MOBILE COMPUTING

UNIT-I INTRODUCTION : Mobile and Wireless Devices – Simplified Reference Model – Need for Mobile Computing – Wireless Transmissions – Multiplexing – Spread Spectrum and Cellular Systems – Medium Access Control – Comparisons.

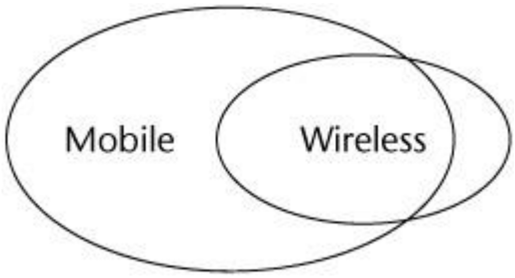
INTRODUCTION

Mobile Computing describes the application of small, portable, wireless computing and communication devices, which is used when mobile is changing its location. It requires wireless network to support outdoor mobility and handover from one network to another network. Challenges of the mobile computing are mobility context aware applications, naming and locating, routing data and messages, reliability in the presence of disconnection, data management, transaction models, security and seamless mobility. The traditional mobile computing research focuses on user, mobile device, interface design, authentication, innovative applications, security, improve the performance, software defined radio, mobile infrastructure, integration and wired with wireless systems internetworking. It supports seamless mobility, Quality of Service (QoS), modeling analysis, mobile agents, ad-hoc networks and wireless test beds for technology evaluation.

Definition of Mobile and Wireless:

The definition of mobile and wireless varies from person to person and organization to organization. In many cases, the terms mobile and wireless are used interchangeably, even though they are two different things. Let's start with the term mobile. Mobile is the ability to be on the move. A mobile device is anything that can be used on the move, ranging from laptops to mobile phones. As long as location is not fixed, it is considered mobile. Areas that are not included in our definition of mobile include remote offices, home offices, or home appliances. While these are definitely remote, they are not considered mobile.

Wireless refers to the transmission of voice and data over radio waves. It allows workers to communicate with enterprise data without requiring a physical connection to the network. Wireless devices include anything that uses a wireless network to either send or receive data. The wireless network itself can be accessed from mobile workers, as well as in fixed locations. Figure 1.1 depicts the relationship between mobile and wireless. As you can see, in most cases, wireless is a subset of mobile; but in many cases, an application can be mobile without being wireless.



Relationship between mobile and wireless.

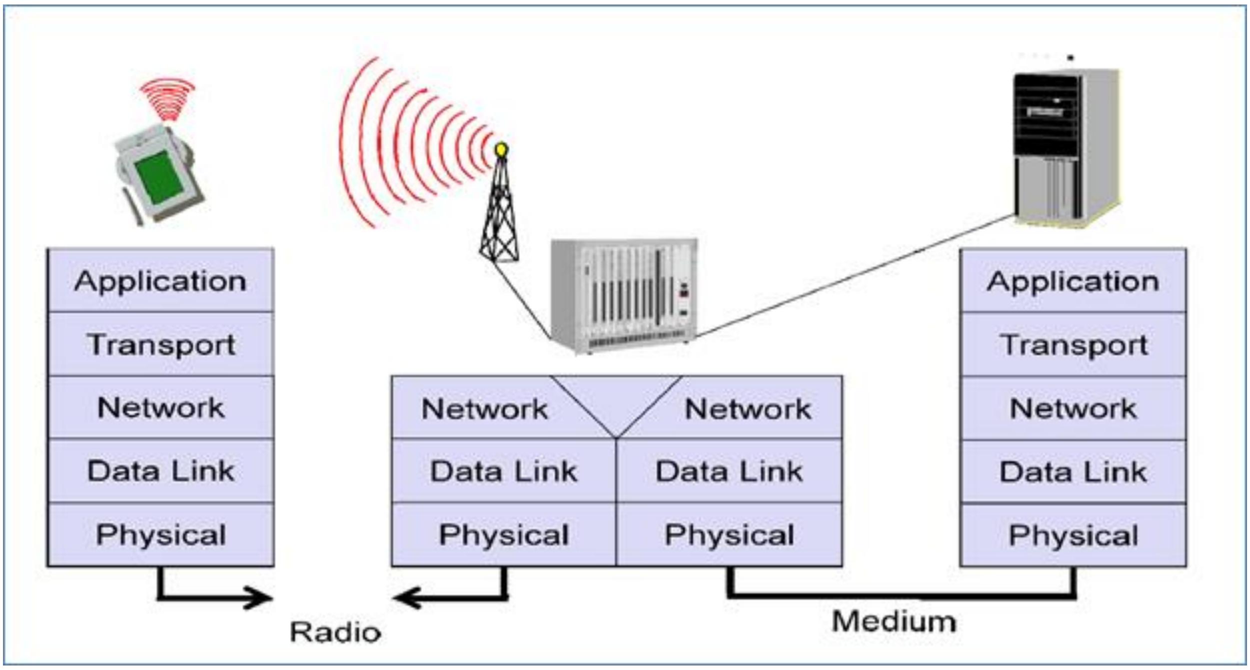
For an application to be considered mobile or wireless, it must be tailored to the characteristics of the device that it runs on. Limited resources, low network bandwidth, and intermittent connectivity all factor into the proper design of these applications.

Wireless applications that are not mobile use fixed wireless networks. These are wireless networks that provide network access in a fixed environment. An example is a wireless local area network (WLAN) that is used to give desktops network access. Many businesses as well as home users are installing WLAN technology to avoid having to install network cables throughout their buildings. Another example is network access via satellites in remote locations where there are no other connectivity options.

