complete routing table, and "incremental update", in whicha node sends only those entries that have changed since last update. Toavoid fluctuations in route updates, DSDV employs a "settling time"data, which is used to predict the time when route becomes stable. InDSDV, broken link may be detected by the layer-2 protocol or it mayinstead be inferred if no broadcasts have been received for a while from aformer neighboring node.

DSDV Characteristics

1. Proactive-based on Bellman–Ford.
2. Packets transmitted according to the routing table.
3. Each node maintains routing table with entry for each node in thenetwork.
4. Each node maintains its own sequence number.
5. Updates at each change in neighborhood information.
6. Used for freedom from loops.
7. To distinguish stale routes from new ones.

Pros

1. Proactive Routes maintained through periodic and event triggeredrouting table exchanges.
2. All available information is transmitted.

Cons

Frequency of transmitting full updates is reduced if the volume of databegins to consume significant bandwidth.

DSR routing protocol

DSR, an acronym for Dynamic Source Routing protocol, is an entirely on-demand ad hoc network routing protocol composed of two parts: Route Discovery and Route Maintenance. In DSR, when a node has a packet to send to some destination and does not currently have a route to that destination in its Route Cache, the node initiates Route Discovery to find a route; this node is known as the initiator of the Route Discovery, and the destination of the packet is known as the Discovery's target. The initiator transmits a ROUTE REQUEST packet as a local broadcast, specifying the target and a unique identifier from the initiator. Each node receiving the ROUTE REQUEST, if it has recently seen this request identifier from the initiator, discards the REQUEST. Otherwise, it appends its own node address to a list in the REQUEST and rebroadcasts the REQUEST. When the ROUTE REQUEST reaches its target node, the target sends a ROUTE REPLY back to the initiator of the REQUEST, including a copy of the accumulated list of addresses from the REQUEST. When the REPLY reaches the

initiator of the REQUEST, it caches the new route in its Route Cache. Route Maintenance is the mechanism by which a node sending a packet along a specified route to some destination detects if that route has broken, for example because two nodes in it have moved too far apart.

DSR is based on source routing: when sending a packet, the originator lists in the header of the packet the complete Sequence of nodes through which the packet is to be forwarded. Each node along the route forwards the packet to the next hop indicated in the packet's header, and attempts to confirm that the packet was received by that next node; a node may confirm this by means of a link-layer acknowledgment, passive acknowledgment, or network-layer acknowledgment. If, after a limited number of local retransmissions of the packet, a node in the route is unable to make this confirmation, it returns a ROUTE ERROR to the original source of the packet, identifying the link from itself to the next node as broken. The sender then removes this broken link from its Route Cache; for subsequent packets to this destination, the sender may use any other route to that destination in its Cache, or it may attempt a new Route Discovery for that target if necessary.

AODV Routing Protocol

AODV, an acronym for Ad-hoc On-demand Distance Vector routingprotocol, is a method of routing messages between mobile computers. Itallows these mobile computers, or nodes, to pass messages through theirneighbors to nodes with which they cannot directly communicate. AODVdoes this by discovering the routes along which messages can be passed.AODV makes sure these routes do not contain loops and tries to find theshortest route possible. AODV is also able to handle changes in routesand can create new routes if there is an error. Because of the limitedrange, each node can only communicate with the nodes next to it.

AODV is one of the most efficient routing protocols in terms ofestablishing the shortest path and lowest power consumption. It is mainlyused for ad-hoc networks but also in wireless sensor networks. It uses theconcepts of path discovery and maintenance. However, AODV buildsroutes between nodes on-demand i.e. only as needed. So, AODV's primary objectives are:

1. To broadcast discovery packets only when necessary,
2. To distinguish between local connectivity management (neighborhood detection) and general topology maintenance,
3. To disseminate information about changes in local connectivity to those neighboring mobiles nodes that are likely to need the information

AODV Characteristics

1. Will find routes only as needed.
2. Use of Sequence numbers to track accuracy of information.
3. Only keeps track of next hop for a route instead of the entireroute.
4. Use of periodic HELLO messages to track Neighbors.

Pros

1. The AODV routing protocol does not need any centraladministrative system to control the routing process.

2. Reactive protocols like AODV tend to reduce the control trafficmessages overhead at the cost of increased latency in finding newroutes.

Cons

1. It is possible that a valid route is expired.
2. The performance of the AODV protocol without any misbehaving nodes is poor in larger networks.

5.8 Comparison of 802.15 Standards

IEEE Standard	802.15.1	802.15.3	802.15.4
Topic	Bluetooth	HR-WPAN	LR-WPAN/ZigBee
Operational Spectrum	2.4 GHz ISM Band	2.402-2.480 GHz ISM band	2.4 GHz and 868/915MHz
Physical Layer Detail	FHSS	QPSK, 16/32/64 - QAM scheme	DSSS with BPSK or MSK
Channel Access	TDD	CSMA-CA	CSMA-CA
Data Throughput	Up to 1Mbps	>20Mbps	<0.25 Mbps
Modulation Technique	DPSK, GFSK	QPSK, 16/32/64 - QAM scheme	DSSS, BPSK
Coverage	<10m	<10m	<20m
Approximate Range	100m	10m	75m
Interference	Present	Present	Present
Security	Less Secure	Very high level of security including, piracy, encryption and digital service certificate	Security feature in development
Number of Channels	79	5	16
QoS needs	QoS suitable for voice application	Very high QoS	Relaxed needs for data rate and QoS
Applications	Mobile phones, printers, displays, etc	Digital Imaging	Vehicles, medical applications
Ad hoc	Yes	Yes	Yes
Infrastructure	No	No	No
Price	Low (<$10)	Medium	Very low

CHAPTER 6

WIRELESS METROPOLITAN AREA NETWORKS (WMAN)

6.1 Introduction

- A WMAN is a**wireless network** intended to provide a signal over an **area** approximately the size of a **metropolitan area** (approximately 50 kilometers or 31 miles).
- A WMAN is typically owned by a single entity such as an Internet service provider (ISP), government entity, or large corporation.
- Access to a WMAN is usually restricted to authorized users or subscriber devices.
- WiMAX is the most widely used form of WMAN.
- **Goal:** Provide high-speed Internet access to home and business subscribers, without wires.
- Base stations (BS) can handle thousands of subscriber stations (SS)
- BS can control all data traffic that goes between BS and SS through the allocation of bandwidth on the radio channel.
- **Supports**
  - Legacy voice systems
  - Voice over IP
  - TCP/IP
  - Applications with different QoS requirements.
- **Main advantage**: fast deployment, dynamic sharing of radio resources and low cost.

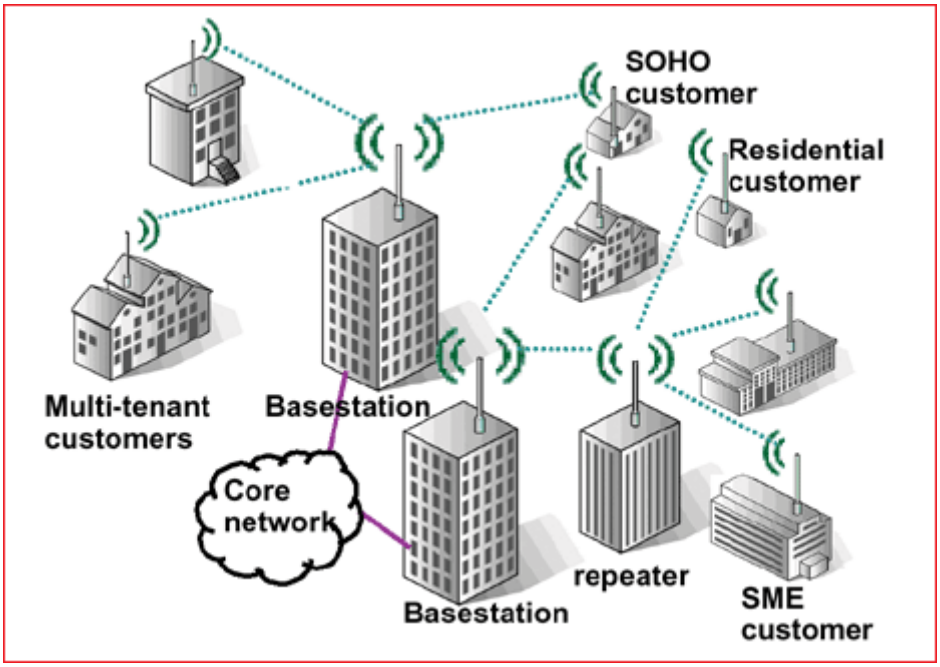


Figure: WMAN Network

SOHO Customer: Small Office/ Home Office Customer
SME: Small/ Medium Sized Enterprise

WMANs are implemented with the help of following wireless technologies:

1. **Local Multipoint Distribution Service(LMDS):**Refers to a wireless broadband point-to-multipoint access technology that provides data, voice, Internet and video-services using microwave frequencies.
2. **Multichannel Multipoint Distribution Service (MMDS):**Refers to a wireless broadband point-to-multipoint specification that uses Ultra High Frequency (UHF).
3. **Free Space Optics (FSO):** Refers to the transmission of Infrared (IR) beams to get broadband communications.
4. **Wireless Local Loop (WLL):** Refers to a technology in which the subscriber gets connected to an exchange with the help of a radio link rather than using copper wires.
5. **Worldwide Interoperability for Microwave Access (WiMAX):** Refers to a technology defined by IEEE 802.16 standards providing access to a metropolitan area and are called WMAN standards.

6.2 IEEE 802.16 (WiMAX)

IEEE 802.16 is a series of wireless broadband standards written by the Institute of Electrical and Electronics Engineers (IEEE). The IEEE Standards Board established a working group in 1999 to develop standards for broadband for wirelessmetropolitan area networks. The Workgroup is a unit of the IEEE 802local area network and metropolitan area network standards committee.

Although the 802.16 family of standards is officially called WirelessMAN in IEEE, it has been commercialized under the name "WiMAX" (from "Worldwide Interoperability for Microwave Access") by the WiMAX Forum industry alliance. The Forum promotes and certifies compatibility and interoperability of products based on the IEEE 802.16 standards.

Table below lists the various wireless broadband standards. The proposed standards are indicated by a prefixed P letter. This proposed standard later gets dropped and replaced by a dash and year after the standard gets approved and published.

