LECTURE NOTES (E- Content) for

B. Sc. Electronics Part – II (2019-20)

SEMESTER -IV

PAPER – VII: DSC-D9

DIGITAL MODULATION AND MOBILE TELEPHONE SYSTEM

UNIT – III: MOBILE TELEPHONY SYSTEM &

UNIT – IV: MULTIPLE ACCESS TECHNIQUES & WIRELESS COMMUNICATION

As per syllabus of

SHIVAJI UNIVERSITY, KOLHAPUR

UNDER CHOICE BASED CREDIT SYSTEM

Prepared & Circulated

For B. Sc. – II Electronics Students

BY

Dr. A. M. Shaikh
Head, Department of Electronics
The New College, Kolhapur

(For Private Circulation only)

8 April 2020

Unit No. 3 Mobile Telephony System

Basic concept of mobile communication, frequency bands used in mobile communication, concept of cell splitting and cell sectoring, SIM number, IMEI number, need for data encryption, architecture (block diagram) of mobile communication network, simplified block diagram of mobile phone handset, Concept of GSM.

3.1 Introduction to Mobile Communication

Mobile telephone or cellular technology is widely used since early 1980s and is based upon the concept of frequency re-use by the application on a series of coverage cells. Since its first introduction, its use has increased very rapidly to the extent that a major portion of the global population has access to the technology. From developed nation to growing nation, mobile phone or cellular communications technology has been installed in all countries around the globe. The cellular telecommunications industry has been a major driver in the growth of the radio and electronics industries.

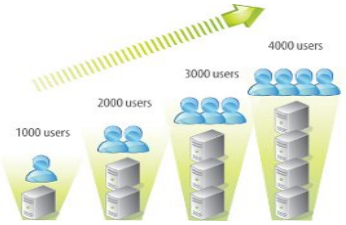
Mobile Communication is the use of technology that allows us to communicate with others in different locations without the use of any physical connection (wires or cables). Mobile communication makes our life easier, and it saves time and effort.

A mobile phone (also called mobile cellular network, cell phone or hand phone) is an example of mobile communication (wireless communication). It is an electronic device used for full duplex two way radio telecommunication over a cellular network of base stations known as cell site.

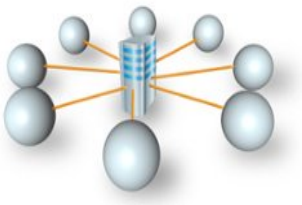
Features of Mobile Communication

The following are the features of mobile communication:

- **High capacity load balancing:** Each wired or wireless infrastructure must incorporate high capacity load balancing. High capacity load balancing means, when one access point is overloaded, the system will actively shift users from one access point to another depending on the capacity which is available.



- **Scalability:** The growth in popularity of new wireless devices continuously increasing day by day. The wireless networks have the ability to start small if necessary, but expand in terms of coverage and capacity as needed - without having to overhaul or build an entirely new network.



- **Network management system:** Now a days, wireless networks are much more complex and may consist of hundreds or even thousands of access points, firewalls, switches, managed power and various other components. The wireless networks have a smarter way of managing the entire network from a centralized point.

- **Indoor as well as outdoor coverage options:** It is important that your wireless system has the capability of adding indoor coverage as well as outdoor coverage.
- **Network access control:** Network access control can also be called as mobile device registration. It is essential to have a secure registration.
  Network access control (NAC) controls the role of the user and enforces policies. NAC can allow your users to register themselves to the network. It is a helpful feature that enhances the user experience.

- **Mobile device management:** Mobile device management can provide control of how you will manage access to programs and applications. Even you can remotely wipe the device if it is lost or stolen.
- **Roaming:** You don't need to worry about dropped connections, slower speeds or any disruption in service as you move throughout your office or even from building to building wireless needs to be mobile first. Roaming allows your end-users to successfully move from one access point to another without ever noticing a dip in a performance.
- **Proper Security means using the right firewall:** The backbone of the system is your network firewall. With the right firewall in place you will be able to:
  - See and control both your applications and end users.
  - Create the right balance between security and performance.
  - Reduce the complexity with:
    - Antivirus protection.
    - Deep Packet Inspection (DPI)
    - Application filtering
- **Switching:** Basically, a network switch is the traffic cop of your wireless network which making sure that everyone and every device gets to where they need to go.
  Switching is an essential part of every fast, secure wireless network for several reasons:
  - It helps the traffic on your network flow more efficiently.
  - It minimizes unnecessary traffic.
  - It creates a better user experience by ensuring your traffic is going to the right places.

Advantages of Mobile Communication

There are following advantages of mobile communication:

- **Flexibility:** Wireless communication enables the people to communicate with each other regardless of location. There is no need to be in an office or some telephone booth in order to pass and receive messages.
- **Cost effectiveness:** In wireless communication, there is no need of any physical infrastructure (Wires or cables) or maintenance practice. Hence, the cost is reduced.

- **Speed:** Improvements can also be seen in speed. The network connectivity or the accessibility was much improved in accuracy and speed.
- **Accessibility:** With the help of wireless technology easy accessibility to the remote areas is possible. For example, in rural areas, online education is now possible. Educators or students no longer need to travel to far-flung areas to teach their lessons.
- **Constant connectivity:** Constant connectivity ensures that people can respond to emergencies relatively quickly. For example, a wireless device like mobile can ensure you a constant connectivity though you move from place to place or while you travel, whereas a wired landline can't.

Cellular telecommunications generations

There is a lot of talk about the mobile phone generations. Each mobile phone generation had its own aims and was able to provide different levels of functionality.

Generation	Launching Year	Focus
1G	1979	Mobile Voice
2G	1991	Mobile Voice
3G	2001	Mobile Broadband
4G	2009	Mobile Broadband
5G	2020	Ubiquitous Connectivity

3.2 Frequency bands used in India: Here is a table for the different frequency bands in India for mobile technology 2G, 3G, and 4G.

Sr. No.	Mobile Technology in India	Frequency used
1	GSM (2G)	900 Mhz , 1800 MHz
2	CDMA	850 MHz
3	WCDMA (3G)	900 MHz, 2100 MHz
4	Wi-MAX	2300 MHz
5	4G (LTE)	850 MHz (Jio), 1800 MHz & 2300 MHz (AirTel, Idea, Vodafone, Jio) 2500 MHz (BSNL, Idea & Vodafone)

Key cellular communication concepts

As the name indicates, cellular telecommunication technology is based around the concept of using a large number of base stations each covering a small area called as a ***'cell'.*** With each base station communicating with a reasonable number of users, it means that the whole system can accommodate a huge number of connections, and the levels of frequency use are good.

