Choice Based Credit System
2 Credits

S.Y.B.Sc.

(Computer Science)

(Sem - IV)

E2

Electronics Paper-II

Course code: ELC-242

According to New CBCS
Syllabus w.e.f. 2020-21

A text book of

Wireless Communication & Internet of Things

Dr. Deepa Ramane

Innovation Throughout
VISION

CONTENTS

VISION

Unit 1

Wireless Communication: Cellular Telephony

1. Introduction

In 1897 Gugelielmo Marconi first demonstrated radio's ability to provide continuous contact with ships sailing the English channel. Since then mobility feature got attached to communication technology. Afterwards many new wireless communication methods and services have been enthusiastically adopted by people throughout the world. The past three decades have witnessed exponential growth in the wireless industry.

The term 'wireless' is often used to describe all types of devices and technologies that use air/ space as a data communication medium. Wireless communication is defined as the transmission of user information without the use of wires. The user information can be human voice, digital data, e-mail messages or video. Wireless communication is revolutionizing almost every aspect of our daily lives and is poised to continue expanding at a very fast pace. Using wireless communications sending and receiving of messages, browsing of the internet and accessing of corporate databases anywhere, anytime across the world has already become common.

2. Overview of Wireless Communication

Wireless communication is enjoying the fastest development in the history of science, due to the technologies that allow widespread deployment. Mobile telephony has penetrated in our day to day life. It is observed that there is phenomenal growth of wireless subscribers in the late 1990s.

We are coming across a wide range of wireless applications in our day to day life. It could be simple opening of door, security alarm, controlling of home entertainment equipments using remote, cordless telephones, bluetooth devices or cellular telephones. All are *examples* of radio communication systems. The impact of wireless communication is gradually increasing.

Wireless communication is allowing business to develop WANs, MANs and LANs without a cable installation. The IEEE has developed 802.11 as a standard for wireless LANs. The Bluetooth industry consortium is also working to provide better and better wireless technology.

Wireless technology has been using higher and higher frequencies that support greater data rates and throughput. Following table highlights some of the important stages in the development of wireless communication.

Year	Implementation	Specification
1896	Guglielmo Marconi - wireless telegraphy (Morse code - digital)	Operating at 1MHz
1906	1st World Radio Conference	-
1915	Wireless Voice Communication	
1920	Marconi Detected short waves	-
1960	Bell laboratory developed cellular concept	-
1992	Introduction of GSM (2G)	Entirely digital, 900 MHz, 124 channels. Data with 9.6 kbit/s
1997	Wireless LANs	IEEE-Standard, 2.4 - 2.5 GHz, 2 Mbit/s
1998	Universal Mobile Telecommunication System (UMTS)	
2000, 2010-2013, 2020	Bluetooth Specification & Implementation of 3G,4G,5G	

The reason of popularity and growth of wireless communication technology is clearly understood by following table.

	Wired Communication	Wireless Communication
i.	In wired communication wired medium conducts electrical signal information from one fixed terminal to another.	Wireless medium is of broadcast nature.
ii.	It provides reliable guided link.	It's unreliable as compared to wired communication.
iii.	Wired medium does not support mobility.	Wireless medium supports mobility.
iv.	This has high bandwidth and addition of cables in general can duplicate the wired medium and increase the bandwidth.	This has low bandwidth.
v.	Different signals are conducted through different types of wires such as co-axial cable, twisted pair cable, optical fiber etc.	All signals are transmitted over the same medium, i.e., air.
vi.	Complicated and expensive.	Simple and inexpensive.

3. Introduction of Cellular Telephony System

In 1960, Bell Laboratories developed the concept of cellular telephony system. Over the year this concept matured and the cellular or mobile communication captured the world and is witnessing a phenomenal growth in number of subscribers and advancement in cellular technology. There has been a clear shift from fixed to cellular telephony. Both the mobile network operators and vendors have felt the importance of efficient networks with equally efficient design.