Standard	Description	Status
802.16-2001	Fixed Broadband Wireless Access (10–66 GHz)	Superseded
802.16.2-2001	Recommended practice for coexistence	Superseded
802.16c-2002	System profiles for 10–66 GHz	Superseded
802.16a-2003	Physical layer and MAC definitions for 2–10 GHz	Superseded
P802.16b	License-exempt frequencies (Project withdrawn)	Withdrawn
P802.16d	Maintenance and System profiles for 2–11 GHz (Project merged into 802.16-2004)	Merged
802.16-2004	Air Interface for Fixed Broadband Wireless Access System (rollup of 802.16–2001, 802.16a, 802.16c and P802.16d)	Superseded
P802.16.2a	Coexistence with 2–11 GHz and 23.5–43.5 GHz (Project merged into 802.16.2-2004)	Merged

802.16.2-2004	IEEE Recommended Practice for **Local and metropolitan area networks** **Coexistence of Fixed Broadband Wireless Access Systems** (Maintenance and rollup of 802.16.2–2001 and P802.16.2a) Released on 2004-March-17.	Current
802.16f-2005	Management Information Base (MIB) for 802.16-2004	Superseded
802.16-2004/Cor 1–2005	Corrections for fixed operations (co-published with 802.16e-2005)	Superseded
802.16e-2005	Mobile Broadband Wireless Access System	Superseded
802.16k-2007	IEEE Standard for **Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges** **Amendment 2: Bridging of IEEE 802.16** (An amendment to IEEE 802.1D) Released on 2007-August-14.	Current
802.16g-2007	Management Plane Procedures and Services	Superseded
P802.16i	Mobile Management Information Base (Project merged into 802.16-2009)	Merged
802.16-2009	Air Interface for Fixed and Mobile Broadband Wireless Access System (rollup of 802.16–2004, 802.16-2004/Cor 1, 802.16e, 802.16f, 802.16g and P802.16i)	Superseded
802.16j-2009	Multihop relay	Superseded
802.16h-2010	Improved Coexistence Mechanisms for License-Exempt Operation	Superseded
802.16m-2011	Advanced Air Interface with data rates of 100 Mbit/s mobile and 1 Gbit/s fixed. Also known as *Mobile WiMAX Release 2* or *WirelessMAN-Advanced*. Aiming at fulfilling the ITU-R IMT-Advanced requirements on 4G systems.	Superseded[2]
802.16-2012	IEEE Standard for **Air Interface for Broadband Wireless Access Systems** It is a rollup of 802.16h, 802.16j and Std802.16m (but excluding the WirelessMAN-Advanced radio interface, which was moved to IEEE Std 802.16.1). Released on 2012-August-17.	Current
802.16.1-2012	IEEE Standard for **WirelessMAN-Advanced Air Interface for Broadband Wireless Access Systems** Released on 2012-September-07.	Current
802.16p-2012	IEEE Standard for **Air Interface for Broadband Wireless Access Systems** **Amendment 1: Enhancements to Support Machine-to-Machine Applications** Released on 2012-October-08.	Current
802.16.1b-2012	IEEE Standard for **WirelessMAN-Advanced Air Interface for Broadband Wireless Access Systems** **Amendment 1: Enhancements to Support Machine-to-Machine Applications** Released on 2012-October-10.	Current
802.16n-2013	IEEE Standard for **Air Interface for Broadband Wireless Access Systems**	Current

	Amendment 2: Higher Reliability Networks Approved on 2013-March-06.	
802.16.1a-2013	IEEE Standard for **WirelessMAN-Advanced Air Interface for Broadband Wireless Access Systems** **Amendment 2: Higher Reliability Networks** Approved on 2013-March-06.	

Goals of Working Group 802.16

The goal of the Working Group 802.16 is to form standards that accomplish the following conditions:

- Utilize licensed spectrum
- Utilize wireless links having microwave or millimeter wave radios
- Transmits data at broadband speeds up to 2Mbps
- Offer public network service to customers who pay fees
- Offer efficient transmission of heterogeneous traffic, thereby supporting QoS.
- Utilize point-to-multipoint architectures with the help of antennas.

Key Features of IEEE 802.16

1. Broadband Wireless Access
2. Coverage area up to 50 km.
3. Data rate up to 70 Mbps.
4. Modulation technique used is BPSK, 64-QAM.
5. Offers non-line of site (NLOS) operation.
6. 1.5 to 28 MHz channel support.
7. Hundreds of simultaneous sessions can be carried per channel.
8. Delivers >1Mbps data throughput per user.
9. Supports both licensed and unlicensed spectrum.
10. QoS for voice, video, and T1/E1, continuous and bursty traffic.
11. Support Point-to-Multipoint (PMP) and Mesh network models.

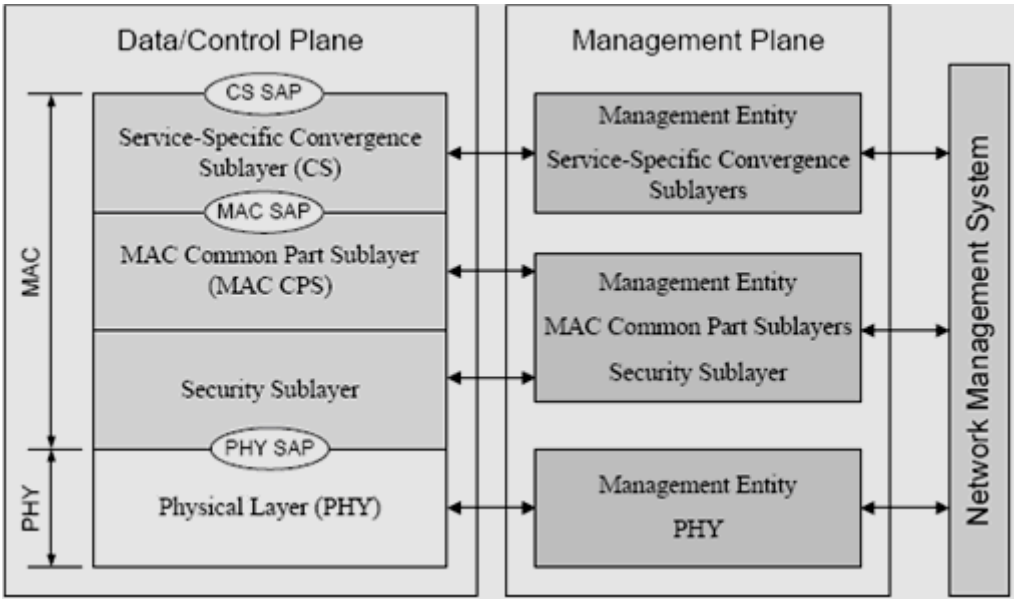
6.3 IEEE 802.16 Protocol Architecture

IEEE 802.16 is a broadband wireless access network standard that describes two layers, PHY and MAC to provide services for Point-to-Multipoint (PMP) broadband wireless access.

MAC Layer

- The MAC layer refers to an interface that reads data between the physical layer and the data link layer.
- The main goal of the MAC layer is to provide support to PMP architecture using a central base station that controls the subscriber stations connected to it.
- The 802.16 MAC protocol is connection based, which when connected to a network, every subscriber station creates one or multiple connections with the help of which data can be transmitted.
- A 16-bit unique Connection Identification (CID) is assigned to the transport connection by the base station.
- All uplink connections are unicast and all the downlink connections can be either unicast or multicast.

IEEE 802.16 MAC Layer Reference Model



The IEEE 802.16 MAC layer is categorized into the following three sublayers:

Service Specific Convergence Sublayer (CS):

- ✓ The service specific convergence sublayer (CS) provides any transformation or mapping of external network data, received through the CS service access point (SAP) into MAC SDUs received by the MAC CPS through the MAC SAP.
- ✓ Accepts higher layer protocol data units (PDUs) from the higher layer.
- ✓ Perform classification of higher layer PDUs and associates them to the proper service flow identified by the connection identifier (CID).
- ✓ Delivering CS PDUs to the appropriate MAC SAP.

MAC Common part sublayer

- ✓ Defines multiple-access mechanism
- ✓ Bandwidth allocation
- ✓ Connection establishment
- ✓ Connection maintenance
- ✓ Connection-oriented protocol
- ✓ Assign connection ID to each service flow.

Security sublayer

- ➢ Deals with privacy and security.
- ➢ The security sublayer provides subscribers with privacy or confidentiality across the broadband wireless network.
- ➢ It manages :
  - ✓ Authentication
  - ✓ Secure key exchange
  - ✓ Encryption

PHY Layer

- 802.16 uses scalable OFDMA to carry data, supporting channel bandwidths of between 1.25 MHz and 20 MHz, with up to 2048 subcarriers.

- It supports adaptive modulation and coding, so that in conditions of good signal, a highly efficient 64 QAM coding scheme is used, whereas when the signal is poorer, a more robust BPSK coding mechanism is used.
- In intermediate conditions, 16 QAM and QPSK can also be employed.
- Other PHY features include support for multiple-input multiple-output (MIMO) antennas in order to provide good non-line-of-sight propagation (NLOS) characteristics (or higher bandwidth) and hybrid automatic repeat request (HARQ) for good error correction performance.
- Although the standards allow operation in any band from 2 to 66 GHz, mobile operation is best in the lower bands which are also the most crowded, and therefore most expensive.

6.3 IEEE 802.16a (Broadband Wireless Access BWA)

Features:

- Supports low latency applications such as voice and video,
- Provides broadband connectivity without requiring a direct line of sight between subscriber terminals and the base station (BTS) and
- Will support hundreds if not thousands of subscribers from a single BTS.

Application of IEEE 802.16 Standard

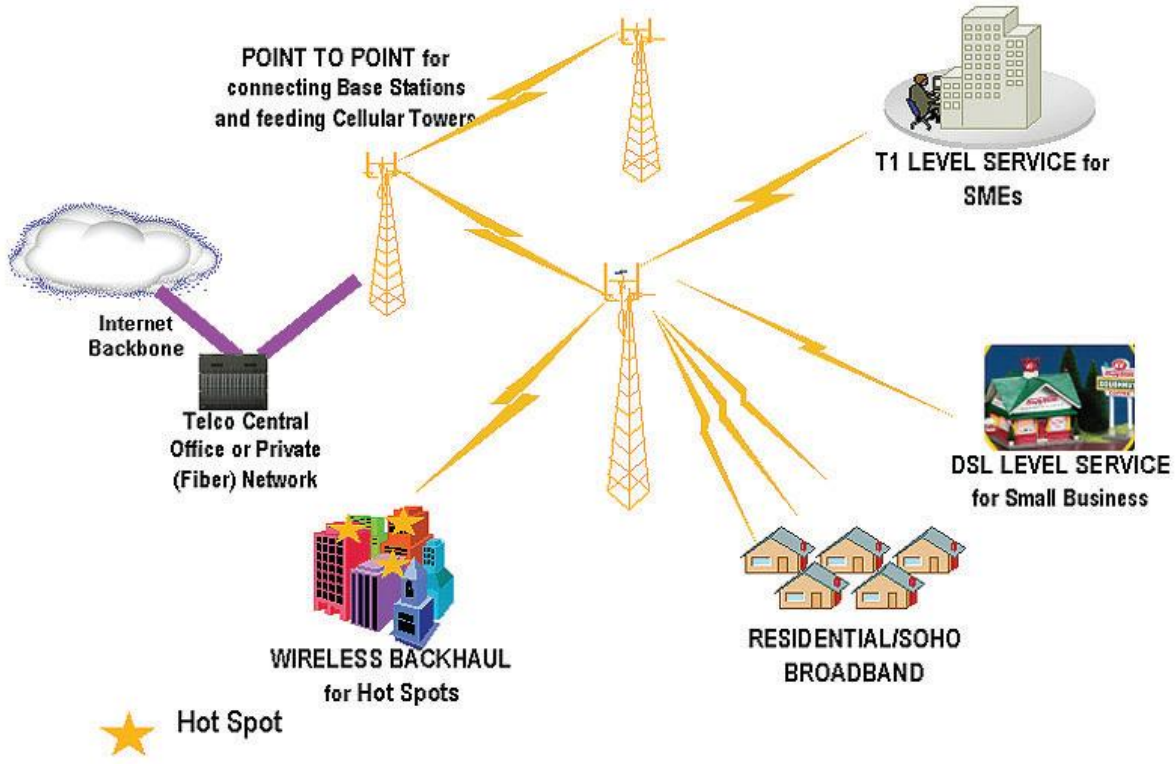


Figure 1. BWA (IEEE 802.16) Everywhere

- In BWA, applications include residential broadband access-- DSL-level service for SOHO and small businesses,
- T1/E1 level service for enterprise, all supporting not just data but voice and video as well,
- wireless backhaul for hotspots and

- cellular tower backhaul service to name a few.