On the other side, we have mobile applications that are not wireless. There are many examples where this is the case. Any application that can be used on the move and that does not have wireless connectivity fits into this category. This includes many laptop and personal digital assistant (PDA) applications. Until only a few years ago, it was actually rare to have wireless data access for mobile devices. For these mobile applications, data is often synchronized using a fixed connection and stored on the device for use at a later time. It is worthwhile to note that even though these applications do not require wireless connectivity, they can often benefit from it when it is available. A sizeable portion of this book is dedicated to looking at these types of applications, which are referred to as smart client applications.

Now that we have defined mobile and wireless, it is time to look at some of the areas in which mobile applications are being deployed. Similar to the terms mobile and wireless, there is often confusion around the terms m-commerce and m-business.

Simplified Reference Model of Communication:



The above figure shows a personal digital assistant (PDA) which provides an example for a wireless and portable device. This Personal digital assistant communicates with a base station in the middle of the picture. The base station consists of a radio transceiver (receiver and sender) and an interworking unit connecting the wireless link with the fixed link. The communication partner of the Personal Digital Assistant, a conventional computer, is shown on the right hand side. Under earth each network element (such as PDA, interworking unit, computer), the figure shows the protocol stack implemented in the system according to the reference model.

End-systems, such as PDA and computer in the example, need a full protocol stack comprising the application layer, transport layer, network layer, data link layer and physical layer. Applications on the end-systems communicate with each other using the services of the lower layer.

Intermediate systems such as interworking unit; do not necessarily need all of the layers. Above figure shows the network, data link and physical layers. As (according to the reference model) only entities at the same level communicate with each other (i.e. transport with transport, network with network).

Influence of mobile communication to the layer model

Layers	Key points
Application layer	○ service location ○ new applications, multimedia ○ adaptive applications
Transport layer	○ congestion and flow control ○ quality of service
Network layer	○ addressing, routing, device location ○ hand-over
Data link layer	○ authentication ○ media access ○ multiplexing ○ media access control
Physical layer	○ encrption ○ modulation ○ interference ○ attenuation ○ frequency

Physical layer

This is the lowest layer in a communication system and is responsible for the conversion of a stream of bits into signals that are transmitted on the sender side. The physical layer of the receiver transforms the signals back into a bit stream. For wireless communication, the physical layer is responsible for generation of the carrier frequency, frequency selection, signal detection (although heavy interference may disturb the signal), modulation of data into a carrier frequency and encryption.

Data link layer

The main tasks of the data link layer include accessing the medium, multiplexing of different data streams, correction of transmission errors and synchronization (i.e. detection of a data frame). In short, the data link layer is responsible for a reliable point to point connection between two devices or a point to multipoint connection between one sender and several receivers.

Network layer

The third layer which is called network layer is responsible for routing packets through network or establishing a connection between two entities over many other intermediate systems. Some topics are addressing, routing, device location, and handover between different networks. The several solutions for the network layer protocol of the internet (the Internet Protocol IP).

Transport layer

Transport layer is used in the reference model to establish an end to end connection. Topics like quality of service, flow and congestion control are relevant, especially if the transport protocols known from the internet, TCP and UDP, are to be used over a wireless link.

Application layer

The applications (complemented by additional layers that can support applications) are situated on top of all transmission oriented layers. Some context on this layer are service location, support for multimedia applications, adaptive applications that can handle the variations in transmission characteristics, and wireless access to the World Wide Web using a portable device. Most demanding applications are video (high data rate) and interactive gaming (low jitter, low latency).

Need for mobile computing:

Mobile computing has changed the complete landscape of our day-to-day life. Following are the major advantages of Mobile Computing −

Location Flexibility

This has enabled users to work from anywhere as long as there is a connection established. A user can work without being in a fixed position. Their mobility ensures that they are able to carry out numerous tasks at the same time and perform their stated jobs.

Saves Time

The time consumed or wasted while travelling from different locations or to the office and back, has been slashed. One can now access all the important documents and files over a secure channel or portal and work as if they were on their computer. It has enhanced telecommuting in many companies. It has also reduced unnecessary incurred expenses.

Enhanced Productivity

Users can work efficiently and effectively from whichever location they find comfortable. This in turn enhances their productivity level.

Ease of Research

Research has been made easier, since users earlier were required to go to the field and search for facts and feed them back into the system. It has also made it easier for field officers and researchers to collect and feed data from wherever they are without making unnecessary trips to and from the office to the field.

Entertainment

Video and audio recordings can now be streamed on-the-go using mobile computing. It's easy to access a wide variety of movies, educational and informative material. With the improvement and availability of high speed data connections at considerable cost, one is able to get all the entertainment they want as they browse the internet for streamed data. One is able to watch news, movies, and documentaries among other entertainment offers over the internet. This was not possible before mobile computing dawned on the computing world.

Streamlining of Business Processes

Business processes are now easily available through secured connections. Looking into security issues, adequate measures have been put in place to ensure authentication and authorization of the user accessing the services.

Some business functions can be run over secure links and sharing of information between business partners can also take place.