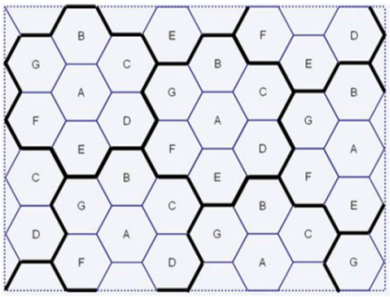
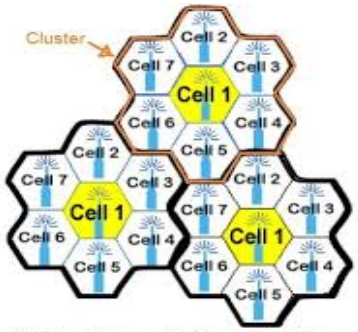


Fig. 1. Schematic of a cellular system with hexa-gonal cells. Cells marked with same letter are co-channel cells.

Cell systems for frequency re-use

Any radio transmitter will only have a certain coverage area. Beyond this the signal level will fall to a limited below which it cannot be used and will not cause significant interference to users associated with a different radio transmitter. This means that it is possible to re-use a channel outside the range of the radio transmitter. The same is also true in the reverse direction for the receiver, where it will only be able to receive signals over a given range. In this way it is possible to split up an area into several smaller regions, each covered by a different transmitter / receiver station.



Cellular Communication -cell splitting
Frequency reuse concept

These regions are conveniently known as cells, and give rise to the name of a "cellular" technology used today. Diagrammatically these cells are often shown as hexagonal shapes that conveniently fit together. In reality this is not the case. They have irregular boundaries because of the terrain (*the vertical and horizontal dimensions)* over which they travel. Hills, buildings and other objects all cause the signal to be attenuated and diminish differently in each direction. Therefore it is never possible to have a sharp cut-off between cells. In some areas they may overlap, whereas in others there will be a "hole" in coverage.

Cell clusters

When devising the infrastructure technology of a cellular system, the interference between adjacent channels is reduced by allocating different frequency bands or channels to adjacent cells so that their coverage can overlap slightly without causing interference. In this way cells can be grouped together in what is termed a cluster.

Often these clusters contain seven cells, but other configurations are also possible. Seven is a convenient number, but there are a number of conflicting requirements that need to be balanced when choosing the number of cells in a cluster for a cellular system:

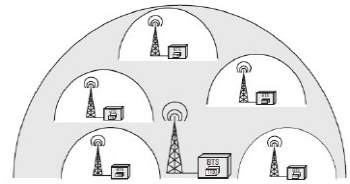
Cell size

Even though the number of cells in a cluster in a cellular system can help govern the number of users that can be accommodated, by making all the cells smaller it is possible to increase the overall capacity of the cellular system. However a greater number of transmitter receiver or base stations are required if cells are made smaller and this increases the cost to the operator. Accordingly in areas where there are more users, small low power base stations are installed.

The different types of cells are given different names according to their size and function:

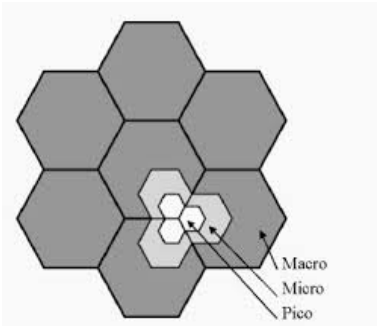
- ***Macro cells:*** Macro cells are large cells that are usually used for remote or thinly populated areas. These may be 10 km or possibly more in diameter.
- ***Micro cells:*** Micro cells are those that are normally found in densely populated areas which may have a diameter of around 1 km.
- ***Pico cells:*** Pico cells are generally used for covering very small areas such as particular areas of buildings, or possibly tunnels where coverage from a larger cell in the cellular system is not possible.
- ***Selective cells:*** Sometimes cells termed selective cells may be used where full 360 degree coverage is not required. They may be used to fill in a hole in the coverage in the cellular system, or to address a problem such as the entrance to a tunnel etc.

- ***Umbrella cells:*** Another type of cells known as an umbrella cell is sometimes used in instances such as those where a heavily used road crosses an area where there are microcells.



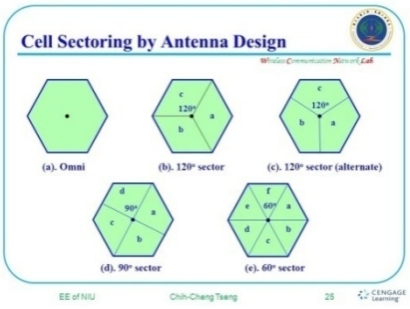
3.3 Concept of cell splitting and cell sectoring

As the number of users increase channel capacity decreases. So in order to increase the coverage and channel capacity two types of techniques are used. These techniques are cell splitting and cell sectoring.



Cell splitting: Cell splitting is the process of subdividing a congested cell into smaller cells**.** Each small cell has its own base station and a corresponding reduction in antenna height and transmitter power. Cell splitting is done by defining and installing new cells which have a smaller radius than the original cells (macro cells). The smaller cells are called microcells. The radius R of every microcell is cut in half, (R/2).

Cell splitting increases the capacity of a cellular system since in increases the number of times that channels are reused. The consequence of the cell splitting is that the frequency assignment has to be done again, which affects the neighbouring cells.



Cell sectoring: Cell sectoring is done by replacing an omnidirectional antenna (providing 360 degree coverage) by several directional antennas (providing 120 degree or 60 degree coverage) without changing cell radius. Cell sectoring is done to overcome co-channel interference and to increase the capacity. Each sector can be considered as a new cell, with its own (set of) frequency channel(s). Cell sectoring is done in two ways –

1. 120^0 sectoring & 2. 60^0 sectoring

In the first case an omnidirectional antenna is replaced by three directional antennas having 120 degree coverage. These antennas are placed either at the corners of a hexagonal cell or at the centre of a cell. In second case an omnidirectional antenna is replaced by six directional antennas having 60 degree coverage. These six antennas are placed at the six corners of the cell as shown in the figure above. Cell Sectoring is less expensive than cell-splitting, as it does not require the acquisition of new base station sites**.**

3.4 SIM Number and IMEI number

A Subscriber Identity Module or Subscriber Identification Module (SIM), widely known as a 'SIM Card', is an integrated circuit identification that is intended to securely store the international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers).

SIM number: or Integrated Circuit Card Identifier (ICCID) is 19 or 20 digit number printed on back side of a SIM card. Let us suppose this number is: 8991000900375752261U. Each group of number has some specific meaning.

89 91 00 090037575226 1 U

89 – First 2 digits are industry code

91 – Next 2 digits for country code

00 – Next 2 digits for issuer number

0900 37575226 – Next 12 digits for customer id

1 – Next one digit for checksum &

U – Stands for Universal

It is also possible to store contact information on many SIM cards. SIM cards are always used on GSM phones; for CDMA phones, they are only needed for newer LTE-capable handsets. SIM cards can also be used in satellite phones, smart watches, computers, or cameras.