IEEE 802.16a PHY Layer

Feature	Benefit
256 point FFT OFDM waveform	• Built in support for addressing multipath in outdoor LOS and NLOS environments
Adaptive Modulation and variable error correction encoding per RF burst	• Ensures a robust RF link while maximizing the number of bits/ second for each subscriber unit.
TDD and FDD duplexing support	• Address varying worldwide regulations where one or both may be allowed
Flexible Channel sizes (e.g. 3.5MHz, 5MHz, 10MHz, etc)	• Provides the flexibility necessary to operate in many different frequency bands with varying channel requirements around the world.
Designed to support smart antenna systems	• Smart antennas are fast becoming more affordable, and as these costs come down their ability to suppress interference and increase system gain will become important to BWA deployments.

IEEE 802.16a MAC Layer

Feature	Benefit
TDM/TDMA Scheduled Uplink/Downlink frames.	• Efficient bandwidth usage
Scalable from 1 to hundreds of subscribers	• Allows cost effective deployments by supporting enough subs to deliver a robust business case
Connection-oriented	• Per Connection QoS • Faster packet routing and forwarding
QoS supportContinuous GrantReal Time Variable Bit RateNon Real Time Variable Bit RateBest Effort	• Low latency for delay sensitive services (TDM Voice, VoIP) • Optimal transport for VBR traffic(e.g., video)· Data prioritization
Automatic Retransmission request (ARQ)	• Improves end-to-end performance by hiding RF layer induced errors from upper layer protocols
Support for adaptive modulation	• Enables highest data rates allowed by channel conditions, improving system capacity
Security and encryption (Triple DES)	• Protects user privacy
Automatic Power control	• Enables cellular deployments by minimizing self interference

6.4 WiMAX and LTE/3GPP Comparison

- **LTE**
  - Long Term Evolution is more commonly referred to as LTE
  - LTE is the 4th generation network that was designed through the Third Generation Partnership Project (3GPP).
  - It is an all IP network.

- Its primary goals were to improve efficiency, lower infrastructure costs, create a higher QoS, all while making use of new spectrum opportunities, and better integrating with other open standards
- Predominantly created by Ericsson, Nortel and Nokia-Siemens

- **WiMax**
  - Mobile WiMax is short for Wireless Interoperability for Microwave Access
  - WiMax is the 4th Generation wireless broadband access network developed by the IEEE
  - It is the 802.16e or upcoming 802.16m standards
  - It is an all IP network
  - Many hardware manufacturers are already supporting WiMax due to its open standards. Some of the larger ones include Samsung, Motorola and Intel.

Similarities between WiMAX and LTE

- Both the technologies are IP technologies.
- Both use Multiple Input and Multiple Output (MIMO) antenna technology.
- Both use modulation technology that is based on OFDM.

Differences between WiMAX and LTE

Features	WiMAX	LTE
Channel Bandwidth Utilization	40 MHz	1.4 to 100 MHz
Modulation Technology	SCFDMA for both uplink and downlink	SCFDMA for uplink OFDMA for downlink
Frame Duration	5 ms	10 ms
Speed	120 km/hr	40 km/hr
Compliant to 2G and 3G	No	Yes
Cost to build network	Less	More

LTE Advantages over WiMAX

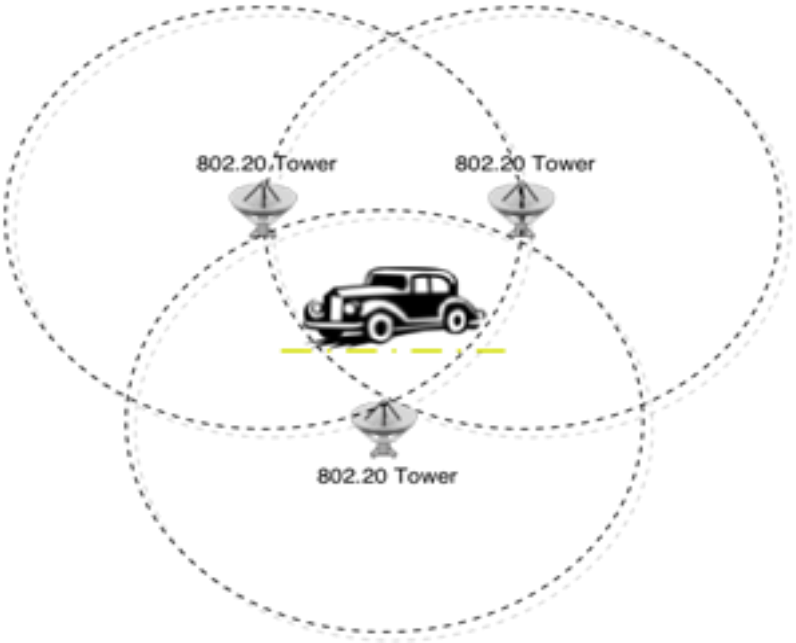
- **LTE is compatible with previous mobile technologies** – GSM, GPRS, UMTS, EDGE, WCDMA, HSPA, CDMA-one, CDMA2000, EV-DO, EV-DV and the synchronous SC-CDMA
- Enables much greater speed for the mobile users – speed up to 450 km/h or 250 mph
- Better technology for power consumption of mobile terminals – it uses SC-FDMA for uplink – modulation technology that saves battery life of mobile terminals
- LTE-A is only true 4G technology.

WiMAX Advantages over LTE

- Deployment of WiMAX network is much cheaper than deployment of LTE network.
- Great choice for private mobile broadband wireless networks.

6.5 IEEE 802.20 Standard

- Also known as Mobile Broadband Wireless Access, or MBWA.
- It aims to provide "vehicular" mobility at speeds of up to 250 km/h.
- 802.20 is a clean-sheet design focused exclusively on providing high-speed mobility at speeds similar to ADSL.
- The 802.20 standard is being positioned as an alternative to 2.5 and 3G cellular services.



802.20 PHY Layer Overview

- The PHY layer of the 802.20 standard is loosely based on technologies developed in the 802.16 working groups.
- The 802.20 standard is set to operate in licensed bands below 3.5 GHz in a NLOS mode of operation.
- Licensed bands will be used to provide a packet-switched connection similar to that of the circuit-switched networks operated by current cellular providers.
- Wide variety of channel bandwidths from 1.25 MHz to 40 MHz are also expected to be supported with both TDD and FDD duplexing.
- Modulation and coding in 802.20 is essentially identical to that of 802.16a/d.
- Modulation rates from BPSK to 64QAM are all supported, along with both convolutional and turbo coding.
- In order to allow flexible high-speed mobility, the 802.20 standard is expected to support essentially all of the advanced transmission options that the 802.16 family of standards defines. These include, but are not limited to, AAS, STBC and various forms of Spatial Multiplexing/MIMO.
- SDMA is forward-link transmission technique used at the BS to signal multiple users via the same time-frequency resources.

802.20 MAC Layer Overview

- Like the PHY layer, the MAC layer of the 802.20 standard is also loosely based on technologies developed in the 802.16 working groups.

- Being a fully mobile standard, 802.20 will include support for all sorts of handoff mechanisms to enable users to freely roam between service areas without interruption.
- Since different forward and reverse-link connection mechanisms may be used, handoff will need to occur in both directions.
- In order to conserve power in mobile devices, support for a sleep-like operation mode is described in the current 802.20 partial standard proposal. Before a device enters the idle state it negotiates a paging period with the BS. The device is then allowed to "sleep".
- Data sent over devices supporting 802.20 will be encrypted with public keys generated by the AES 128-bit algorithms. In combination with AES-128, mechanisms for ensuring that data integrity is preserved will be included in the standard. Further security features will include cross-authentication to prevent user and BS spoofing, as well as some sort of mechanism for preventing and/or avoiding Denial of Service (DoS) attacks.

6.6 Comparing Technologies

	802.11 WiFi	**802.16 WiMAX**	**802.20 Mobile-FI**	**UMTS 3G**
Bandwidth	11-54 Mbps shared	Share up to 70 Mbps	Up to 1.5 Mbps each	384 Kbps – 2 Mbps
Range (LOS) **Range (NLOS)**	100 meters 30 meters	30 – 50 km 2 - 5 km	3 – 8 km	Coverage is overlaid on wireless infrastructure
Mobility	Portable	Fixed (Mobile - 16e)	Full mobility	Full mobility
Frequency/ Spectrum	2.4 GHz for 802.11b/g 5.2 GHz for 802.11a	2-11 GHz for 802.16a 11-60 GHz for 802.16	<3.5 GHz	Existing wireless spectrum
Licensing	Unlicensed	Both	Licensed	Licensed
Standardization	802.11a, b and g standardized	802.16, 802.16a and 802.16 REVd standardized, other under development	802.20 in development	Part of GSM standard
Availability	In market today	Products 2H05	Standards coming Product late '06	CW in 6+ cities
Backers	Industry-wide	Intel, Fujitsu, Alcatel, Siemens, BT, AT&T, Qwest, McCaw	Cisco, Motorola, Qualcom and Flarion	GSM Wireless Industry

CHAPTER 7
SECURITY ISSUES IN WIRELESS SYSTEMS

7.1 The Need for Wireless Network Security

- A wireless local area network is a flexible data communication system.
- Wireless LANs transmit and receive the data over the air using the radio frequency technology.
- Thus, wireless LANs combine data connectivity with user mobility.
- But one of the scariest revelations is that wireless LANs are insecure and the data sent over them can be easily broken and compromised.
- The security issue in wireless networks is much more critical than in wired networks.
- The major issues are: (a) threats to the physical security of the network; (b) unauthorized access by unwanted parties; and (c) privacy.

7.2 Attacks on Wireless Networks

- Attacks on computer systems and networks can be divided into passive and active attacks.

7.2.1 Active Attacks

- Active attacks involve altering data or creating fraudulent streams.
- These types of attacks can be divided into the following subclasses: (a) masquerade; (b) reply; (c) modification of messages; and (d) denial of service.
- A masquerade occurs when one entity pretends to be a different entity.
- Reply involves the passive capture of a data unit and its subsequent retransmission to construct unwanted access.
- Modification of messages means that some portion of a genuine message is changed or that messages are delayed or recorded to produce an unauthorized result.

7.2.2 Passive Attacks

- Passive attacks are inherently eavesdropping or snooping on transmission.
- The attacker tries to access information that is being transmitted.
- There are two subclasses: release of message contents, and traffic analysis.
- In the first type, the attacker reaches the e-mail messages or a file being transferred.
- In traffic analysis type of attack, the attacker could discover the location and identity of communicating hosts and could observe the frequency and length of encrypted messages being exchanged.
- Such information could be useful to the attacker as it can reveal useful information in guessing the nature of the information being exchanged.