The cellular wireless generation (G) generally refers to a change in the fundamental nature of the service and frequency spectrum used for transmission. New generations have appeared in every ten years, since the first move from 1981 - An analog (1G) to digital (2G) network. After that, there was multimedia support and spread spectrum transmission. These are the features of 3G. Year 2011, witnessed 4G - IP switched networks. Next generation is witnessing re-configurable, multi- core technology.

3.1 Cellular Concept

The term 'mobile' is used to classify any radio terminal that could be moved during the operation. Firstly developed conventional mobile system had a high power transmitters to cover large geographical area, may be an entire city. *Major drawbacks of this system were*:

i. When mobile user was moving from one geographical area to other, user's call used to drop and he had to initiate the call again.

ii. Inefficient spectrum utilization.

The above two drawbacks of conventional mobile system are eliminated in cellular mobile system. The basic idea is to use many low power transmitters instead of single high power transmitter. Each small power transmitter covers a small portion of the service area.

The concept of cellular mobile system is explained in detail in the following paragraphs:

i. A large geographical area is divided into smaller areas; each one is called as cell. While forming the cells, two properties are followed:
   a. no gap between two neighboring cells and
   b. no overlap between two cells

ii. Each cell has a base station which serves all the local mobile stations in the cell. The base station has its own frequency spectrum. Each base station has transmitter, receiver and control unit.

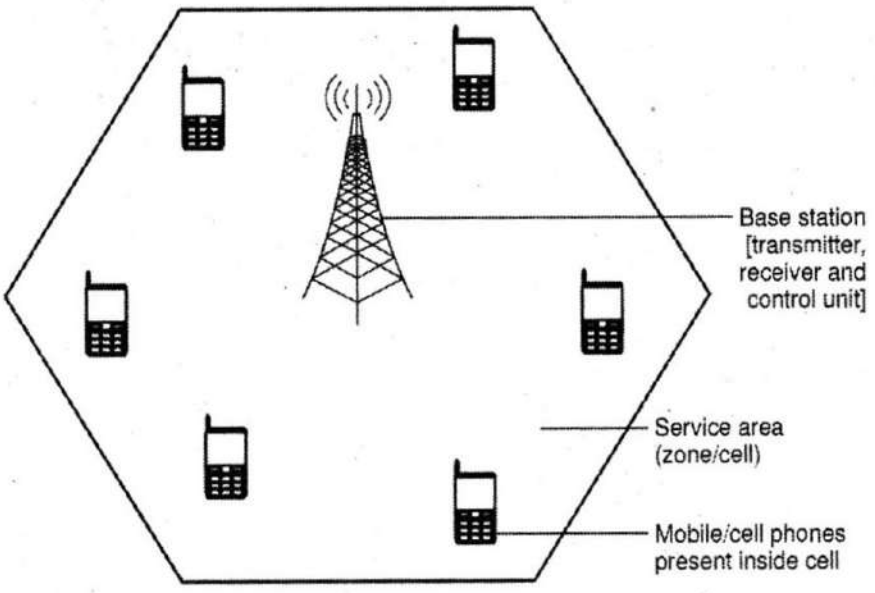
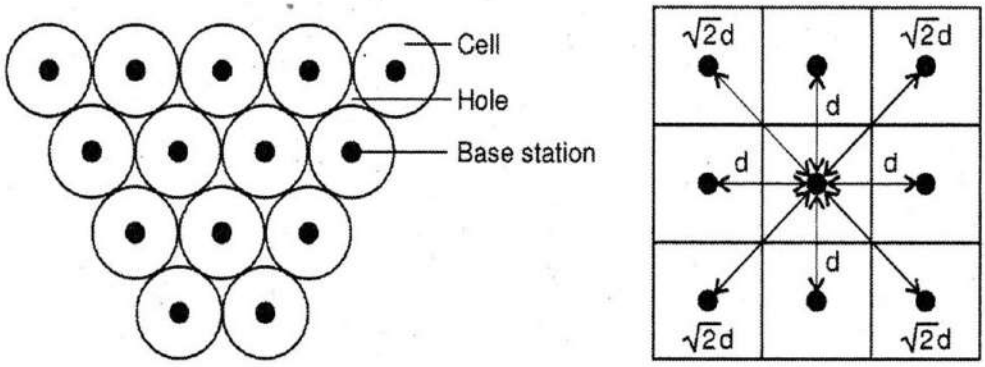