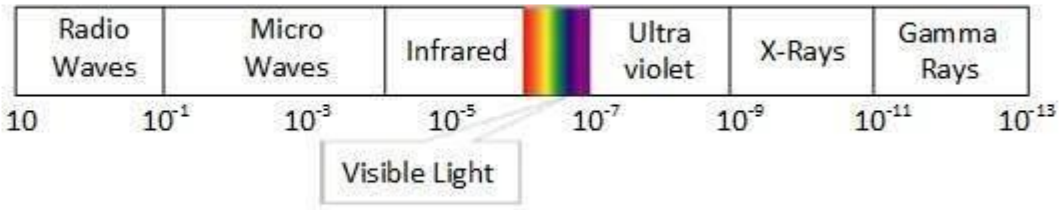
Meetings, seminars and other informative services can be conducted using video and voice conferencing. Travel time and expenditure is also considerably reduced.

Wireless transmission

Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the air and are received and interpreted by appropriate antennas.

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

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

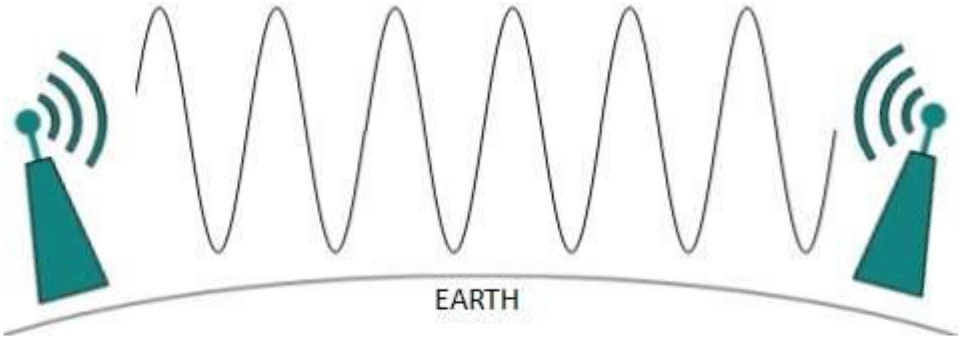


Radio Transmission

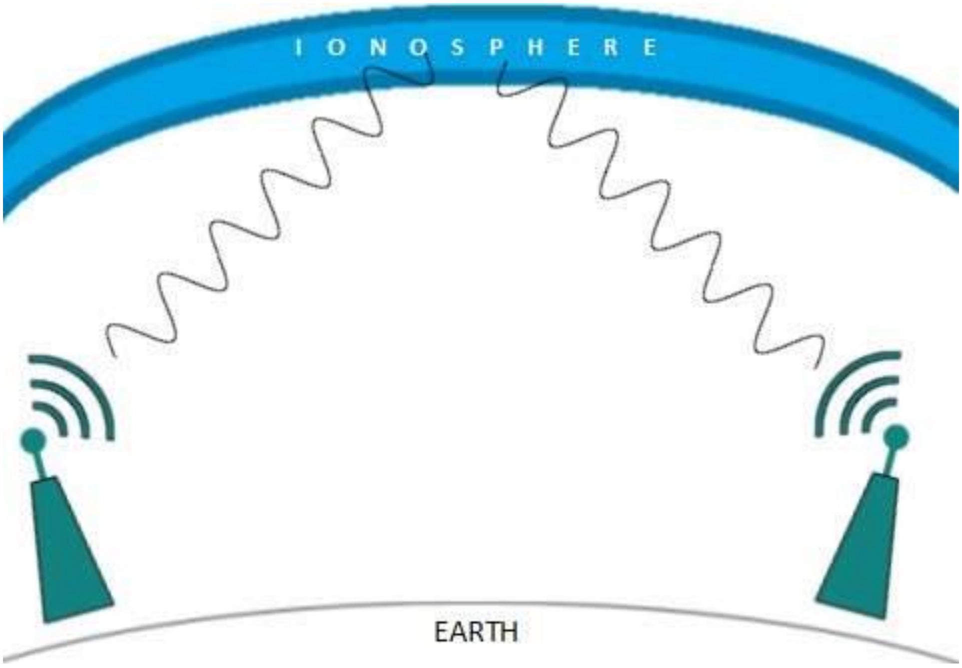
Radio frequency is easier to generate and because of its large wavelength it can penetrate through walls and structures alike.Radio waves can have wavelength from 1 mm – 100,000 km and have frequency ranging from 3 Hz (Extremely Low Frequency) to 300 GHz (Extremely High Frequency). Radio frequencies are sub-divided into six bands.

Radio waves at lower frequencies can travel through walls whereas higher RF can travel in straight line and bounce back.The power of low frequency waves decreases sharply as they cover long distance. High frequency radio waves have more power.

Lower frequencies such as VLF, LF, MF bands can travel on the ground up to 1000 kilometers, over the earth's surface.



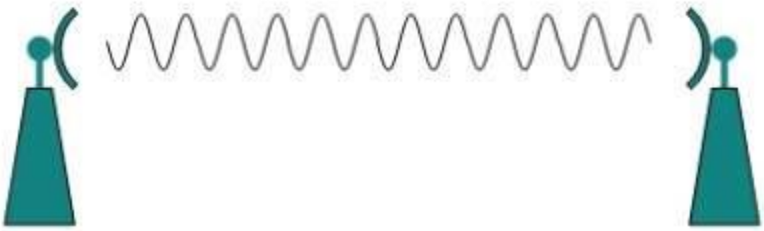
Radio waves of high frequencies are prone to be absorbed by rain and other obstacles. They use Ionosphere of earth atmosphere. High frequency radio waves such as HF and VHF bands are spread upwards. When they reach Ionosphere, they are refracted back to the earth.