7.3 Categories of attack on wireless computer networks

The main categories of attack on wireless computer networks are:

- **Interruption of service**: Here, the resources of the system are destroyed or become unavailable.
- **Modification**: This is an attack on the integrity of the system. In this case, the attacker not only gains access to the network, but tampers with data such as changing the values in a database, altering a program so that it does different tasks.
- **Fabrication:** This is an attack on the authenticity of the network. Here the attacker inserts counterfeit objects such as inserting a record in a file.

- **Interception**: This is an attack on the confidentiality of the network such as wiretapping or eavesdropping to capture data in a network.
- **Jamming**: Interruption of service attacks is also easily applied to wireless networks. In such a case, the legitimate traffic cannot reach clients or access points due to the fact that illegitimate traffic overwhelms the frequencies.
- **Client-to-client attacks**: Wireless network users need to defend clients not just against an external threat, but also against each other. Wireless clients that run TCP/IP protocols such as file sharing are vulnerable to the same mis-configurations as wired networks. Also, duplication of IP or MAC addresses whether it's intentional or accidental, may cause disruption of service.
- **Attacks against encryption**: The IEEE 802.11b standard uses an encryption scheme called Wired Equivalent Privacy (WEP) which has proven to have some weaknesses. Sophisticated attacker can break the WEP scheme.
- **Mis-configuration**: In order to have ease and rapid deployment, the majority of access points have an unsecured configuration. This means that unless the network administrator configures each access point properly, these access points remain at high risk of being accessed by unauthorized parties or hackers.
- **Brute force attacks against passwords of access points:** The majority of access points use a single password or key, which is shared by all connecting wireless clients. Attackers can attempt to compromise this password or key by trying all possibilities. Once the attacker guesses the key or the password, he/she can gain access to the access point and compromise the security of the system.
- **Insertion attacks**: This type of attack is based on deploying a new wireless network without following security procedure. Also, it may be due to installation of an unauthorized device without proper security review.

7.4 Characteristics of Network Security System

Any network security system should maintain the following characteristics:

- **Integrity:** This requirement means that operations such as substitution, insertion or deletion of data can only be performed by authorized users using authorized methods.
- **Confidentiality:** This means that the network system can only be accessed by authorized users. The type of access can be read-only access.
- **Denial of service:** This term is also known by its opposite, availability. An authorized individual should not be prevented or denied access to objects to which he has legitimate access.

7.5 Reasons for Security Problems in Computer Networks

- **Sharing:** Since network resources are shared, more users have the potential to access networked systems rather than just a single computer node.
- **Complexity:** Due to the complexity of computer networks of all types, reliable and secure operation is a challenge. Moreover, computer networks may have dissimilar nodes with different operating systems, which make security more challenging.
- **Anonymity:** A hacker or intruder can attack a network system from hundreds of miles away and thus never have to touch the network or even come into contact with any of its users or administrators.
- **Multiple point of attack:** When a file exists physically on a remote host, it may pass many nodes in the network before reaching the user.
- **Unknown path:** In computer networks, routes taken to route a packet are seldom known ahead of time by the network user. Also these users have no control of the

routes taken by their own packets. Routes taken depend on many factors such as traffic patterns, load condition, and cost.

7.6 Security Services

Security services can be classified as follows:

- **Confidentiality:** This service means the protection of data being carried by the networkfrom passive attacks. The broadcast service should protect data sent by users. Other formsof this service include the protection of a single message or a specific field of a message.Another aspect of confidentiality is the protection of traffic from a hacker who attempts toanalyze it. In other words, there must be some measures that deny the hackers fromobserving the frequency and length of use, as well as other traffic characteristics in thenetwork.
- **Non-repudiation:** This service prevents the sending or receiving party from denying the sent or received message. This means that when a message is received, the sender canconfirm that the message was in fact received by the assumed receiver.
- **Authentication:** The authentication service is to ensure that the message is from an authentic source. In other words, it ensures that each communicating party is the entity that it claims to be. Also, this service must ensure that the connection is not interfered with in a way that a third party impersonates one of the authorized parties.
- **Access control**: This service must be accurate and intelligent enough so that only authorized parties can use the system. Also, this accuracy should not deny authorized parties from using the network system.
- **Integrity:** In this context, we differentiate between connection-oriented and connection based integrity services. The connection-oriented integrity service deals with a stream of messages, and ensures that the messages are sent properly without duplication, modification, reordering or reply. Moreover, the denial of service aspect is covered under the connection-oriented service. The connectionless integrity service deals only with the protection against message modification.
- **Availability:** Some attacks may result in loss or reduction of availability of the system. Automated schemes can resolve some of these problems while others require some type of physical procedures.

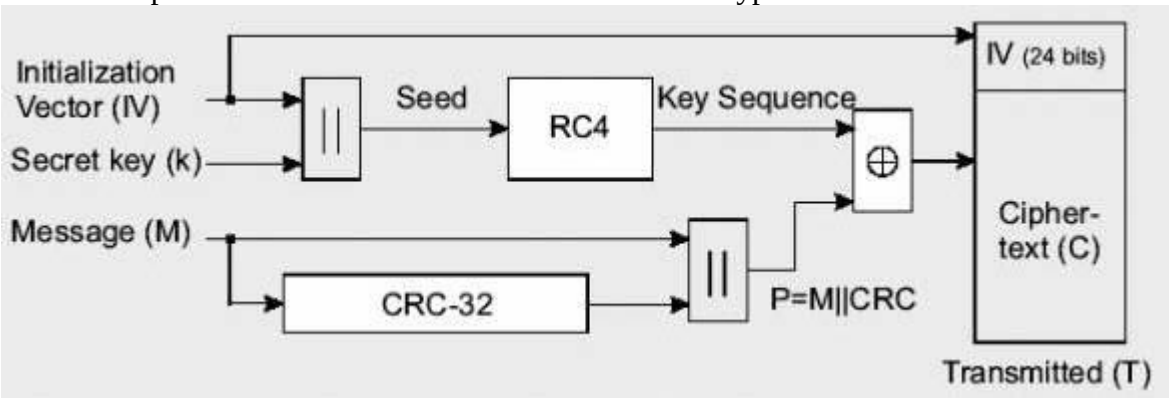
7.7 Wired Equivalent Privacy (WEP)

- WEP is “Wired Equivalent Privacy” or “Wireless Encryption Protocol”
- It is the original wireless security protocol for the 802.11 standard.
- It uses the RC4 stream cipher, using a 64-bit key consisting of:
  - A 40-bit master key
  - A 24-bit initialization vector (IV)
- An **initialization vector** (IV) is an arbitrary number that can be used along with a secret key for data encryption.
- It also employs a CRC integrity checksum.
- The key does not need to be replaced every packet since the end points are synchronized and RC4 can produce the same key stream at both ends using the session key.
- In contrast to the wireless medium, 802.11 changes keys for every packet because the synchronization between the end-points is not perfect and is subject to packet loss.
- This way each packet can be encrypted and decrypted disregarding the previous packets loss.

- The same key is used to encrypt and decrypt the data. The WEP encryption algorithm works the following way:

WEP Encryption

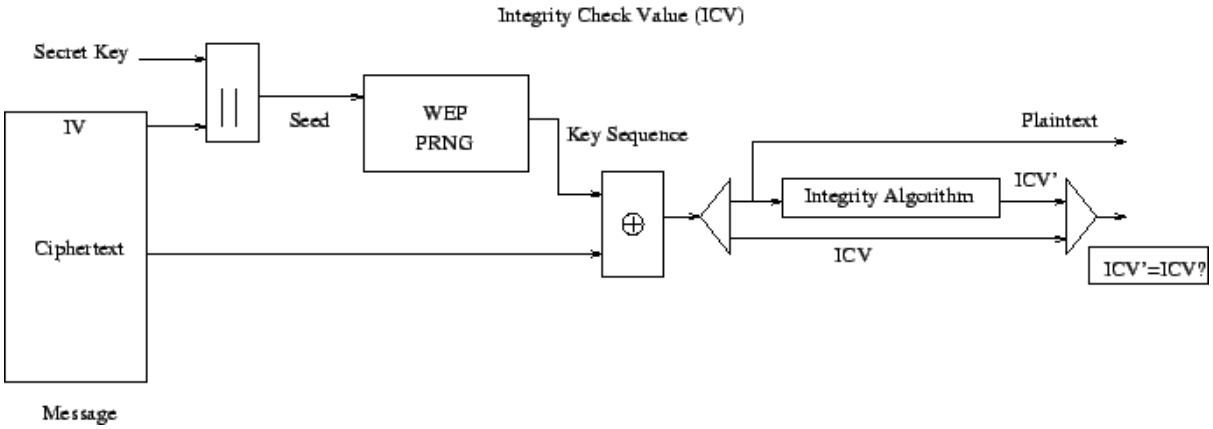
- Two processes are applied to the plaintext data. One encrypts the plaintext; the other protects the data from being modified by unauthorized personnel.
- The 40-bit secret key is connected with a 24-bit Initialization Vector (IV) resulting in a 64-bit total key size. The resulting key is input into the **Pseudo-random Number Generator (PRNG).**
- The **PRNG** (**RC4**) outputs a pseudorandom key sequence based on the input key.
- The resulting sequence is used to encrypt the data by doing a bitwise XOR.
- The result is encrypted bytes equal in length to the number of data bytes that are to be transmitted in the expanded data plus four bytes.
- This is because the key sequence is used to protect the 32-bit Integrity Check Value(ICV) as well as the data.
- The picture below illustrates how the WEP is encrypted.



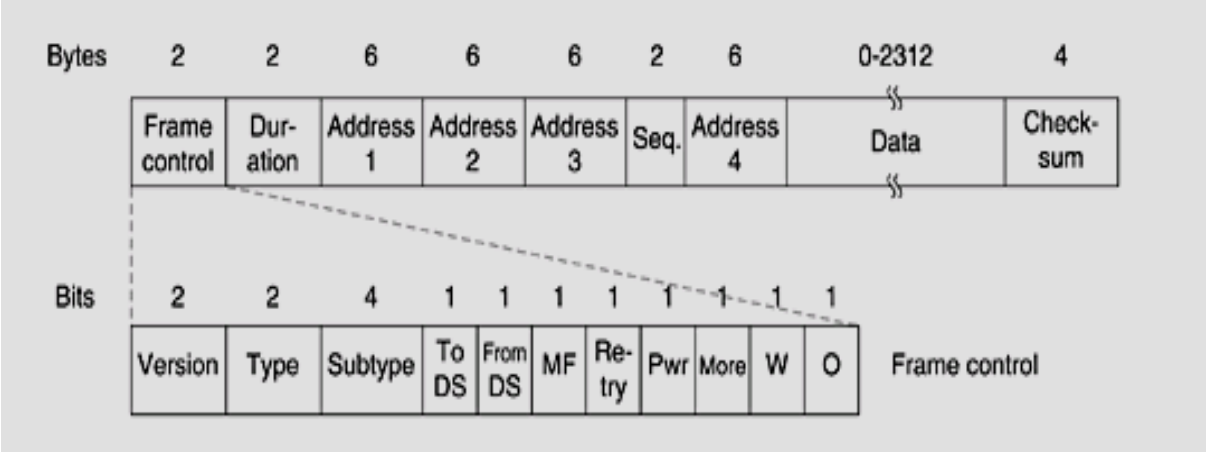
- To prevent unauthorized data modification, an *integrity algorithm,* CRC-32 operates on the plaintext to produce the ICV.
- The ciphertext is obtained by computing the ICV using CRC-32 over the message plaintext.
- The IV, plaintext, and ICV triplet forms the actual data sent in the data frame.