Figure 1.1 : Individual Cell

iii. The shape of the cell is a major design aspect in cellular system. Various shapes possible are circular, square, triangular etc. But in circular shape, some geographical area is present, where no base station can serve the mobile users. It is called 'Hole'. The square shape is not ideal, as mobile users within cells are not equidistant from the adjacent antennas.



(a) Circular shape cell (b) Square shape cell

Figure 1.2: Cellular structure sizes

iv. A hexagonal shape is the ideal one. Reasons are:

a. The hexagonal pattern provides equidistant antennas.

b. It provides a theoretical coverage of an area without any overlapping cells or gaps in the coverage area (no 'Holes').

c. The use of hexagons makes the theoretical calculations of system parameters easy.

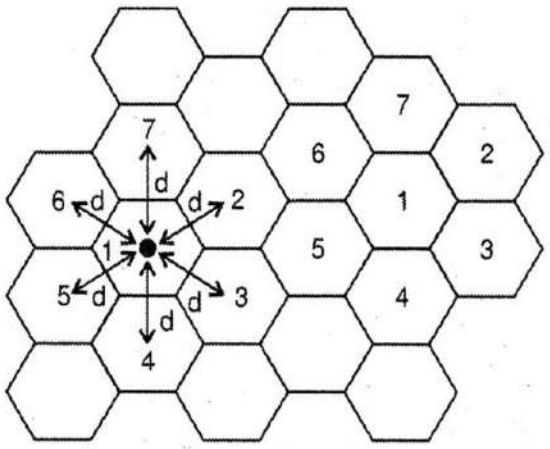
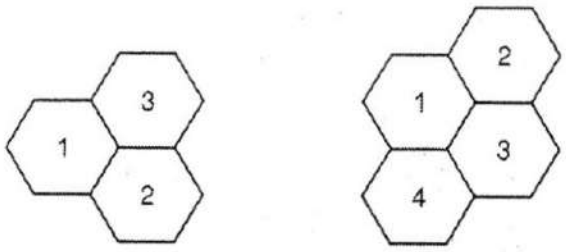


Figure 1.3: Hexagonal pattern of cellular system (seven-cell cluster)

v. In practice, a precise hexagonal pattern is not used. Variations from the ideal are seen due to terrain architecture and practical limitation on siting antennas due to buildings, trees etc. Moreover cell sizes are smaller in crowded / densely populated area.

vi. As seen in *figure 1.4*, the cells are hexagons with the base station at the center. The N cells which collectively use the available frequency spectrum is called a **cluster**. Only certain cluster sizes are allowed. Typical cluster sizes are 3, 4, 7 and 12.



3-Cell cluster **4-Cell cluster**

Figure 1.4: Formation of Cell Cluster

vii. The capacity of cellular system is dependent on the number of frequency channels that can be allocated within a cell and the cell size. If, n is the number of users that can communicate simultaneously, then

$$n = \frac{m\,(BW_{total}/N)}{BW_{user}}$$

where, m = no. of cells required to cover an area

BW_{total} = total frequency spectrum allocated for cell

BW_{user} = required bandwidth for individual user

N = frequency reuse factor

Thus, capacity of the cellular system can be increased by

a. increasing m

b. decreasing frequency reuse factor.