The SIM circuit is part of the function of a universal integrated circuit card (UICC) physical smart card, which is usually made of PVC with embedded contacts and semiconductors. SIM cards are transferable between different mobile devices. The first UICC smart cards were the size of credit and bank cards; sizes were reduced several times over the years, usually keeping electrical contacts the same, so that a larger card could be cut down to a smaller size.

A SIM card contains its unique serial number (ICCID), international mobile subscriber identity (IMSI) number, security authentication and ciphering information, temporary information related to the local network, a list of the services the user has access to, and two passwords: a personal identification number (PIN) for ordinary use, and a personal unblocking code (PUC) for PIN unlocking.

IMEI number: International Mobile Equipment Identity number is cell phone's unique identity number. This is the hardware number of a device. Dual SIM cards device has two IMEIs. IMEIs tell information about the device. It is useful for software updates for device and blocking device for accessing telecom network. When a device is stolen its only IMEI which is used to detected the device by roaming network.

It is usually a 15 digit unique number found printed inside the battery compartment of the phone, but can also be displayed on-screen on most phones by entering *#06# on the dial pad, or alongside other system information in the settings menu on smart phone operating systems.

GSM networks use the IMEI number to identify valid devices, and can stop a stolen phone from accessing the network. For example, if a mobile phone is stolen, the owner can have their network provider use the IMEI number to blacklist the phone. This renders the phone useless on that network and sometimes other networks, even if the thief changes the phone's subscriber identity module (SIM).

Devices without a SIM card slot usually don't have the IMEI code. However, the IMEI only identifies the device and has no particular relationship to the subscriber. The phone identifies the subscriber by transmitting the International mobile subscriber identity (IMSI) number i.e. SIM number.

When someone has their mobile equipment stolen or lost, they can ask their service provider to block the phone from their network, and the operator does so if required by law. If the local operator maintains an Equipment Identity Register (EIR), it adds the device IMEI to it. Optionally, it also adds the IMEI to shared registries, such as the Central Equipment Identity Register (CEIR),

which blacklists the device with other operators that use the CEIR. This blacklisting makes the device unusable on any operator that uses the CEIR, which makes mobile equipment theft pointless, except for parts.

3.5 Data encryption

Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. Encrypted data is commonly referred to as ciphertext, while unencrypted data is called plaintext. Currently, encryption is one of the most popular and effective data security methods used by organizations. Two main types of data encryption exist - asymmetric encryption, also known as public-key encryption, and symmetric encryption.

Science and encryption are used today to keep our most sensitive and personal data safe and secure from those who we don't wish to access it. Today we have many sophisticated and refined tools that can be put to use in protecting our data. These tools not only keep our data safe, but they also ensure that even if it does fall into the wrong hands, only the intended recipient is available to read it.

Need for data encryption

There are five reasons to encrypt the data. These are-

1. Privacy:
The privacy concern is the big one. Anyone who can lay their hands on an unencrypted file can read its contents. Even with an unknown file type, a lack of encryption would make it possible to find out what it said.

2. Protection by Default:
Having all your mobile storage encrypted is definitely helpful in preventing anyone who steals your phone from stealing your identity. But, what about the stuff you haven't encrypted? A thief can pull those files from your unencrypted phone without even having to power it on and log in.

For this reason, all modern smart phones and all Windows machines since Vista encrypt their hard drives automatically when they are powered off. Until the user turns the device on and enters their password, the files are virtually impossible to decrypt. This means that the average user benefits from strong encryption by default.

3. Virtual Private Networks:
A virtual private network (VPN) is an essential tool for anyone who wants or needs to keep their Wi-Fi communications secure. A VPN creates a secure encrypted communications channel between your device and the internet. A VPN can be used by businesses to keep information encrypted until it reaches its destination. Without the strong encryption offered by a VPN, many businesses would have to reconsider their operations.

4. Trustable Apps:
We all hand over vast amounts of sensitive and personal information to app developers. Whether this is to allow the app to function as intended or not, we would all hope that any data stored about us is kept encrypted. Otherwise, any other app developer could slip in and take a peek at the unencrypted information.

5. Personal Rights:

If a file is unencrypted, anyone can access and view it. However, with an encrypted file, the consent of the data owner is required to access it. Encryption means you can store personal information on your device with confidence. Even governments have been defeated by the strength of modern encrypted smart phones.

3.6 Architecture (block diagram) of mobile communication network

[Source:bmsit.ac.in/system/study_materials/documents]

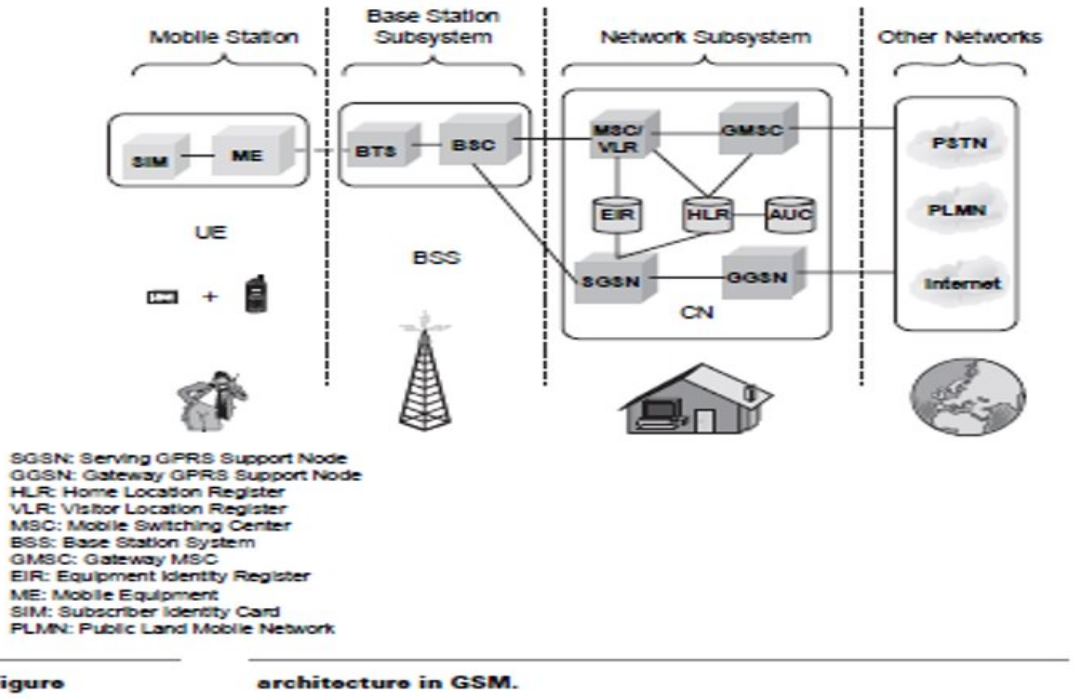


Figure architecture in GSM.