WEP Decryption

- The IV of the incoming message is used to generate the key sequence necessary to decrypt the incoming message.
- Combining the cipher text with the proper key sequence will give the original plaintext and ICV.
- The decryption is verified by performing the Integrity check algorithm on the recovered plaintext and comparing the output of the ICV' to the ICV submitted with the message.
- If the ICV' is not equal to the ICV, the received message is in error, and an error indication is sent to the MAC management and back to the sending station.
- The following diagram exhibits how WEP is decrypted.



WEP Frame Format



The 802.11 standard defines three different classes of frames on the wire: data, control, and management. Each of these has a header with a variety of fields used within the MAC sublayer.

- First comes the **Frame Control** field. It itself has 11 subfields.
  - The first of these is the ***Protocol version***, which allows two versions of the protocol to operate at the same time in the same cell.
  - Then comes the ***Type*** (data, control, or management) and ***Subtype*** fields (e.g., RTS or CTS).
  - The ***To DS*** and ***From DS*** bits indicate the frame is going to or coming from the intercell distribution system (e.g., Ethernet).
  - The ***MF*** bit means that more fragments will follow.
  - The ***Retry*** bit marks a retransmission of a frame sent earlier.
  - The ***Power management*** bit is used by the base station to put the receiver into sleep state or take it out of sleep state.
  - The ***More*** bit indicates that the sender has additional frames for the receiver.
  - The ***W*** bit specifies that the frame body has been encrypted using the WEP (Wired Equivalent Privacy) algorithm.
  - Finally, the ***O*** bit tells the receiver that a sequence of frames with this bit on must be processed strictly in order.

- The second field of the data frame, the **Duration field**, tells how long the frame and its acknowledgement will occupy the channel. This field is also present in the control frames and is how other stations manage the NAV mechanism.
- The frame header contains **four addresses**, all in standard IEEE 802 format. The ***source*** and ***destination*** are obviously needed, but what are the other two for? Remember that frames may enter or leave a cell via a base station. The other two addresses are used for the ***source and destination base stations for intercell traffic***.
- The **Sequence** field allows fragments to be numbered. Of the 16 bits available, 12 identify the frame and 4 identify the fragment.
- The **Data** field contains the payload, up to 2312 bytes, followed by the usual Checksum.

Management frames have a format similar to that of data frames, except without one of the base station addresses, because management frames are restricted to a single cell.

Control frames are shorter still, having only one or two addresses, no Data field, and no Sequence field. The key information here is in the Subtype field, usually RTS, CTS, or ACK.

Weaknesses of WEP

- **The IV is too small and in clear text:** It's a 24-bit field sent in the clear text portion of a message. This 24-bit string, used to initialize the key stream generated by the RC4 algorithm, is a relatively small field when used for cryptographic purposes.
- **The IV is static:** Reuse of the same IV produces identical key streams for the protection of data, and because the IV is short, it guarantees that those streams will repeat after a relatively short time (between 5 and 7 hours) on a busy network.
- **The IV makes the key stream vulnerable:** The 802.11 standard does not specify how the IVs are set or changed, and individual wireless adapters from the same vendor may all generate the same IV sequences, or some wireless adapters may possibly use a constant IV. As a result, hackers can record network traffic, determine the key stream, and use it to decrypt the cipher text.
- **The IV is a part of the RC4 encryption key:** The fact that an eavesdropper knows 24-bits of every packet key, combined with a weakness in the RC4 key schedule, leads to a successful analytic attack that recovers the key after intercepting and analyzing only a relatively small amount of traffic. Such an attack is so nearly a no-brainer that it's publicly available as an attack script and as open-source code.
- **WEP provides no cryptographic integrity protection:** However, the 802.11 MAC protocol uses a non-cryptographic Cyclic Redundancy Check (CRC) to check the integrity of packets, and acknowledges packets that have the correct checksum. The combination of non-cryptographic checksums with stream ciphers is dangerous — and often introduces vulnerabilities.

7.8 Mobile IP

- Mobile IP enable computers to maintain Internet connection during their movement from one Internet access point to another.
- The term mobile implies that the user is connected to one or more application across the Internet and the access point changes dynamically.
- Mobile IP is the modification to the standard IP so that it allows the client to send and receive datagrams no matter where it is attached to the network.
- The only security problem using this mechanism is redirection attacks.

- A redirection attack occurs when a malicious client gives false information to the home agent in the mobile IP network.
- The home agent is informed that the client has a new care of address. So all IP datagrams addressed to the actual client are redirected to the malicious client.
- Mobile IP is designed to resist two kinds of attacks: (a) a malicious agent that may reply to old registration messages and cut the node from its network, and (b) a node that may pretend to be a foreign agent and send a registration request to a home agent in order to divert traffic that is intended for a mobile node to itself.
- Message authentication and proper use of the identification field of the registration request and reply messages are often used to protect mobile IPs from these kinds of attack.
- In order to protect against such attacks, the use of message authentication and proper use of the identification field of the registration request and reply messages is supposed to be effective.
- Each registration request and reply contains an authentication extension that has the following fields:
  - **Type**: This is an 8 bit field that designates the type of authentication extension.
  - **Length**: This is an 8 bit field that identifies the number of bytes in the authenticator.
  - **Security Parameter Index**: This field has 4 bytes and is used to identify the security context between a pair of nodes. The configuration of the security context is made so that the two nodes share the same secret key and parameters relevant to the authentication scheme.
  - **Authenticator**: This field has a code that is inserted by the sender into the message using a shared secret key. The receiver uses the same code to make sure that the message has not been modified. The default authentication scheme is the keyed-MD5 (Message Digest 5) which produces a 128-bit message digest.

7.9 Virtual Private Network (VPN)

- A Virtual Private Network (VPN) connects the components and resources of one network over another network.
- VPNs accomplish this by allowing the user to tunnel through the wireless network or other public network in such a way that the tunnel participants enjoy at least the same level of confidentiality and features as when they are attached to a private wired network.
- A VPN is a group of two or more computer systems connected to a private network, which is built and maintained by the organization for its own use with limited public network access.
- In the remote user application, a VPN provides a secure, dedicated path called a tunnel over an untrusted network.
- A comprehensive VPN requires three main technology components: security, traffic control, and enterprise management.

VPNs provide the following main **advantages**:

- **Security**: By using advanced encryption and authentication schemes, VPNs can secure data from being accessed by hackers and unauthorized users.
- **Scalability**: They enable organizations to use the Internet infrastructure within ISPs and devices in an easy and cost-effective manner. This will enable organizations to add large amounts of capacity without the need to add new significant infrastructure.

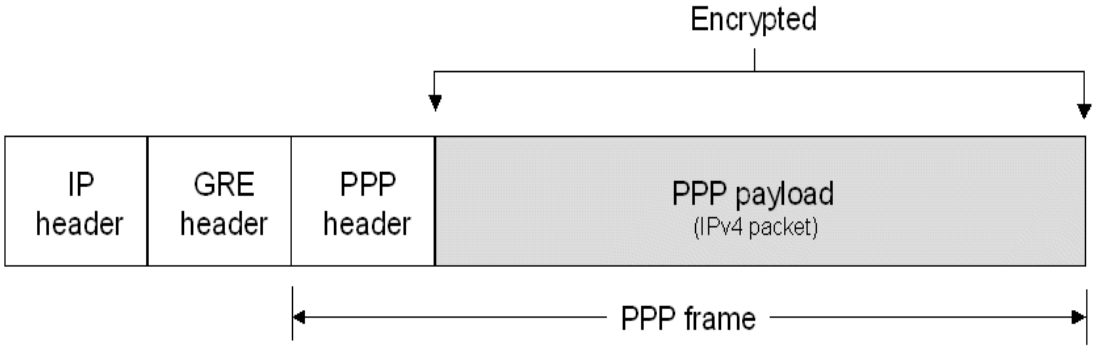
- **Compatibility with broadband technology**: VPN technology allows mobile users and telecommuters to benefit from the high-speed access techniques such as DSL and cable modem, to get access to their organization networks. This provides users with significant flexibility and efficiency. Moreover, such high-speed broadband connections provide a cost-effective solution for connecting remote offices.
- They are currently **deployed on many enterprise networks.**
- They have **low administration** requirements.
- The **traffic to the internal network is isolated** until VPN authentication is performed.
- **WEP key and MAC address list management become optional** since the security measures are created by the VPN channel itself.

The main **drawbacks** of the current VPNs as applied to WLANs are:

- Lack of support for multicasting and roaming between the wireless networks.
- They are not completely transparent since users receive a login dialog when roaming between VPN servers on the network or when a client system resumes from standby mode.

Various tunneling protocols:

1. **Point-to-Point Tunneling Protocol (PPTP)**
   - This protocol is built on the Internet communications protocol called Point to Point Protocol (PPP) and the TCP/IP protocol.
   - PPP offers authentication as well as methods of privacy and compression of data.
   - PPTP allows the PPP session to be tunneled through an existing IP connection. The existing connection can be treated as if it were a telephone line. Therefore, a private network can run over a public network.
   - Tunneling is achieved because PPTP provides encapsulation by wrapping packets of information within IP packets for transmission through the Internet.
   - Upon reception, the external IP packets are stripped away, exposing the original packets for delivery.
   - Encapsulation allows the transport of packets that will not otherwise conform to Internet address standards.
   - Figure shows the main components of the Point-to-Point Tunneling Protocol (PPTP).



   - For data transmission using PPTP, tunneling makes use of two basic packet types: (a) data packets and (b) control packets.
   - Control packets are used strictly for status inquiry and signaling information and are transmitted and received over a TCP connection.

- The data portion is sent using PPP encapsulated in Generic Routing Encapsulation (GRE) protocol.
- GRE protocol provides a way to encapsulate arbitrary data packets within an arbitrary transport protocol.
- Although PPTP did not have any provision for authentication or encryption when it was first developed, it has been enhanced recently to support encryption and authentication methods.

2. Layer-2 Transport Protocol (L2TP)

- Similar to PPTP, L2TP is basically a tunneling protocol and does not include any encryption or authentication mechanism.
- The main difference between PPTP and L2TP is that L2TP combines the data and control channels and runs over the User Datagram Protocol (UDP).
- The latter is faster for sending packets that are commonly used in real-time Internet communication because it does not retransmit lost packets.
- On the other hand, PPTP separates the control stream, which runs over TCP, and the data stream, which runs over GRE.
- Combining these two channels and using high performance UDP makes L2TP more firewall friendly than the PPTP. This is the main advantage as most firewalls do not support GRE.
- In PPP, a connection is tunneled using IP. An L2TP access concentrator is the client end of the connection while an L2TP network server is the server side.
- The PPP packets are encapsulated in an L2TP header that is encapsulated in IP. These IP packets can traverse the network just like ordinary IP datagrams.
- Data transmission in an L2TP can be implemented as a UDP-based IP protocol.
- The packet is first generated at the client computer. This IP packet is sourced from the client computer and destined for the remote network.
- The packet is encapsulated in PPP. This packet is then encapsulated in L2TP.
- UDP header is added to this L2TP packet and is encapsulated in an IP datagram. This IP packet is destined for the Internet Service Provider (ISP) network.
- The IP packets will again be encapsulated at PPP and terminate at the ISP's network authentication server.
- This final heavily encapsulated packet will be sent over the circuit switched layer 2 network.