Microwave Transmission

Electromagnetic waves above 100 MHz tend to travel in a straight line and signals over them can be sent by beaming those waves towards one particular station. Because Microwaves travels in straight lines, both sender and receiver must be aligned to be strictly in line-of-sight.

Microwaves can have wavelength ranging from 1 mm – 1 meter and frequency ranging from 300 MHz to 300 GHz.



Microwave antennas concentrate the waves making a beam of it. As shown in picture above, multiple antennas can be aligned to reach farther. Microwaves have higher frequencies and do not penetrate wall like obstacles.

Microwave transmission depends highly upon the weather conditions and the frequency it is using.

Infrared Transmission

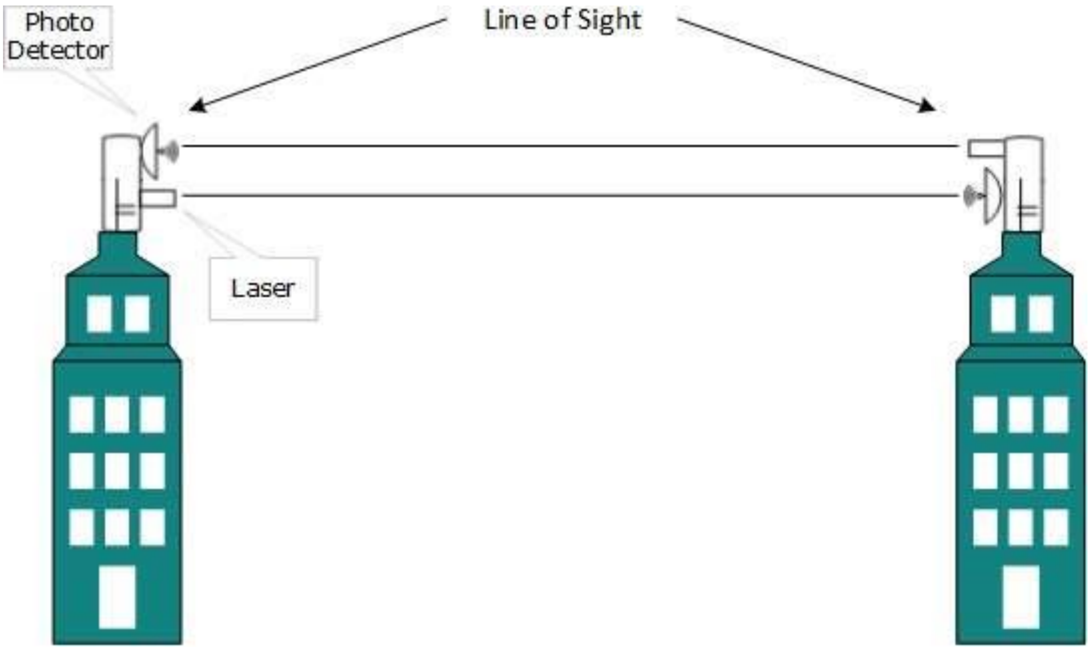
Infrared wave lies in between visible light spectrum and microwaves. It has wavelength of 700-nm to 1-mm and frequency ranges from 300-GHz to 430-THz.

Infrared wave is used for very short range communication purposes such as television and it’s remote. Infrared travels in a straight line hence it is directional by nature. Because of high frequency range, Infrared cannot cross wall-like obstacles.

Light Transmission

Highest most electromagnetic spectrum which can be used for data transmission is light or optical signaling. This is achieved by means of LASER.

Because of frequency light uses, it tends to travel strictly in straight line.Hence the sender and receiver must be in the line-of-sight. Because laser transmission is unidirectional, at both ends of communication the laser and the photo-detector needs to be installed. Laser beam is generally 1mm wide hence it is a work of precision to align two far receptors each pointing to lasers source.



Laser works as Tx (transmitter) and photo-detectors works as Rx (receiver).

Lasers cannot penetrate obstacles such as walls, rain, and thick fog. Additionally, laser beam is distorted by wind, atmosphere temperature, or variation in temperature in the path.

Laser is safe for data transmission as it is very difficult to tap 1mm wide laser without interrupting the communication channel.

Multiplexing

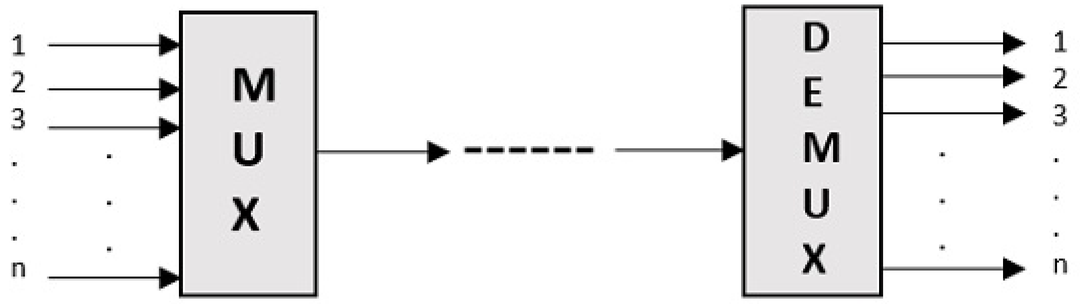
Multiplexing is the process of combining multiple signals into one signal, over a shared medium.

- The process is called as analog multiplexing if these signals are analog in nature.
- If digital signals are multiplexed, it is called as digital multiplexing.