The GSM network architecture consists of three major subsystems:

- Mobile Station (MS)
- Base Station Subsystem (BSS)
- Network and Switching Subsystem (NSS)

The wireless link interface between the MS and the Base Transceiver Station (BTS) is a part of BSS. Many BTSs are controlled by a Base Station Controller (BSC). BSC is connected to the Mobile Switching Center (MSC), which is a part of NSS. Figure shows the key functional elements in the GSM network architecture.

1. **Mobile Station (MS)**:

A mobile station communicates across the air interface with a base station transceiver in the same cell in which the mobile subscriber unit is located. The MS communicates the information with the user and modifies it to the transmission protocols if the air-interface to communicate with the BSS. The user's voice information is interfaced with the MS through a microphone and speaker for the speech, keypad, and display for short messaging, and the cable connection for other data terminals. The MS has two elements. The Mobile Equipment (ME) refers to the physical device, which comprises of transceiver, digital signal processors, and the antenna. The second element of the MS is the GSM is the Subscriber Identity Module (SIM). The SIM card is unique to the GSM system. It has a memory of 32 KB.

2. Base Station Subsystem (BSS):

A base station subsystem consists of a base station controller and one or more base transceiver station. Each Base Transceiver Station defines a single cell. A cell can have a radius of between 100m to 35km, depending on the environment. A Base Station Controller may be connected with a BTS. It may control multiple BTS units and hence multiple cells. There are two main architectural elements in the BSS – the Base Transceiver Subsystem (BTS) and the Base Station Controller (BSC). The interface that connects a BTS to a BSC is called the A-bis interface. The interface between the BSC and the MSC is called the A interface, which is standardised within GSM.

3. Network and switching subsystem (NSS)

The NSS is responsible for the network operation. It provides the link between the cellular network and the Public switched telecommunicates Networks (PSTN or ISDN or Data Networks). The NSS controls handoffs between cells in different BSSs, authenticates user and validates their accounts, and includes functions for enabling worldwide roaming of mobile subscribers. In particular the switching subsystem consists of:

- Mobile switch Center (MSC)
- Home location Register (HLR)
- Visitor location Register (VLR)
- Authentications Center (Auc)
- Equipment Identity Register (EIR)
- Interworking Functions (IWF)

The NSS has one hardware, Mobile switching center and four software database element: Home location register (HLR), Visitor location Register (VLR), Authentications center (Auc) and Equipment Identity Register (EIR). The MSC basically performs the switching function of the system by controlling calls to and from other telephone and data systems. It includes functions such as network interfacing and common channel signalling.

HLR:

The HLR (Home Location Register) is database software that handles the management of the mobile subscriber account. It stores the subscriber address, service type, current locations, forwarding address, authentication/ciphering keys, and billings information. In addition to the ISDN telephone number for the terminal, the SIM card is identified with an International Mobile Subscribes Identity (IMSI) number that is totally different from the ISDN telephone number. The HLR is the reference database that permanently stores data related to subscribers, including subscriber's service profile, location information, and activity status.

VLR:

The VLR (Visitor Location Register) is temporary database software similar to the HLR identifying the mobile subscribers visiting inside the coverage area of an MSC. The VLR assigns a Temporary mobile subscriber Identity (TMSI) that is used to avoid using IMSI on the air. The visitor location register maintains information about mobile subscriber that is currently physically in the range covered by the switching center.

When a mobile subscriber roams from one LA (Local Area) to another, current location is automatically updated in the VLR. When a mobile station roams into a new MSC area, if the old and new LA's are under the control of two different VLRs, the VLR connected to the MSC will

request data about the mobile stations from the HLR. The entry on the old VLR is deleted and an entry is created in the new VLR by copying the database from the HLR.

AuC:

The AuC database holds different algorithms that are used for authentication and encryptions of the mobile subscribers that verify the mobile user's identity and ensure the confidentiality of each call. The AuC holds the authentication and encryption keys for all the subscribers in both the home and visitor location register.

EIR:

The EIR is another database that keeps the information about the identity of mobile equipment such the International mobile Equipment Identity (IMEI) that reveals the details about the manufacturer, country of production, and device type. This information is used to prevent calls from being misused, to prevent unauthorised or defective MSs, to report stolen mobile phones or check if the mobile phone is operating according to the specification of its type.

White list:

This list contains the IMEI of the phones who are allowed to enter in the network.

Black list:

This list on the contrary contains the IMEI of the phones who are not allowed to enter in the network, for example because they are stolen.

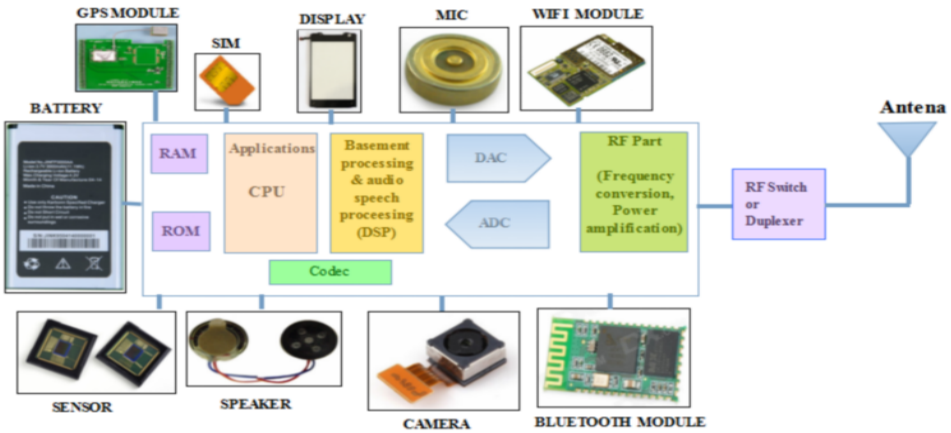
Grey list:

This list contains the IMEI of the phones momentarily not allowed to enter in the network, for example because the software version is too old or because they are in repair.

IWF Interworking Function:

It is a system in the PLMN that allows for non speech communication between the GSM and the other networks. The tasks of an IWF are particularly to adapt transmission parameters and protocol conversions. The physical manifestations of an IWF may be through a modem which is activated by the MSC dependent on the bearer service and the destination network.