3. Internet Protocol Security (IPSec)

- IPSec is an open standard that is based on network layer 3 security protocols.
- The latter protects IP datagrams by defining a method of specifying how the traffic is protected and to whom it is sent.
- In order to protect IP datagrams, the IPSec protocol uses either the Encapsulation Security Payload (ESP) or Authentication Header (AH) protocols.
- The data origin authentication ensures that the received data is the same as that sent and the recipient knows who sent the data.
- Data integrity ensures data transmission without alteration while relay protection offers partial sequence integrity.
- Data confidentiality ensures that no one can read the transmitted data which can be possible by using encryption algorithms.

- Integrating L2TP with IPSec offers the ability to use L2TP as a tunneling protocol; however, securing the data is achieved using an IPSec scheme.
- Using L2TP as the tunneling protocol gives the added advantage of increased manageability for end-to-end communications.
- Moreover, L2TP is a widely available standard; therefore the interoperability between vendors is far better than just IPSec alone.
- The same VPN technology can be used to secure wireless systems.
- The Access Points (APs) are configured for open access with no WEP encryption, but wireless access is isolated from the enterprise network by a VPN server and a VLAN between the APs and VPN servers.
- Authentication and full encryption over the wireless network is provided using the VPN servers which also act as gateways to the private network.
- Clearly, a VPN-based solution has the advantage of being scalable for a very large number of users.

7.10 Some Bluetooth Attacks

- **Bluejacking**— temporarily hijacking another person's cell phone by sending it an anonymous text message using Bluetooth wireless networking system.
- **Bluespamming**— sending unsolicited commercial messages.
- **Warchalking**— using chalk to place a special symbol on a sidewalk or other surface that indicates a nearby wireless network, especially one that offers Internet access.
- **Bluestumbling**— randomly searching for hackable Bluetooth devices.
- **Bluesnarfing**— exploiting the object exchange (OBEX) protocol for pairing of two Bluetooth devices and copying e-mail messages, calendars, etc. by the crackers.
- **Bluebugging**— reading data on a Bluetooth enabled cell phone, eavesdropping on conversations and even sending executable commands to the phone to initiate phone calls, sending text messages, connecting to the Internet, and more. •
- **Bluetracking**— tracking people's locations by following the signal of their Bluetooth devices.
- **Bluesnipping**— scanning with a Bluetooth scanning device that looks like a sniper rifle with an antenna instead of a barrel.
- **Man-in-the-Middle Attack**— is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

CHAPTER 8
ECONOMICS OF WIRELESS NETWORKS

8.1 Introduction

- The field of mobile wireless communications is currently one of the fastest growing segmentsof the telecommunications industry.
- Wireless devices have nowadays found extensive use and have become an indispensable tool on the everyday life of many people, both the professionally and personally.
- To gain insight into the momentum of the growth of the wireless industry, it is sufficient to state the tremendous growth in the number of worldwide subscribers of wireless systems.
- With such growth rates, it is just a matter of time before the use of wireless systems surpasses that of wire-line systems.

8.2 Economic Benefits of Wireless Networks

- A wireless network requires minimal cabling or rather no cabling at all, resulting in reasonable cost cutting as there is no need of installing wires or cables.
- In a wireless network, multiple computers and devices within the network range can use the same ISP for using the internet. Users can also sign in at the same time from any location in the range.
- Wireless networks offer a quick and complete use of network capacity. The remaining unused capacity of each wireless access point can be easily used to serve a new subscriber in the range.
- The use of wireless networks also helps in increasing productivity. With the help of a wireless network, employees can be more productive as they can complete their work from any convenient place.
- Wireless networks also increase productivity by reducing unproductive time, improving logistics significantly, allowing a faster and more efficient decision making and empowering small businesses.

8.3 The Changing Economics of the Wireless Industry

- The movement towards integration of wireless networks and the Internet has reached a point which marks a change for the business of the wireless industry.
- The evolution from a voice-oriented to a data-oriented market will be the reason for introduction of new services and revenues as well as major changes in the industry's value chain.
- Furthermore, the wireless industry is likely to move from a vertical integration model to a horizontal integration model.
- ***Vertical integration*** refers to the situation of one or more companies covering the entire range of layers that are needed to offer services to the consumer.
- On the other hand, ***horizontal integration*** follows a layered approach, where the products of multiple companies are needed in order to offer services to the consumers.
- Overall, the trend towards data-oriented wireless systems is expected to change the economics of the wireless industry.
- In the following section, we summarize the main factors affected by this change:

8.3.1 Terminal Manufacturers

8.3.1.1 Movement Towards Internet Appliances

- It is expected that current wireless terminals will be substituted by Internet-enabled ones, such as Internet-enabled pagers, phones, digital assistants, etc.
- Thus, terminal manufacturers will face a new challenge in the design and implementation of their products.
- Whereas today the main target of terminal manufacturers is reduction in size and battery power consumption, in the future the target will also be terminals that support high-speed data services.
- It is likely that terminals will be classified into a number of categories, with each category addressing a different part of the consumer base.
- Thus, terminal categories will possibly be characterized by different device costs and capabilities.

8.3.1.2 Increasing Sales Figures

- Mobile terminals are expected to continue to enjoy a sales increase despite the previously mentioned expectation for a reduction in the growth rate of the customer base.
- This is to be expected, since people are likely to change their terminals every couple of years in order to be able to keep up with the new services offered by mobile carriers.
- This fact already characterizes the mobile industry, with a simple example being the upgrade from a GSM to a GPRS phones in order to be able to use the higher data rates offered by GPRS.
- This evolution towards terminals of higher capabilities will be a challenging task due to the added complexity induced by the extra functionality.

8.3.1.3 Lower Prices

- Mobile terminals will continue to be based on silicon technology.
- This will continue to lower terminal sizes and prices.
- The evolution of silicon-based technology will also result in lower levels of power consumption.
- Thus, average battery lifetime is expected to increase.

8.3.2 Role of Governments

8.3.2.1 Revenue due to Spectrum Licensing

- Governments are actually very interested in the wireless telecommunication market from thepoint of view of economical benefits for themselves.
- This can be seen in the case of 3Gspectrum auctions, which turned out to be very profitable for some governments.
- Such was the case with 3G spectrum auctions in Great Britain, which eventually created revenue of about 40 billion dollars for the British government, ten times more than was expected.
- The fact that governments are likely to get a lot of money through spectrum licensing can be made clearer by stating that, compared to the 40 billion dollar revenue for the British government due to 3G spectrum, the total revenue to all European countries for 2G spectrum was about ten times less.

- The huge prices of 3G spectrum clearly show a difficult competitive environmentfor the mobile carriers.

8.3.2.2 License Use

- Licensing spectrum parts to specific companies does not mean selling the spectrum; rather,the spectrum parts are leased for a certain period of time.
- Different governments lease spectrum for different time periods and some of them also restrict its use to only certain services.
- For example, the Federal Communications Commission (FCC), the national regulatorinside the United States, licenses spectrum to operators without limiting them on thetype of service to deploy over this spectrum.
- On the other hand, the spectrum regulator of the European Union does impose such a limitation. This helps growth of a specific type of standard, an example being the success of GSM in Europe.

8.3.2.3 Governments Can Affect the Market

- Since governments control the way spectrum is used, they can control the number of licenses and thus the number of competing carriers.
- By increasing or decreasing this number, governments can affect the growth rate of the market and the competitiveness of the carriers.
- Finally, another way of affecting the market comes through privatization of telecommunication companies, which is a general trend around the world.

8.3.3 Infrastructure Manufacturers

8.3.3.1 Increased Market Opportunities

- Due to the deployment of the next generations of wireless networks in the near future, theinfrastructure of the mobile market is likely to rapidly increase in size.
- It is estimated thatuntil 2006, this market will grow to a 200 billion dollars, four times the size it had achieved in1999.
- Such conditions obviously promise a bright future for the infrastructure manufacturers.

8.3.3.2 Increased Entry Barriers

- The increased complexity of infrastructure equipment for the next generations of wirelessnetworks and the increased demand for such equipment is likely to favor companies whichalready enjoy a large market share.
- Furthermore, manufacturers of equipment for datanetworks are likely to enter this market.

8.3.4 Mobile Carriers

8.3.4.1 Market Challenges

- The mobile carriers will face the greatest challenges in the new era of the wireless industry.
- They will have to adapt to the reducing growth rates of the subscriber base and the decliningprices.
- Furthermore, mobile carriers will have to adapt to the movement towards the wireless Internet and find ways to make profit from it.

- Of course this also means a risk for carriers, as they will have to spend a lot of money on investments (such as 3G licenses, new infrastructure and equipment, etc.) hoping that the wireless Internet finds the necessary popularity among the subscribers so that the carrier eventually gets its money back.
- This adoption of the wireless Internet as a primary means of revenue means that mobile carriers need to play a number of additional roles in order to stay competitive.
- These additional roles are that of the Internet Service Provider (ISP), the portal, the application service provider and the content provider. These roles are summarized below:

- **The ISP role:** The mobile carriers will have to carefully examine the case of the fixedInternet world. Finally, it should see whether ISPs of the fixed Internet world will enter the wireless Internet arena.
- **The portal role**: Mobile carriers will also have to run their own portals to the wirelessInternet world. In that case, mobile carriers will have the advantage of gaining from the knowledgeand customer base of the successful fixed-Internet portal.
- **The application service provider role:** In the 3G generations and beyond of wireless networks, many new services will appear. Thus, mobile carriers are potential providersof these new services, which may constitute a significant portion of revenue. Examples ofsuch services are location-based services.
- **The content provider role**: Mimicking the world of fixed Internet, mobile carriers will alsohave to prepare content for their portals.

8.3.4.2 Few Carriers

- The cost of the equipment for the rollout of the new services is estimated to be 2–4 times higher than the cost of 2G equipment.
- This means that a reduced number of carriers is likely to characterize each market. This number is estimated to be between two and four carriers for each country's market.
- In cases where a larger number of competitive carriers appear, the chances are that those with the largest subscriber base will probably acquire the biggest part of the market.
- This means that the market is divided between those carriers with obvious advantages to their revenues. Smaller carrier companies obviously will not be able to survive the competition and they will be forced to merge in order to stay competitive.
- Overall, the market for mobile Internet will resemble an oligopoly, with a streak of strategic behavior from competing carrier companies. This means that the prices of products of a company affect those of its competitors.
- In such an environment, companies implicitly come to a common agreement regarding their prices. This kind of agreement is known as self-enforcing, since the competitors abide by it due to the fact that this is in their interest.
- Such a market, where a company chooses its strategy given the strategies of its competitors in order to maximize its profit is said to be in a **Nash equilibrium**.

8.3.4.3 Bundled Products

- In most cases, consumers appear to prefer bundled products.
- Carriers associated with telecomoperators, especially for data services, will have a relative advantage.

8.3.4.4 Changing Traffic Patterns

- Increased intra-country mobility, especially within the European Union where a commonstandard (GSM) is used, increases traffic related to roaming between countries.
- In some smallcountries, traffic due to roaming will actually constitute more than half of the trafficexchanged.