Multiplexing was first developed in telephony. A number of signals were combined to send through a single cable. The process of multiplexing divides a communication channel into several number of logical channels, allotting each one for a different message signal or a data stream to be transferred. The device that does multiplexing, can be called as a MUX.

The reverse process, i.e., extracting the number of channels from one, which is done at the receiver is called as demultiplexing. The device which does demultiplexing is called as DEMUX.

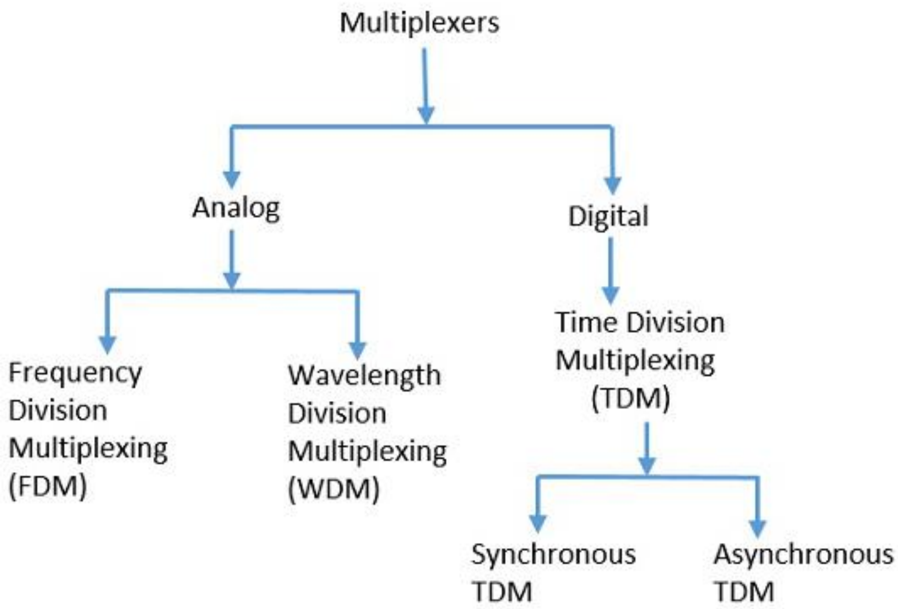
The following figures illustrates the concept of MUX and DEMUX. Their primary use is in the field of communications.



Multiplexing and Demultiplexing

Types of Multiplexers

There are mainly two types of multiplexers, namely analog and digital. They are further divided into FDM, WDM, and TDM. The following figure gives a detailed idea about this classification.



There are many types of multiplexing techniques. Of them all, we have the main types with general classification, mentioned in the above figure. Let us take a look at them individually.

Analog Multiplexing

The analog multiplexing techniques involve signals which are analog in nature. The analog signals are multiplexed according to their frequency (FDM) or wavelength (WDM).

Frequency Division Multiplexing

In analog multiplexing, the most used technique is Frequency Division Multiplexing (FDM). This technique uses various frequencies to combine streams of data, for sending them on a communication medium, as a single signal.

Example − A traditional television transmitter, which sends a number of channels through a single cable uses FDM.

Wavelength Division Multiplexing

Wavelength Division multiplexing (WDM) is an analog technique, in which many data streams of different wavelengths are transmitted in the light spectrum. If the wavelength increases, the frequency of the signal decreases. A prism which can turn different wavelengths into a single line, can be used at the output of MUX and input of DEMUX.

Example − Optical fiber Communications use the WDM technique, to merge different wavelengths into a single light for the communication.

Digital Multiplexing

The term digital represents the discrete bits of information. Hence, the available data is in the form of frames or packets, which are discrete.

Time Division Multiplexing (TDM)

In TDM, the time frame is divided into slots. This technique is used to transmit a signal over a single communication channel, by allotting one slot for each message.

Of all the types of TDM, the main ones are Synchronous and Asynchronous TDM.

Synchronous TDM

In Synchronous TDM, the input is connected to a frame. If there are ‘n’ number of connections, then the frame is divided into ‘n’ time slots. One slot is allocated for each input line.

In this technique, the sampling rate is common for all signals and hence the same clock input is given. The MUX allocates the same slot to each device at all times.

Asynchronous TDM

In Asynchronous TDM, the sampling rate is different for each of the signals and a common clock is not required. If the allotted device, for a time slot transmits nothing and sits idle, then that slot is allotted to another device, unlike synchronous.

This type of TDM is used in Asynchronous transfer mode networks.

Demultiplexer

Demultiplexers are used to connect a single source to multiple destinations. This process is the reverse of multiplexing. As mentioned previously, it is used mostly at the receivers. DEMUX has many applications. It is used in receivers in the communication systems. It is used in arithmetic and logical unit in computers to supply power and to pass on communication, etc.

Demultiplexers are used as serial to parallel converters. The serial data is given as input to DEMUX at regular interval and a counter is attached to it to control the output of the demultiplexer.

Both the multiplexers and demultiplexers play an important role in communication systems, both at the transmitter and receiver sections.