3.7 Block diagram of mobile phone handset *[Source: Techplayon.com]*



Typically Mobile phone will have display (LCD, touch screen), keypad, microphone, speaker, SIM card, battery, USB port, antenna, memory unit(RAM,ROM), camera, CODEC, RF part, DAC/ADC, baseband part (L1/Layer1/physical layer) running on DSP, Application/protocol layers running on CPU, ON/OFF switch and Bluetooth/GPS features. All these features are based on specific standard specifications designed, like it may be based on GSM, WCDMA or LTE etc.

RF Part:

As shown in figure above, every phone has RF part which consists of RF frequency up converter and frequency down converter, many analog filters, digital attenuator, driver amplifiers etc. For system, up converter converts modulated baseband signal (I and Q) either at zero IF (Intermediate frequency) or some IF to RF frequency. RF down converter converts RF signal to baseband signal (I and Q). The basic component used for frequency conversion is RF mixer. Analog filters pass only desired band of signals. Amplifiers boost up the signal to the required transmit power level.

Baseband Part:

Baseband part in a mobile is comprised of a digital signal processor (DSP) to process forward voice/data signals for transmission and to process reverse voice/data signals received.

This is the core processing part which changes for various air interface standards like GSM, HSPA, LTE and more. It is often named as physical layer or Layer 1 or L1. For Speech/audio, codec is used to compress and decompress the signal to match the data rate to the frame it has to fit in. The baseband or physical layer will add redundant bits to enable error detection as well as error correction.

ADC and DAC:

ADC (Analog to Digital Converter) and DAC (Digital to Analog Converter) is used to convert analog speech signal to digital signal and vice versa in the mobile handset.

RF Switch / Duplexer:

RF switch is used for TDD (Time Division Duplex) configuration, which switches the RF path between transmit chain and receive chain and on the other side, Duplexer is used for FDD (Frequency Division Duplex) configuration which passes the transmitted signal and received signal at the same time through it.

Application layer

It consists of protocols that focus on process-to-process communication across an IP network and provides a firm communication interface and end-user services. It also runs on CPU. It include audio, video and image/graphics applications. The application layer provides many services, including: Simple Mail Transfer, Protocol File transfer, graphics etc.

Camera

Now-a-days with almost all the mobile phone camera feature is available for one to click pictures at various occasions. It is the major specifications in increasing cost of mobile phone. There are various mega pixel cameras such as 13 MP, 23 MP, 48 MP or even 64 MP available in smart phones. This has become evident because of advancement in sensor technology.

Display

There are lot of display types used in mobile phones. They can be either colour or monochrome. The colour displays usually are CSTN, TFT, TFD or OLED with a predominant use of TFT displays in current mobile lineups. There are also two types of touch screen displays – capacitive and resistive, which are both based on TFT technology.

Capacitive touch screens work by sensing the electrical properties of the human body, while Resistive ones operate by sensing direct pressure applied by the user. The Resistive type can be activated by pressing not only with human skin but also with a stylus and thus allow handwriting recognition input.

Microphone

Microphone or mic converts air pressure variations (result of our speech) to electrical signal to couple on the PCB for further processing. Usually in mobile phone mic of types condenser, dynamic, carbon or ribbon is used.

Speaker

It converts electrical signal to audible signal(pressure vibrations) for human being to hear. This is often coupled with audio amplifier to get required amplification of audio signal. It also tied with volume control circuit to change (increase or decrease) the amplitude of the audio signal.

Antenna

An antenna converts electromagnetic radiation into electric signal and vice versa. In mobile phone, antenna is embedded inside, which is not visible to us. A metal strip pattern is served as an antenna.

Connectivity (Wi-Fi, Bluetooth, USB, GPS)

To make data transfer fast enough between mobile phone and other computing devices (laptop, desktop, tablet) or between mobile and mobile various technologies are evolved which include Wi-Fi, Bluetooth, USB. GPS (global positioning system) is used for location assistance and will enable google map to work efficiently.

Sensors

A sensor is a transducer whose purpose is to sense (that is, to detect) some characteristic of its environs. It detects events or changes in quantities and provides a corresponding output, generally as an electrical or optical signal. In mobile phone, there are various kind of sensors are used like accelerometer, magnetometer, proximity sensor, light sensor, barometer, pedometer, thermometer etc.

Various mobile phones have different concepts and design on every aspects, but the methods and operational flow are all exactly the same. It differs on how and what certain IC chips and parts they are being used and installed to a certain mobile phone circuitry.

Questions

A) Long answer type questions for 10 marks.

1. Draw the block diagram of mobile communication (GSM) network and explain the working of each block.
2. Draw the block diagram of mobile phone handset and explain the working of each block.

B) Short answer type questions for 5 marks.

1. What are the frequency bands used mobile communication in India?
2. Explain the concept of cell splitting and cell sectoring.
3. Write a short note on SIM Number and IMEI number.
4. What is data encryption and why it is needed?

---XXX---

***References*:**

To prepare the above e-content for the Unit No. 3, I have collected material from the following sources, websites & Links:

1. *javatpoint.com*
2. *d3i71xaburhd42.cloudfront.net*
3. *Web ProForum Tutorials*
4. *http://www.lec.org (The International Engineering Consortium)*
5. *slidesharecdn.net*
6. *slideplayer.com*
7. *wikipedia.org,*
8. *quora.com*
9. *bhaskar.com,*
10. *youtube .com*
11. *hardreset.info*
12. *wikipedia.org*
13. *digitalguardian.com*
14. *mobileappdaily.com*
15. *bmsit.ac.in/system/study_materials/documents*
16. *Techplayon.com*
17. *digitalguardian.com*

---XXX---

Unit No. 4: Multiple Access Techniques & Wireless Communication

Concepts of SDMA, CDMA, TDMA and FDMA technologies, 2G, 3G and 4G, Bluetooth, Wi-Fi, RFID & GPS navigation system concepts only (qualitative idea only).

4.1 Multiple Access Techniques for Cellular Systems

In any cellular system it is necessary for it to have a scheme whereby it can handle multiple users at any given time. There are many ways of doing this, and as cellular technology has advanced, different techniques have been used. The multiple access schemes are known as FDMA, TDMA, CDMA and OFDMA.

Requirements for a multiple access scheme

There are a number of requirements that any multiple access scheme must be able to meet:

- Ability to handle several users without mutual interference.
- Ability to be able to maximise the spectrum efficiency
- Must be robust, enabling ease of handover between cells.

SDMA – Space Division Multiple Access

SDMA is a channel access method based on creating parallel spatial pipes (focused signal beams) using advanced antenna technology. In traditional mobile cellular network systems, the base station has no information on the position of the mobile units within the cell and radiates the signal in all directions within the cell in order to provide radio coverage. This method results in wasting power on transmissions when there are no mobile units to reach, in addition to causing interference for adjacent cells using the same frequency, so called co-channel cells. Likewise, in reception, the antenna receives signals coming from all directions including noise and interference signals. By using smart antenna technology and differing spatial locations of mobile units within the cell, space-division multiple access techniques offer attractive performance enhancements.