8.3.4.5 Different Situation in each Country

- Due to the different factors that dominate the telecommunications scene and the society of each country, it is difficult to make predictions on successful carriers.
- In the United States, the wireless market is affected by the large distances, lack of spectrum, increased competition, large subscriber base, Internet popularity and a divergence of standards.
- In the European Union, however, the scenario is somewhat different: Internet use is not that widespread, a single standard exists (GSM) and, as mentioned above, roaming traffic is an important part of the total traffic.

8.4 Wireless Data Forecast

- As stated, wireless data will become a significant part of the traffic over future mobilewireless data.
- It is interesting to note the similarity of today' situation regarding the wireless Internet with that of the wired Internet in the early 1990s.
- In those years, Internet was characterized by lower data rates (due to low-speed (up to 9.6 kbps) dial-up modems) and applications far from today's user-friendly ones, such as the inconvenient Mosaic web browser.
- Furthermore, information was available mostly in text format and graphics were of low resolution.
- However, speeds increased (reaching 56 kbps for dial-up and 128 kbps for ISDN)as did usability (an example being the introduction of Netscape's and Internet Explorer'sgraphical interfaces) thus raising the popularity and penetration of the Internet.
- Specifically, it enjoyed a tremendous evolution with traffic per user rising from one MB per month in 1991 to 200 MB per month in 1999.
- A somewhat similar situation with that of the early days of Internet characterizes today's wireless data scene: low data rates, abbreviated user interfaces (e.g. those of

the Short Message Service (SMS) and Wireless Application Protocol (WAP)), text-like output and low-resolution graphics.

- As the capabilities and usability of wireless networks increases, a growth similar to that of fixed Internet will be observed for the wireless Internet as well.

8.4.1 Enabling Applications

A number of capacity-demanding data applications are expected to be used over wirelessnetworks. These will offer compelling value to the consumer and due to their popularity areexpected to increase wireless data traffic. Some of these applications are briefly highlighted below:

- **Video telephony and videoconferencing**: These will be typical mobile multimedia applications. They will offer users the ability to participate in virtual meetings and conferences through their wireless terminals. Moreover, they will offer the ability to access multimedia content, such as CD-quality music and TV-quality video feeds, from service platforms and the Internet.
- **Internet browsing:** This will be a significant application. It will be greatly enabled by the emergence of XML, which will enable internet content to be more accessible by wireless devices without the need to offer web content separately for wireless devices, as is the case with the Wireless Access Protocol (WAP).
- **Mobile commerce**: These will offer the ability to make on-line purchases and reservations upon demand without having to be in front of an Internet-connected PC. Market analystspredict that e-commerce will be a multitrillion dollar industry by 2003. Introducing ecommerceto the mobile platform will be an important source of operator revenues.
- **Multimedia messaging:** These applications will offer support for multimedia-enhancedmessages such as voice mails and notifications, video feeds software applications andmultimedia data files.
- **Geolocation**:Geolocation determines the geographical location of a mobile user. Thereare **two types** of geolocation techniques, one ***based on the handset*** and the ***other on thenetwork***. The first one uses the GPS system to determine user location while in the secondone the replicas of the signals from the same handset at different base stations arecombined in order to determine user location. Some obvious applications employinggeolocation technology include mobile map service and identification of user locationfor emergency calls.

8.4.2 Technological Alternatives and their Economics

There are a number of candidate technologies for offering data transfer in wireless networks. In this section we summarize some of these technologies.

- **cdma2000:** This is a fully backwards-compatible descendant of IS-95 (cdmaOne) utilizing the same 1.25 MHz carrier structure of cdmaOne. Cdma2000 offers both voice and data at rates up to 2 Mbps. It uses two spreading modes, 1X and 3X. The 1X mode uses a single cdmaOne carrier providing average data rates up to 144 kbps, while 3X is a multicarrier system. 1X and 3X are the two modes currently standardized, although modes such as 6X, 9X and 12X may be standardized in the future.

- **High Data Rate (HDR):** This is an enhancement of 1X for data services. HDR uses more modulation, thus offering higher speeds than 1X.
- **Wideband CDMA (WCDMA):** WCDMA introduces a new 5 MHz-wide channel structure, capable of supporting voice and average data at speeds up to 2 Mbps.
- **General Packet Radio Service (GPRS):** GPRS is a packet-switched overlay over 2Gnetworks. Its operation is based on allocation of more slots to a user within a GSMframe. GPRS terminals support a variety of rates, ranging from 14.4 to 115.2 kbps,both in symmetric and asymmetric configurations.

It is estimated that, based on a cost per megabyte scenario, CDMA-based technologieshave an economic advantage over GPRS due to the limited capacity of the latter. Of thecdma-based technologies, HDR is the most advantageous for supporting data traffic, as it hasa two to three times cost advantage over cdma2000 1X and WCDMA. This advantage ofHDR is due to its optimization for data traffic.

8.5 Charging Issues

- A fundamental issue in the wireless market is the way carriers charge their customers.
- Although customers are certainly attracted to new and exciting technologies, most of them will make their choice of carrier based on the charges.
- Thus, it can be seen that charging policies have the potential to greatly impact the success of mobile carriers.

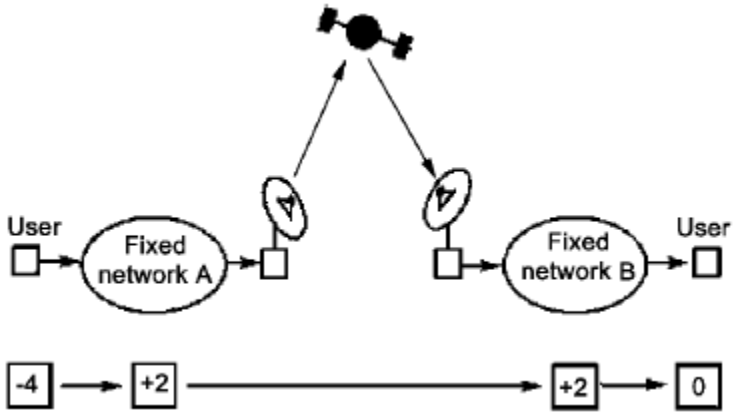


Figure 8.1: Charging on an International Call

- In both fixed and mobile telephony worlds, carriers can send bills only to their owncustomers. This of course means that there must exist a way for users to be charged forcalls terminating at the network of a different carrier.
- In order to illustrate this scenario, Figure 8.1 above shows the charges (in monetary units) when a user of carrier A makes a call to a telephone belonging to a different carrier B.
- It can be seen that the user pays for the usage both of carrier A and B.
- Since most countries originally had only one phone company (typically owned by the government), such a situation arose in international calls trough fixed telephony networks.
- The way the user of a phone company A was charged for making a call to phone Bwas defined through a set of regulations, known as interconnect agreements, between thenational phone companies.
- Obviously, both companies profited from international calls.

- Since the scheme of the interconnect agreements required each carrier to form a separateagreement with every other carrier, the International Telecommunications Organization(ITU) devised the international accounting rate system.
- This actually allowed carriers to charge as much as they wanted for calls terminating on their own network.
- Since charging for this type of service did not affect their own customers, most carriers decided to charge a lot.
- This situation, which resulted in high prices for international calls, began to change in the 1990s, when multiple fixed telephony carriers began to appear within the market of the same country.
- These carriers were interconnected with others of the same country in order to allowusers of competing carriers to call each other.
- The calls between telephones of differentcarriers were charged in a way similar to that presented in Figure 8.1 above.
- Some of these newcarriers also set up connections with carriers of neighboring countries by bypassing theaccounting rate system.
- In order to be competitive, they offered lower charges for internationalcalls and thus prices for such calls began to fall.

8.5.1 Mobility Charges.

- In most cases the price for placing a call through a mobile carrier is significantly higher than that through a fixed telephone carrier. This is because mobile carriers have paid a significant amount of money to acquire spectrum licenses and frequentlyspend large amounts ofmoney installing new infrastructures.
- The actual price for a mobile telephone call is not constant but rather depends on factors including the policy of the carrier, the time at which the call is placed, or the user's contract.
- However, despite the fact that mobile calls cost more than fixed ones, these prices generally follow a declining rate due to the competition between carriers and the concerted effort to make mobile telephony a direct competitor of the traditional fixed telephone carrier.
- Another interesting issue regarding the charges for the case of a user who places a call that ends at the network of a mobile carrier. In this situation, there are two approaches:

  - ***Calling Party Pays (CPP):***This approach, shown in Figure 8.2, is mostly used in European countries. The caller pays for usage of both the fixed and the mobile networks. Thus, calling a mobile phone from a fixed one is more expensive than a call placed between two fixed telephones. In order to provide fairness to the callers, mobile numbers are preceded by special codes, which let the caller know that the charge for such a call will be higher than that for a call to a fixed telephone.

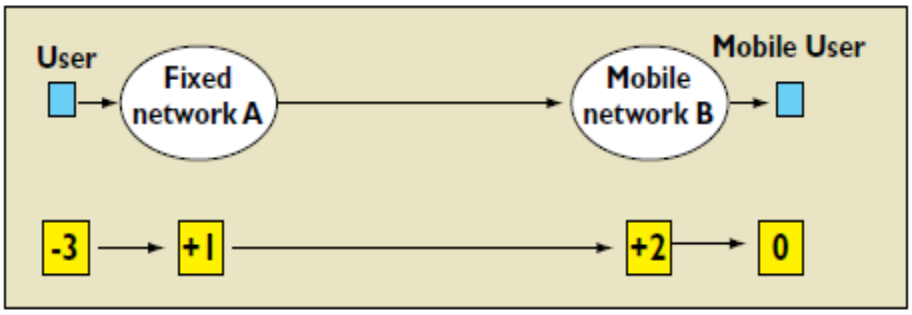


Figure 8.2: CPP Approach

- ***Receiving (called) Party Pays (RPP)*:** This approach, shown in Figure 8.3, is mostly used in the U.S. and Canada. The called party pays for usage of the mobile network. Thus, calling a mobile phone from a fixed phone costs the calling party the same amount of money as when the call is placed between two fixed telephones. This approach is driven by the fact that in the U.S. consumers are accustomed to the situation in which local calls are free, thus paying for a call to a mobile phone in the same area would seem incongruous.

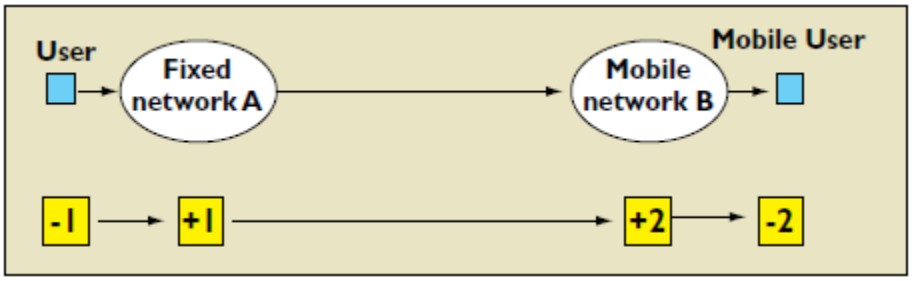


Figure 8.3: RPP Approach

8.5.2 Roaming Charges

- Figure 8.4 shows the case of a call placed from a fixed telephone to a user of a mobile carrier, who has moved to the operating area of mobile carrierlocated in a different country.
- This situation is known as roaming and imposes relatively high charges to the receiving party.