viii. Classification of cellular technology depending upon the coverage area:

a. *Femtocell:* It is a small, low-power cellular base station, typically designed to cover a range of only few meters. They are used in homes or for small offices. Mobile phone utilizes less power hence battery life is longer.

b. *Picocell:* It is a small cellular base station typically covering an area in the range of a few tens of meters. It is used in buildings, shopping malls, train stations etc.

c. *Microcell:* The microcell covers the range of few hundreds of meter. It is useful for big shopping complexes, transportation hub covering larger range than picocell.

d. *Macrocell:* The macrocell covers the range of few km. So it is used in urban areas and its antennas are mounted above the roof top of the buildings. It provides excellent mobile phone services such as high data rates and capacity.

ix. Cell splitting: In practice, the distribution of traffic and topographic features is not uniform. Cells in areas of high usage can be split into smaller cells. Generally, the original cells are about 6.5 to 13 km in size. The cells can themselves be split into small size of 1.5 km. The power level used also reduces. A radius reduction by a factor of F reduces the coverage area and increases the no. of required base stations by a factor of F^2.

With cell splitting, a cell is divided into a number of wedge-shaped sectors. Each has its own set of channels, typically 3 or 6 sectors per cell.

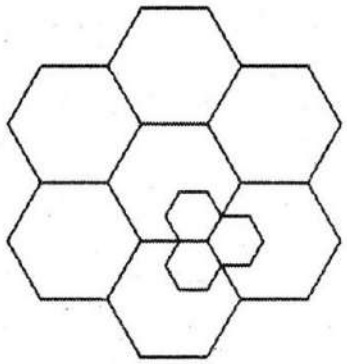


Figure 1.5: Cell Splitting

3.2 Frequency Reuse Concept

In previous section, we have seen cellular concept used in cellular telephony system. Now we will study frequency spectrum allocation to the cells. Frequency spectrum is allocated cluster wise. This spectrum is further subdivided into small frequency spectrums. Each cell in the cluster has allocated unique frequency spectrum. The same set of frequency spectrums can be reused by another cluster which is separated by a considerable distance with minimal interference.

Thus same frequency band can be used for multiple conversations simultaneously by different cells. This is referred to as **frequency reuse**.

In short,

- Frequency reuse is the process of using the same set of frequencies to more than one cell.
- The frequency reuse pattern depends on transmitter power of base station, cell size and cluster size.
- The minimum distance between the centers of two cells using the same frequency band is called as **reuse distance** and is denoted by 'D'.

The frequency reuse pattern and reuse distance for seven cell cluster arrangement is shown in *figure 1.6*. Here seven sets of frequency spectrums f_1, f_2, f_3, f_4, f_5, f_6 and f_7 are used.

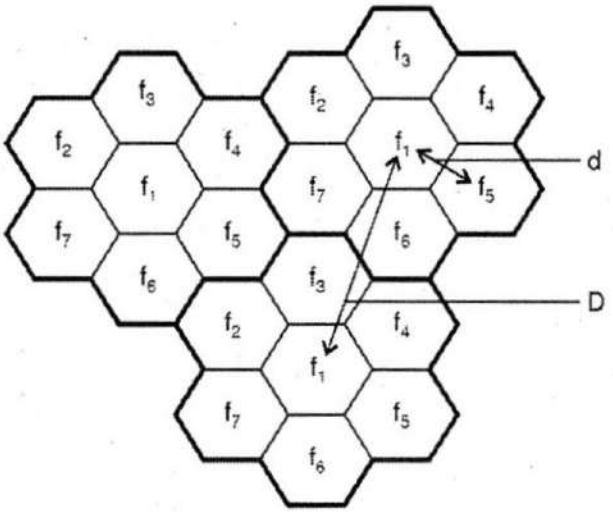


Figure 1.6: Frequency reuse for seven cell cluster

- The reuse distance 'D' is given by

$$\boxed{D = d\sqrt{N}}$$

where, d = distance between centers of adjacent cells

N = no. of cells in a cluster, i.e., cluster size

Example

▸▸1. For a mobile system of cluster size of 12, determine the frequency reuse distance if distance between two adjacent cells is 5 km.