FDMA - Frequency Division Multiple Access

FDMA is the most straightforward of the multiple access schemes that have been used. As a subscriber comes onto the system, or swaps from one cell to the next, the network allocates a channel or frequency to each one. In this way the different subscribers are allocated a different slot and access to the network. As different frequencies are used, the system is naturally termed Frequency Division Multiple Access. This scheme was used by all analogue systems.

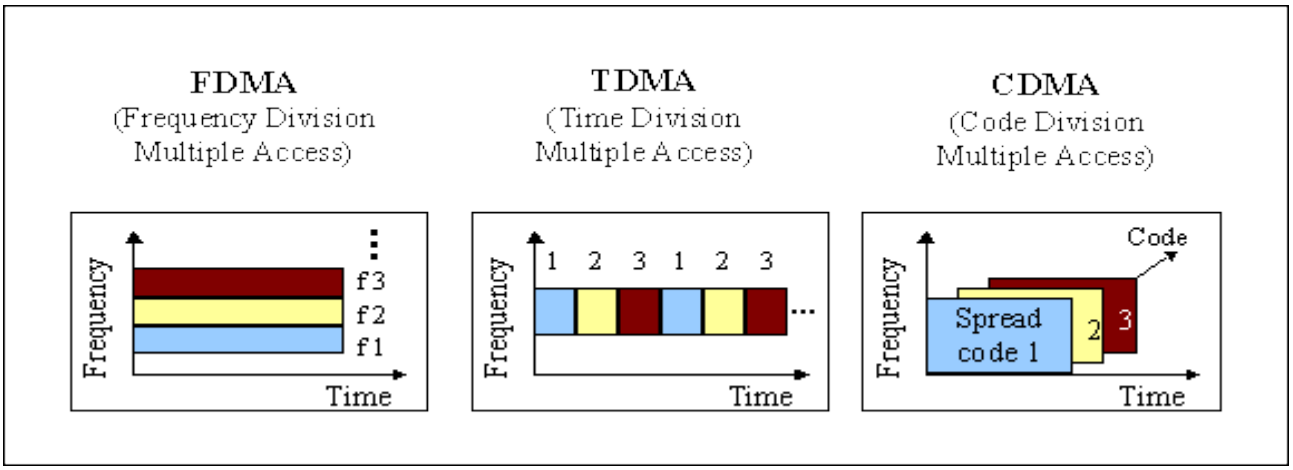
TDMA - Time Division Multiple Access

The second system came about with the transition to digital schemes for cellular technology. Here digital data could be split up in time and sent as bursts when required. As speech was digitised it could be sent in short data bursts, any small delay caused by sending the data in bursts would be short and not noticed. In this way it became possible to organise the system so that a given number of slots were available on a given transmission. Each subscriber would then be allocated a different

time slot in which they could transmit or receive data. As different time slots are used for each subscriber to gain access to the system, it is known as time division multiple access. Obviously this only allows a certain number of users access to the system. Beyond this another channel may be used, so systems that use TDMA may also have elements of FDMA operation as well.

CDMA - Code Division Multiple Access

CDMA uses one of the aspects associated with the use of direct sequence spread spectrum. It can be seen from the article in the cellular telecoms area of this site that when extracting the required data from a DSSS signal it was necessary to have the correct spreading or chip code, and all other data from sources using different orthogonal chip codes would be rejected. It is therefore possible to allocate different users different codes, and use this as the means by which different users are given access to the system.



The scheme has been likened to being in a room filled with people all speaking different languages. Even though the noise level is very high, it is still possible to understand someone speaking in your own language. With CDMA different spreading or chip codes are used. When generating a direct sequence spread spectrum, the data to be transmitted is multiplied with spreading or chip code. This widens the spectrum of the signal, but it can only be decided in the receiver if it is again multiplied with the same spreading code. All signals that use different spreading codes are not seen, and are discarded in the process. Thus in the presence of a variety of signals it is possible to receive only the required one.

In this way the base station allocates different codes to different users and when it receives the signal it will use one code to receive the signal from one mobile, and another spreading code to receive the signal from a second mobile. In this way the same frequency channel can be used to serve a number of different mobiles.

OFDMA - Orthogonal Frequency Division Multiple Access

OFDMA is the form of multiple access scheme that is being considered for the fourth generation cellular technologies along with the evolutions for the third generation cellular systems (LTE for UMTS / W-CDMA and UMB for CDMA2000).

As the name implies, OFDMA is based around OFDM. This is a technology that utilises a large number of close spaced carriers.

4.2 Generations of Wireless Communication

Mobile communication is one of the hottest areas with advanced techniques. It is developing extremely fast in present times and deals with all the fields of mobile and wireless communications. The evolution and development of various generations of mobile wireless technology along with their advantages and disadvantages are discussed below.

1G

- This is the first generation of wireless telephone technology, mobile telecommunications, which was launched in Japan by NTT in 1979.
- The main technological development in this generation that distinguished the First Generation mobile phones from the previous generation was the use of multiple cell sites, and the ability to transfer calls from one site to the next site as the user travelled between cells during a conversation.
- It used analog signals.
- It allowed only voice calls and in one country.
- Not possible to send or receive text messages.

Disadvantages

- Poor quality of voice
- Poor life of Battery
- Size of phone was very large
- No security
- Capacity was limited
- Poor handoff reliability

2G

- This is the second generation of mobile telecommunication was launched in Finland in 1991.
- It was based on GSM standard.
- It used digital signals.
- It enables data transmission like as text messaging (SMS - Short Message Service), transfer or photos or pictures (MMS), but not videos.
- The later versions of this generation, which were called 2.5G using GPRS (General Packet Radio Service) and 2.75G using EDGE (Enhanced data rates for GSM Evolution) networks.
- It provides better quality and capacity.

Disadvantages

- Unable to handle complex data such as Video
- Requires strong digital signals

3G

- 3G is the third generation was introduced in early 2000s.
- The transmission of data was increased up to 2Mbits/s, which allows you to sending or receiving large email messages.
- The main difference between 3G and 2G is the use of packet switching rather than circuit switching for data transmission.
- Faster communication
- High speed web or more security
- Video conferencing
- 3D gaming
- TV streaming, Mobile TV, phone calls etc. are the features of 3G.

Disadvantages

- Costly
- Requirement of high bandwidth
- Expensive 3G phones
- Size of cell phones was very large.