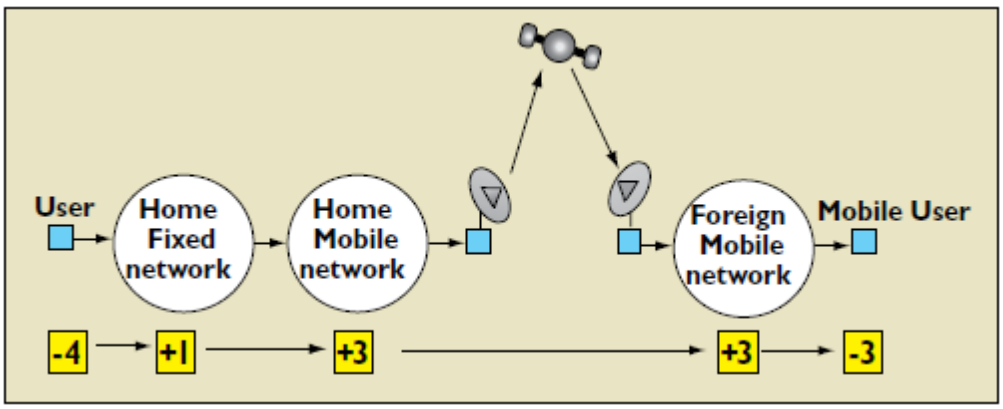


Figure 8.4: Charges for a call placed to a roaming user

- As shown in the figure, an RPP/CPP combination is in effect in roaming situations.

- This is because it would be unfair to charge thecaller for usage of the foreign mobile network since heor she has no way of knowing the called party is roamingto a foreign network.
- Thus, the cost of the call for the calling party is just the sum of the cost of using the fixed network and the cost of using the home mobile network, meaning the charge for the calling party is what it would be if the called party wasn't roaming.
- The extra cost of using the foreign mobile network is charged to the called party.
- This charge is usually much higher than the amount of money is charged to customers of the foreign network, a fact that may make roaming an expensive service**.**

8.5.3 Billing: Contracts vs. Pre-paid Time

- Once the charges for utilizing network resources are summed up, mobile carriers must bill their customers. There exist two main approaches here: contracts and pre-paid billing.
- A ***contract*** is essentially leasing of a connection to the network of the carrier. Users that sign such contracts usually get the mobile handset for free.
- The mobile operators of course eventually get back the cost of the handset, since the contract forces users to pay a monthly rental charge for their connection irrespectiveof the fact that they might not use the connection at all.Of course the user is also charged for both calls.
- Contracts have the disadvantage of limiting the userto a specific carrier for a certain amount of time. Thus,another approach appeared; that of "***pre-paid***" time. Thisapproach, first applied by Telecom Portugal (TMN) in1995, requires users pay in advance for both their handsetsand the calls they make.
- Handsets can be boughtfrom electronics stores and usually include a certainamount of credits, which translate into speaking time(and obviously credits for using other network services,such as SMS).
- Once the user of the phone has exhaustedall the credits, the phone can be recharged via a simpleprocedure. The pre-paid approach has found wide acceptancein Europe and developing countries.

The **advantages of the prepaid approach** are that:

- since no monthly charged is employed, customers have greater control of their costs,
- from the operators point of view prepaying is beneficial since they get their money inadvance and are not burdened with the overhead and cost of producing bills for prepaidcustomers,
- prepaid is beneficial for users who would otherwise not have a credit rating sufficient to qualify for a contract mobile subscription. Such an example is the case of Australia, where the introduction of prepaid mobile services gave access to a very large number of people. These people would otherwise not have access to mobile services due to the fact that they could not meet the credit checks. This accounts for about 40% of all the people that want a mobile phone in Australia.

8.5.4 Charging

There are four main motivations for charging in mobile wireless networks. These are brieflyhighlighted below:

1. Recovery of the investment in infrastructure equipment.
2. Generation of profit for the mobile operators and service providers.

3. Controlling network congestion by providing service levels of different prices.
4. For the case of noncommercial organizations, such as schools and universities, congestion control through a charging scheme is used for social reasons. In this case, charging may be based on ‘tokens’ and thus not reflected in monetary terms.

- Charging methods largely depend on the structure of the network.
- The majority of wireless networks until the 3G era were primarily designed for voice traffic and are thus of a circuit-switched network.
- Nevertheless, the movement towards the next generation of wireless networks is towards a packet-switched network.
- In a circuit-switched network, a dedicated path is assigned between the communicating sides for the entire duration of the connection.
- Of course, the entire capacity of a link is not necessarily dedicated to a single connection butcan rather be time or frequency-multiplexed in order to serve more connections.
- Circuit switching introduces some overhead for link establishment; however, after this takes place, the delay incurred by switching nodes is insignificant.
- Thus, circuit switching can support isochronous services such as voice, which is the primary reason that circuit switching has been widely utilized in earlier cellular systems.
- However, circuit switching is efficient for data traffic; since in such cases the circuit will be idle most of the time.
- Packet switching solves this problem by routing packets between the communicating parties with each packet following a possibly different path.
- Each packet carries a control header, which contains information that the network needs to deliver the packet to its destination.
- In each switching node, incoming packets are stored and the node has to pick up one of its neighbors to hand it the packet.
- This decision entails a number of factors, such as cost, congestion, QoS, etc., and depends on the routing algorithm used.
- A benefit of using packet switching for data services is that bandwidth is used more efficiently, since links are not occupied during idle periods. Furthermore, in a packet-switched network, priorities can be used.

8.5.4.1 Charging Methods

Here, we describe some methodsfor charging in mobile networks. Most ofthese methods have already been proposed for theInternet, but are equally applicable to mobile networks.

1. ***Metered Charging***: The model charges the subscriber with a monthly fee irrespective of the time spent using the network services. However, most of the time this fee also includes some “free” time of network use. When users have spent this time, they are charged for the extra time using the network. This method is used in 2G networks for charging voice traffic. The way to charge voice calls is quite straightforward: The duration of the call is proportional to the call’s cost. Nevertheless, sometimes charges decrease for increased network usage. Metered charging is well suited to voice calls, which are typically circuit-switched, since the user pays for the period of time the circuit is used. Furthermore, it adds little network overhead and is transparent to customers since it does not require configuration in their devices. However, this

model is not suitable for charging the data services expected to be offered by the wireless Internet.

2. ***Packet Charging***: This method is used for charging in packet-switching networks. It is more suitable for data than metered charging. This is because the user is not charged based on time but rather on the number of packets exchanged with the network. Thus, this method obviously calls for a system able to efficiently count the number of packets belonging to a specific user and produce bills based on these measurements. The disadvantage of packet charging is the fact that its implementation might be difficult and thus costly, since the cost of counting packets for each user might increase the complexity to the network. However, the overhead to subscribers remains minimal as the method is transparent to them.

3. ***Expected Capacity Charging:*** This method involves an agreement between the user and the carrier regarding the amount of network capacity that will be received by the user in case of network congestion; and a charge for that level of service. However, users are not necessarily restricted to the agreed capacity. In cases of low network congestion, a user might receive a higher capacity than the agreed one without additional charge. Nevertheless, the network monitors each user's excess traffic and when congestion is experienced, this traffic is either rejected or charged for. The advantage of this method is that it enables mobile carriers to achieve more stable long-term capacity planning for their networks. Expected capacity charging is less complex than packet charging both in terms of network and subscriber overhead.

4. ***Paris-Metro Charging****:* In this method, the network provides different traffic classes, with each class being characterized by different capabilities (such as capacity) and hence a different charge. Thus, users can assign traffic classes to their different applications based on the desired performance/cost ratio. Switching between traffic classes might also be initiated by the network itself in order to provide self-adaptivity. Paris-Metro charging is useful for providing network traffic prioritization in wireless data networks. Another advantage of the method is that it provides customers with the ability to control the cost of their network connections. The disadvantages of this method are an increase in the mathematical complexity of the network's behavior and thus cost of implementation and the fact that users must be familiar with the process of assigning traffic classes to their connections, which introduces some overhead for them.

5. ***Market-based reservation charging***: This method entails an auctioning procedure for acquiring network resources. Users place monetary bids and based on these bids the network assigns appropriate connections to users. An advantage of this method is the fact that users are in control of the quality of service they receive from the network. For example, business users will be more likely to accept a higher charge for their connections than customers that use the network for recreational activities. However, the disadvantages of this method are that (a) due to the bidding procedure, customers are never sure regarding the quality of service they receive from the network, (b) the auctioning approach adds to network overhead, (c) users must make bids, thus the method is not transparent to them and familiarization with it is required. Furthermore, market-based reservation charging raises the issue of unfairness since some customers

may not be able to receive the desired performance. It is generally agreed that this method is not suitable for the wireless Internet.

Table below summarizes some characteristics of the above charging methods:

Charging Method	Implementation Cost	Network Overhead	Transparence to Customers
Metered Charging	Medium-High	Low	Low
Packet Charging	High	High	High
Expected Capacity Charging	Medium-High	Medium	Medium
Paris-Metro Charging	Medium	High	Low
Market-based Reservation Charging	Medium-High	High	Low

8.5.4.2 Content-based Charging

A different approach to the problem of how to charge a customer for utilizing the network iscontent-based charging. The novelty of this approach is that users are not charged based onusage, but rather on the type of content they access. Some examples of the significance ofcontent-based charging follow:

- Content-based charging has been applied in Japan by NTT DoCoMo and experienceshowed that customers are willing to pay extra for certain simple services such as stockquote information.
- Another example is the case of the Short Message Service (SMS): since this serviceconsumes extremely few network resources, it is a significant point of revenue for operatorsdue to the facts that (a) the price of an SMS message is around 0.1 dollar and (b) SMSis a very popular service.
- Another example is that of on-line games through the wireless Internet. Although such applications are both popular and impressive, they require little amount of information exchange between terminals, since graphic display is local to the devices. Thus, the traffic exchanged between devices conveys only game-state information (such as player positions and ball trajectory in sports games) and perhaps instant-messages exchanged between the players. It is obvious that for such an application, users would easily accept a charge significantly higher than that corresponding to the amount of exchanged traffic. The usefulness of this fact to both operators and application providers is obvious.

8.6 Comparison of CDMA 2000 and W-CDMA.

Major differences between WCDMA (3GPP) & CDMA2000 (3GPP2) standards for CDMA-based 3G implementations:

Parameter	**WCDMA**	**CMDA2000**
Carrier Spacing : spacing between CDMA operators to obtain channel protection	5 MHz	3.75 MHz
Chip Rate : number of DSSS pulses per second; a chip is a pulse of DSSS code	4.096 MHz	3.68 MHz
Spreading Factor : SF=(Chip Rate)/(Data Rate)	Higher	Lower
Power Control Frequency : the output power of the transmitter is controlled by itself at this frequency	1500 Hz	800 Hz
Frame Duration: the time duration of a frame; between beginning and end of the frame.	10 ms	20 ms (also uses 5, 30, 40 ms frames)
Base Stations: base stations may or may not need synchronous timings	Asynchronous	Synchronous
Forward Link Pilot: The pilot is a channel modulated only by the PN (Pseudo Noise) spreading codes	TDM, Dedicated pilot	CDM, Common Pilot
Antenna Beam Forming: used for directional signal transmission & reception	TDM, Dedicated pilot	Auxiliary pilot