Medium Access Control

(MAC) address is a hardware address use to uniquely identify each node of a network. It provides addressing and channel access control mechanisms to enable the several terminals or network nodes to communicate in a specified network. Medium Access Control of data communication protocol is also named as Media Access Control. In IEEE 802 OSI Reference model of computer networking, the Data Link Control (DLC) layer is subdivided into two sub-layers:

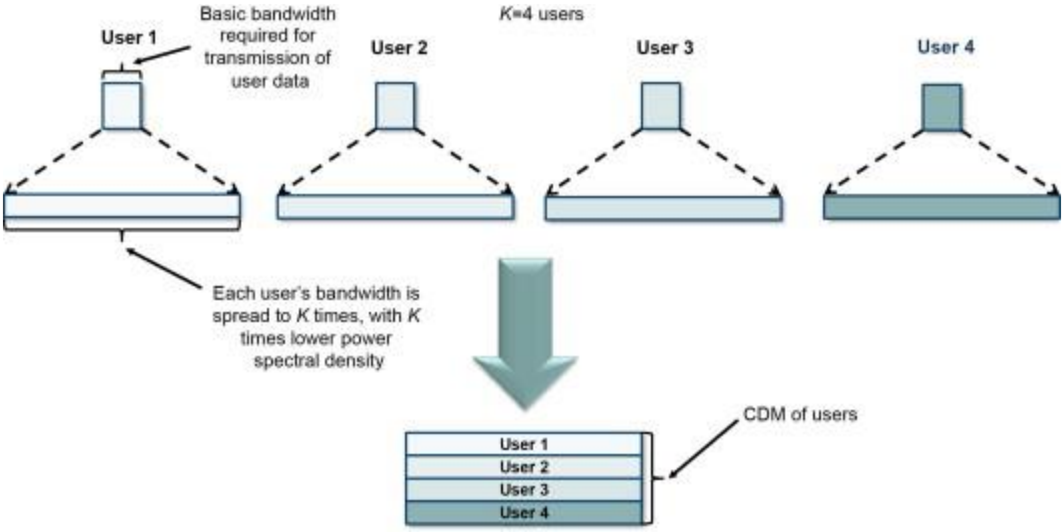
- The Logical Link Control (LLC) layer and
- The Medium Access Control (MAC) layer

The MAC sublayer acts as a direct interface between the logical link control (LLC) Ethernet sublayer and the physical layer of reference model. Consequently, each different type of network medium requires a different MAC layer. On networks that don't conform they are part of IEEE 802 standards but they do conform that they participate OSI Reference Model then the node address is named the Data Link Control (DLC) address. The MAC sublayer emulates a full-duplex logical communication channel in a multipoint network system. These communication channels may provide unicast, multicast and/or broadcast communication services.

Spread Spectrum and Cellular Systems:

A spread spectrum communications system is one that is built upon the principle of transmitting information signals over a much wider bandwidth than is strictly necessary for transferring the information. By transmitting over a larger bandwidth, robustness against external narrowband interference is increased, since the wider the bandwidth of any transmitted signal the lower will be the relative influence of interference over a small part of the bandwidth. Although from a single-link point of view, spread spectrum transmission may seem like very inefficient use of spectrum, this is not the case on a system level as spread spectrum techniques allow for simultaneous multiplexing of multiple transmissions in the same bandwidth.

Thus, if transmissions to/from K users are multiplexed using K times the bandwidth that would be required without spreading, then the bandwidth utilization is not compromised.Furthermore, if the number K of users varies, the spreading applied to each individual user can be varied in such a manner as to ensure that all users are served while bandwidth utilization is maintained.

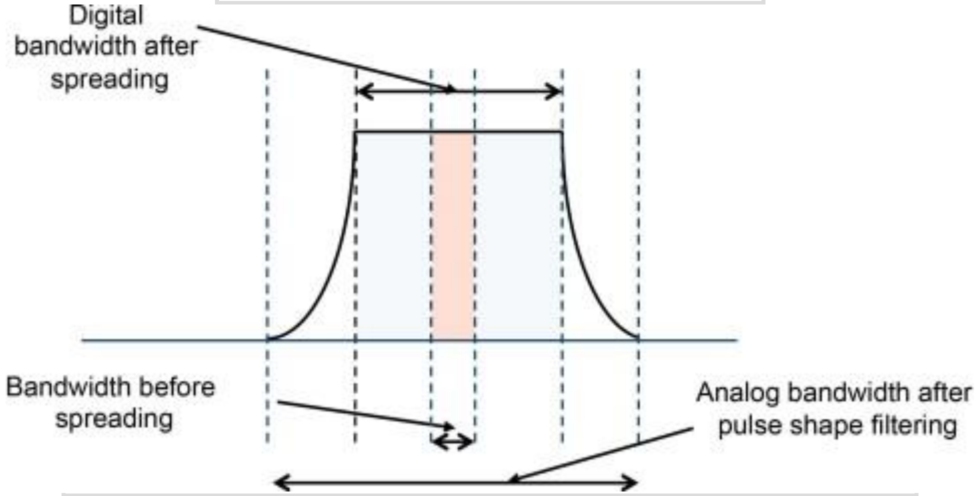


The principle of spread spectrum based user multiplexing.

A variety of spread spectrum techniques exist, such as *Frequency Hopping Spread Spectrum* (FHSS) and *Direct Sequence Spread Spectrum* (DSSS). The focus of this chapter is on DSSS.