4G

- 4G is the fourth generation of mobile telecommunication which was appeared in 2010.
- It was based on LTE (Long Term Evolution) and LTE advanced standards.
- Offer a range of communication services like video calling, real time language translation and video voice mail.
- It was capable of providing 100 Mbps to 1Gbps speed.
- High QoS (Quality of Service) and High security.
- The basic term used to describe 4G technology is
- MAGIC. Where :
  M - Mobile multimedia
  A - Anytime anywhere
  G - Global mobility support
  I - Integarted wireless solution
  C - Customized personal service

Disadvantages

- Uses more battery
- Difficult to implement
- Expensive equipment are required

5G

- It is referred to fifth generation wireless connection which will be probably implemented by 2020, or even some years earlier.
- Machine to machine communication can be possible in 5G.
- 5G will be able to perform Internet of Things (IoT) for smart home and smart city, connected cars etc.
- This generation will be based on lower cost, low battery consumption and lower latency than 4G equipment.
- There will be much faster transmission rate of data to the previous versions. Thus the speed of 5G will be 1Gbit/s.

4 Cell Phone Generations Compared

	Standards	Technology	SMS	Voice Switching	Data Switching	Data Rates
1G	AMPS, TACS	Analog	No	Circuit	Circuit	N/A
2G	GSM, CDMA, EDGE, GPRS	Digital	Yes	Circuit	Circuit	236.8 kbps
3G	UTMS, CDMA2000, HSPDA, EVDO	Digital	Yes	Circuit	Packet	384 kbps
4G	LTE Advanced, IEEE 802.16 (WiMax)	Digital	Yes	Packet	Packet	up to 1 Gbps

4.3 Bluetooth

The development of the "short-link" radio technology, later named Bluetooth, was initiated in 1989 by Nils Rydbeck, CTO at Ericsson Mobile in Lund, Sweden. The purpose was to develop wireless headsets, according to two inventions by Johan Ullman. Both were working for Ericsson in Lund. In 1990, Jaap Haartsen was nominated by the European Patent Office for the European Inventor Award.

Bluetooth is a wireless technology standard used for exchanging data between fixed and mobile devices over short distances using short-wavelength UHF radio waves in the industrial, scientific and medical radio bands, from 2.400 to 2.485 GHz, and building personal area networks (PANs).

Bluetooth operates at frequencies between 2.402 and 2.480 GHz, or 2.400 and 2.4835 GHz including guard bands 2 MHz wide at the bottom end and 3.5 MHz wide at the top. This is in the globally unlicensed (but not unregulated) industrial, scientific and medical (ISM) 2.4 GHz short-range radio frequency band.

Bluetooth uses a radio technology called frequency-hopping spread spectrum. Bluetooth divides transmitted data into packets, and transmits each packet on one of 79 designated Bluetooth channels. Each channel has a bandwidth of 1 MHz. It usually performs 1600 hops per second,

with adaptive frequency-hopping (AFH) enabled. Bluetooth Low Energy uses 2 MHz spacing, which accommodates 40 channels.

Bluetooth is a packet-based protocol with a master/slave architecture. One master may communicate with up to seven slaves in a piconet. All devices within a given piconet use the clock provided by the master as the base for packet exchange. The master clock ticks with a period of 312.5 µs, two clock ticks then make up a slot of 625 µs, and two slots make up a slot pair of 1250 µs. In the simple case of single-slot packets, the master transmits in even slots and receives in odd slots. The slave, conversely, receives in even slots and transmits in odd slots. Packets may be 1, 3 or 5 slots long, but in all cases the master's transmission begins in even slots and the slave's in odd slots.

At any given time, data can be transferred between the master and one other device (except for the little-used broadcast mode). The master chooses which slave device to address; typically, it switches rapidly from one device to another in a round-robin fashion. Since it is the master that chooses which slave to address, whereas a slave is (in theory) supposed to listen in each receive slot, being a master is a lighter burden than being a slave. Being a master of seven slaves is possible; being a slave of more than one master is possible. The specification is vague as to required behaviour in scatternets.

Bluetooth devices automatically detect and connect to one another and can communicate at any one time. They don't interfere with one another because each pair of devices uses a different one of the 79 available channels. If two devices want to talk, they pick a channel randomly and, if that's already taken, randomly switch to one of the others (a technique known as spread-spectrum frequency hopping). To minimize the risks of interference from other electrical appliances (and also to improve security), pairs of devices constantly shift the frequency they're using—thousands of times a second.

When a group of two or more Bluetooth devices are sharing information together, they form a kind of ad-hoc, mini computer network called a piconet. Other devices can join or leave an existing piconet at any time. One device (known as the master) acts as the overall controller of the network, while the others (known as slaves) obey its instructions. Two or more separate piconets can also join up and share information forming what's called a scatternet.

Advantages of Bluetooth

1. Wireless: Bluetooth works without cables.
2. Low energy consumption: Bluetooth uses low power signals.
3. Inexpensive: it is cheap to manufacture, and anyone can buy it.
4. Shares voice and data: Bluetooth allows devices to share voice and data.

Applications of Bluetooth

1. **Consumer –** wireless PC peripherals, smart house integration, advertisements, etc.
2. **Games & Entertainment–** Wireless controllers, virtual reality, iPODs, etc.
3. **Professional -** Pagers, PDAs, cell phones, desktops, automobiles etc.
4. **Services -** Shipping, travel-tourism, hotels, etc.

5. **Industry –** Delivery (e. g. Scanners, printers) assembly lines, inspections, inventory control
6. **Sports training –** Fitness devices, Health sensors, monitors, motion tracking etc.
7. **Military –** Combat and maintenance

4.4 Wi-Fi

Wi-Fi is a popular wireless networking technology. It is commonly called as “Wireless LAN” (local area network). Wi-Fi allows local area networks to operate without cable and wiring. It is making popular choice for home and business networks.

By using this technology we can exchange the information between two or more devices. Wi-Fi has been developed for mobile computing devices, such has laptops, but it is now extensively using for mobile applications and consumer electronics like televisions, DVD players and digital cameras.

There should be two possibilities in communicating with the Wi-Fi connection that may be through access point to the client connection or client to client connection. Wi-Fi is a one type of wireless technology. A computer’s wireless adaptor transfers the data into a radio signal and transfers the data into antenna for users.

[The name Wi-Fi has no further meaning, and was never officially a shortened form of "Wireless Fidelity". Nevertheless, the Wi-Fi Alliance which consists of more than 375 companies used the advertising slogan "The Standard for Wireless Fidelity". The name Wi-Fi, commercially used at least as early as August 1999, was coined by the brand-consulting firm Interbrand. The Wi-Fi Alliance had hired Interbrand to create a name that was "a little catchier than 'IEEE 802.11b Direct Sequence'." Phil Belanger, a founding member of the Wi-Fi Alliance who presided over the selection of the name "Wi-Fi", has stated that Interbrand invented Wi-Fi as a pun on the word hi-fi (high fidelity), a term for high-quality audio technology.] [Source: wikipedia.org]

Working Principle

Wi-Fi is a high speed internet connection and network connection without use of any cables or wires. The wireless network is operating three essential elements that are radio signals, antenna and router. The radio waves are keys which make the Wi-Fi networking possible. The computers and cell phones are ready with Wi-Fi cards.
The radio signals transmitted from antennas and routers are picked up by Wi-Fi receivers such as computers, laptops, and cell phones that are ready with Wi-Fi cards.

Whenever the computer receives the signals within the range of 100-150 feet from the router, it connects the device immediately. The range of Wi-Fi depends upon the environment, indoor or outdoor ranges. The Wi-Fi cards will read the signals and create an internet connection between user and network. The speed of the device using Wi-Fi connection increases as the computer gets closer to the main source and speed decreases as it gets further away.

Wi-Fi Connection

Many laptops, cell phones have inbuilt Wi-Fi card. It is a free-based type of network connection which the user uses a login id and password. The free base network connection is also available in some areas. The Wi-Fi network connection is creating hot spots in the cities, in public places like restaurants, airports, hotels, offices, universities etc.

Security

Security is important element in the Wi-Fi technology. Security is our personal decision but having a wireless connection we should pay attention to protect our private details. If we don't secure our connection then any one can steal the personal data, do illegal activities. So it is necessary to have secured connection.

Applications of Wi-Fi

- Mobile applications
- Business applications
- Home applications
- Browsing internet
- Video conferencing
- e- Teaching - learning

Advantages

- Wireless device can be moved from one place to another.
- Cost of wires is reduced.
- Easy to establish connection
- It is safe and cannot interfere with any network
- Connection via hot spot is also possible

Disadvantages

- Wi-Fi connection radiate radio frequencies which may be harmful to human health
- We must have to disconnect the Wi-Fi connection when not in use
- We cannot transfer data for long distance

4.5 RFID

RFID means Radio Frequency Identification. RFID is a technology which works on radio frequency or radio waves. This technology is used for tracking objects automatically. The objects could be anything. It could be books in the library, or it could be any item purchasing from

shopping mall or inventory in the warehouse or it could be a car. Not only the objects but it can be also used for tracking animals or birds.

In this RFID technology there are two main parts one is RFID reader and other is RFID tag. We have to attach a RFID tag to the object which we want to track. The RFID reader is continuously sending the radio signals. Whenever this object is in the range of reader then the RFID tag sends its feedback signals to the reader. So it is similar to barcode technology. In the barcode the object and scanner should in a line of sight. But the RFID technology is not a line of sight technology. As far as the object is in the range of the reader, the object is able to identify the reader or able to send feedback signal. Using this RFID technology it is possible to identify multiple objects at the same time.

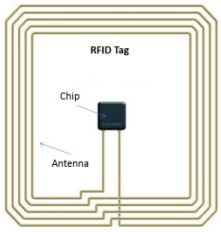
RFID tags are three types- Active tag, Passive tag, and Semi Passive tag. Passive tags do not have their own power supply so they have to rely on radio waves coming from reader for the source of energy. In case of semi passive tags, they have their own power supply. But for transmitting the feedback signal back to the reader they have to also rely on radio waves coming from reader. While in case of active tags, they have their own power supply. Since the passive tags do not have power supply, the range is less compared to active and semi passive tags.

RFID readers come in many sizes. It may be hand held size or may be as big as that of doors, as we see in shopping malls.

Working

RFID belongs to a group of technologies referred to as Automatic Identification and Data Capture (AIDC). AIDC methods automatically identify objects, collect data about them, and enter those data directly into computer systems with little or no human intervention. RFID methods utilize radio waves to accomplish this.

At a simple level, RFID systems consist of three components: an RFID tag or smart label, an RFID reader, and an antenna. RFID tags contain an integrated circuit and an antenna, which is used to transmit data to the RFID reader (also called an interrogator). The reader then converts the radio waves to a more usable form of data. Information collected from the tags is then transferred through a communications interface to a host computer system, where the data can be stored in a database and analyzed at a later time.



Applications

- Inventory management (Product Tracing)
- Asset tracking
- Personnel tracking
- Toll Road Payments
- ID Badging (photo ID cards)
- Supply chain management
- Libraries
- Animals & Birds Tracking

4.6 GPS navigation

The Global Positioning System (GPS) was developed by the U.S. Department of Defence. The only system of its kind in the world, GPS uses the transmission of microwave signals from a network of 30 satellites orbiting 12,000 miles above Earth to pinpoint a receiver's location, as well as its speed and direction of travel.

A **Satellite navigation device**, called a **GPS receiver**, or simply a **GPS**, is a device that is capable of receiving information from GNSS satellites and then to calculate the device's geographical position. Using suitable software, the device may display the position on a map, and it may offer routing directions. The Global Positioning System (GPS) is one of a handful of global navigation satellite systems (GNSS) made up of a network of a minimum of 24, but currently 30, satellites placed into orbit by the U.S. Department of Defence.

GPS was originally developed for use by the United States military, but in the 1980s, the United States government allowed the system to be used for civilian purposes. Though the GPS satellite data is free and works anywhere in the world, the GPS device and the associated software must be bought or rented.

A satellite navigation device can retrieve (from one or more satellite systems) location and time information in all weather conditions, anywhere on or near the Earth. GPS reception requires an un unobstructed line of sight to four or more GPS satellites, and is subject to poor satellite signal conditions. In exceptionally poor signal conditions, for example in urban areas, satellite signals may exhibit multipath propagation where signals bounce off structures, or are weakened by meteorological conditions. Obstructed lines of sight may arise from a tree canopy or inside a structure, such as in a building, garage or tunnel.

The Russian Global Navigation Satellite System (GLONASS) was developed simultaneously with GPS, but suffered from incomplete coverage of the globe until the mid-2000s. GLONASS can be added to GPS devices to make more satellites available and enabling positions to be fixed more quickly and accurately, to within 2 meters.

Questions

Short answer type questions for 5 marks.

1. Explain the concept of FDMA, TDMA and CDMA techniques.
2. Write a short note on 2G, 3G and 4G of wireless communication.
3. Write a short note on Bluetooth.
4. Write a short note on Wi-Fi.
5. Write a short note on RFID technology.
6. Write a short note on GPS navigation.

---xxx---

***References*:**

To prepare the above e-content for the Unit No. 4, I have collected material from the following sources, websites & Links:

1. *wkipedia.org*
2. *slideplayer.com*
3. *itu.int*
4. *slideshare.net*
5. *cellphones.org*
6. *elprocus.com*
7. *youtube.com /All about Electronics*
8. *analogictips.com*
9. *nicer.in*

---xxx---