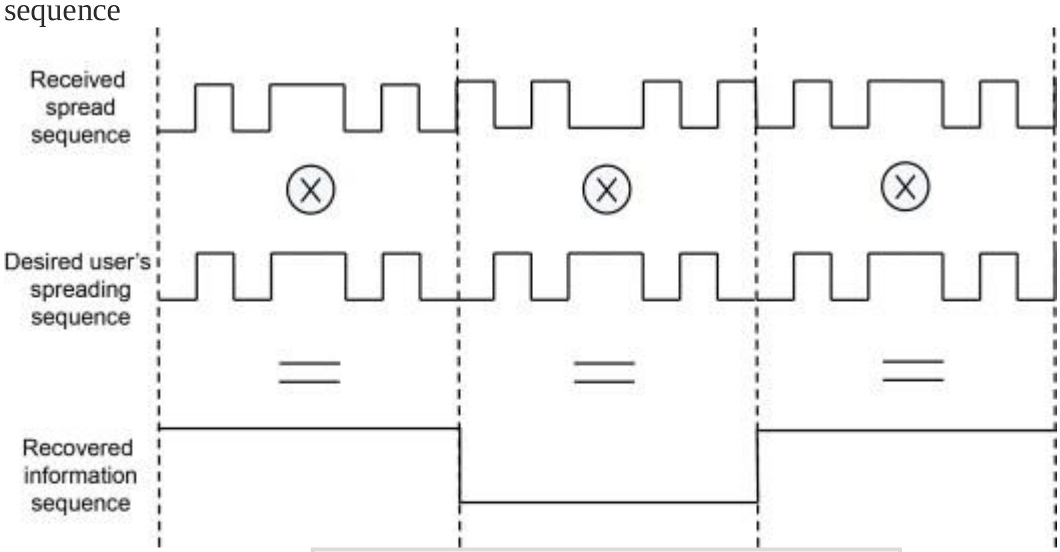
Consider an information sequence coded/modulated into a sequence of N modulation symbols. In order to spread the sequence using DSSS, an M-chip-long spreading sequence is selected. The M chips of the spreading sequence are replicated N times, with each of the replications being multiplied by one of the N symbols.The symbols of this spread sequence are referred to as “chips.” The resulting sequence of $N \times M$ chips must be transmitted within the same time as the original N symbol message in order to maintain the data rate. In the frequency domain, this implies an increase in the occupied spectrum for the signal of M times. Hence, M is referred to as the “spreading factor.” In practice, a pulse-shaping filter is then applied, such as a *root raised cosine* (RRC) filter. The overall occupied bandwidth of the transmitted signal is somewhat larger than M times the bandwidth of the information sequence.

Spreading of an information sequence.



The impact of pulse shape filtering to the occupied bandwidth.

In the absence of other types of channel effects, the receiver can detect the information sequence by means of a synchronized correlation of the spreading sequence with the received sequence



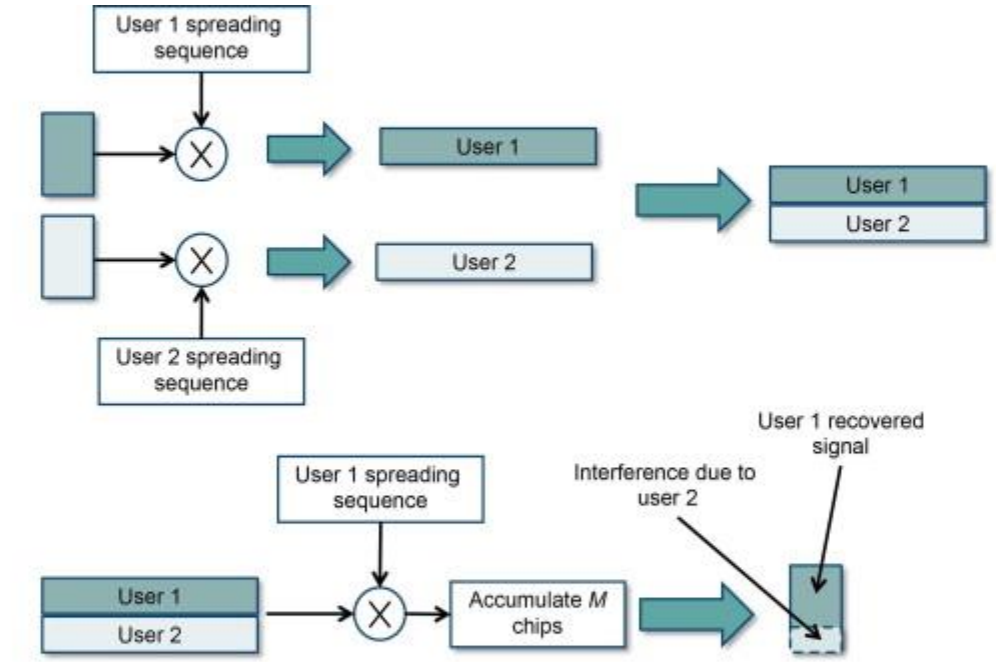
Simple despreading of a spread sequence.

The spreading sequence may in principle be a sequence of random chips. If this is the case, then transmissions to/from different users may be assigned different random sequences. In order to detect a sequence transmitted to or from a particular user, the total received signal, which will consist of aggregation of all users' sequences, can be correlated with the users' spreading code at the receiver side.

In this case, the target user's signal will experience a combining gain across the M chips, whereas the other users' signals will not and hence appear as uncorrelated noise. This combining gain is referred to as spreading gain. This principle is illustrated in Figure 3.5. In Figure 3.5a, two users' signals are spread with different random sequences and combined. In Figure 3.5b, the combined signal is correlated (that is, multiplied and accumulated) with the same random sequence used for the first user. In this case, the first user's signal is recovered with a (power) gain factor of M, whereas the multiplication of the second user's sequence with the first user's random spreading sequence results in a further random sequence with no gain factor.

(a)

(b)



Pseudo-noise (PN) code based spreading (a) and despreading (b).

In the following paragraphs, a situation in which two users have information to transmit is considered, in order to simplify the discussion and equations. The discussion may, however, be generalized to consider any number of users.

Spreading of a single modulation symbol is equivalent to

(3.1)S(k)=s1c1(k)+s2c2(k), k=1,…,M,

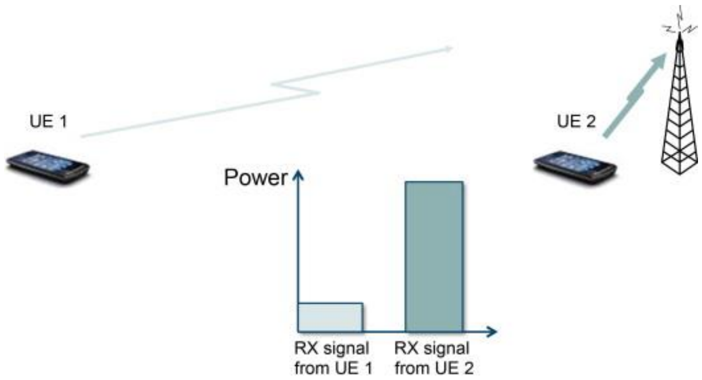
where s_1 is the first user's modulation symbol, s_2 the second user's modulation symbol, $c_i(k)$ the random spreading sequence used for the ith user, and $S(k)$ the combined spread sequence. It is assumed that the elements of the spreading sequences are normalized according to $|c_i(k)| = 1$.

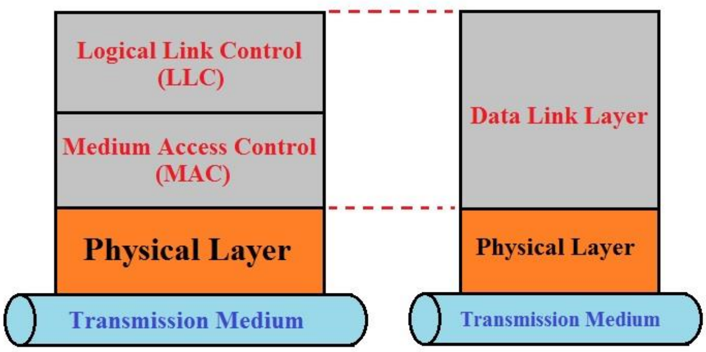
The process of recovering the wanted sequence from the spread sequence is known as despreading. Despreading user 1’s signal then becomes

$$(3.2)\tilde{s}_1=\sum_{k=1}^{M} S(k)c_1^*(k)=\sum_{k=1}^{M} s_1c_1(k)+s_2c_2(k)c_1^*(k)=Ms_1+\sum_{k=1}^{M} s_2c_2(k)c_1^*(k).$$

In equation (3.2), the second term in the right-hand side has a power level *M* times lower than the first term (note that $c_x(k)\cdot c_x^*(k)$. is always equal to unity).

A problem can arise when the signals from different users are received at very different power levels, for example, because in the uplink one user is close to the base station whereas a second user is not, as shown in Figure 3.6. In this case, the spreading gain will not be able to suppress the interference from the (strong) second user’s transmission sufficiently and the reception of the first user will experience a poor signal-to-interference ratio because of interference from the second user. This problem is known as the “near-far” problem and is mitigated by the use of power control that keeps the receive power from different transmissions at appropriate levels (depending on the users’ relative data rates).





LLC and MAC Sublayer

MAC address is suitable when multiple devices are connected with same physical link then to prevent from collisions system uniquely identify the devices one another at the data link layer, by using the MAC addresses that are assigned to all ports on a switch. The MAC sublayer uses MAC protocols to prevent collisions and MAC protocols uses MAC algorithm that accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC address.

Functions performed in the MAC sublayer:

The primary functions performed by the MAC layer as per the IEEE Std 802-2001 section 6.2.3 are as follows:

1. Frame delimiting and recognition: This function is responsible to creates and recognizes frame boundaries.
2. Addressing: MAC sublayer performs the addressing of destination stations (both as individual stations and as groups of stations) and conveyance of source-station addressing information as well.
3. Transparent data transfer: It performs the data transparency over data transfer of LLC, PDUs, or of equivalent information in the Ethernet sublayer.
4. Protection: MAC sublayer function is to protect the data against errors, generally by means of generating and checking frame check sequences.
5. Access control: Control of access to the physical transmission medium form unauthorized medium access.

One of the most commonly used of MAC sublayer for wired networks i.e. Carrier Sense Multiple Access with Collision Detection (CSMA/CD). Through MAC schema, a sender senses the medium (a wire or coaxial cable) before transmission of data to check whether the medium is free or not. If MAC senses that the medium is busy, the sender waits until it is free. When medium becomes free, the sender starts transmitting of data and continues to listen into the medium. If any kind of collision detected by sender while sending data, it stops at once and sends a jamming signal. But this scheme doest work well with wireless networks. Some of the problems that occur when it uses to transfer data through wireless networks are as follow;

- Signal strength decreases proportional to the square of the distance
- The sender would apply Carrier Sense (CS) and Collision Detection (CD), but the collisions happen at the receiver
- It might be a case that a sender cannot “hear” the collision, i.e., CD does not work
- Furthermore, CS might not work, if for e.g., the terminals are “hidden”.

REFERENCES:

Text Book:

Jochen Schiller, “Mobile Communications”, Pearson Education, Delhi, 2000.