Solution

Frequency reuse distance, $D = d\sqrt{N}$

$= 5\text{ km} \times \sqrt{12}$

$= 17.32\text{ km}$

Thus to repeat the frequency pattern the frequency reuse distance between the cells should be greater than or equal to 17.32 km for cluster size of 12.

3.3 Handoff Concept

We have seen that each cell activities are managed by the base station. Sometimes base station is also called as MTSO (Mobile Telephony Switching Office). Each mobile present in the cell, communicates the information to the base station. Further base station route the information to the communication network through the system called as Mobile Switching Center (MSC). MSC is a core part of GSM/CDMA network system which connects calls between subscribes by switching the digital packets between network paths.

When a mobile is moving from one cell to another cell, the control needs to be transferred from old base station to base station of new cell. This is accomplished by handoff technique. This handoff requires two operations:

i. To identify a new base station

ii. To transfer control of mobile from old base station to new base station

Thus ***handoff*** processing is an important task in any cellular system. It is defined as -

When the subscriber is moving between cells, during a journey, the communication with the base station of the departing cell ceases and communication with the base station of the entering cells commences. Thus, simply, it is the ability to transfer mobile control from one base station to another base station.

Handoff must be performed successfully without any discontinuation in communication. It assures the continuity of calls. Handoff of a call to a new base station implies transfer of all functions.

Handoff Mechanism

i. Each mobile continuously emits signals for base station.

ii. System designer sets an optimum signal level, called as threshold level, at which handoff is to be initiated.

iii. The base station continuously monitors the signal strength emitted by each mobile in the cell. Depending upon the strength, the decision for handoff is made.

iv. When the received signal strength goes below the threshold level, the handoff is initiated. This is an indication that mobile device is at the boundary of the cell.

v. At the border between two cells, the subscriber is under the influence of two or three base stations.

vi. The control of mobile device will be handover to the base station which receives the strongest signal.

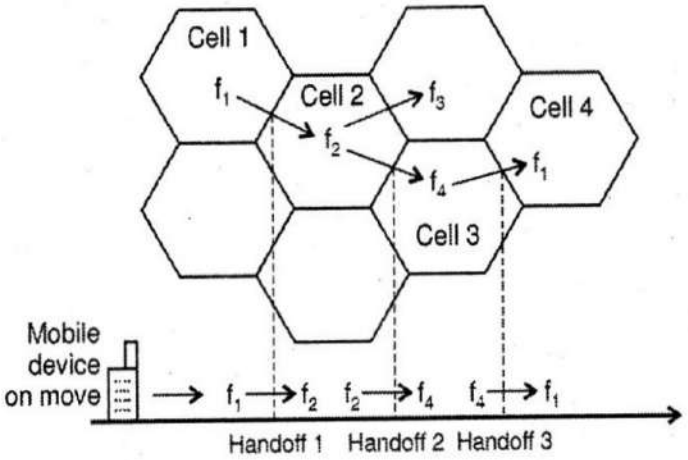


Figure 1.7: Handoff

As seen in *figure 1.7*, mobile has moved from cell 1 → Cell 2 → Cell 3 → Cell 4. During this travel, three times hand-off process has accomplished. When it enters into new cell, frequency band of operation also changes. Thus mobile had used f_1, f_2, f_4 and f_1 frequencies respectively.

3.4 Interference

Interference is the major limiting factor in the performance of mobile communication systems. There can be 'n' reasons for this interference:

i. Due to mobile devices present in the same cell

ii. A call in progress in a neighboring cell

iii. Other base stations operating in the same frequency band

Interference causes cross talk. It may lead to missed and blocked calls due to errors in the digital signaling. It's effect is remarkable in urban areas because of greater RF noise and large no. of base stations and mobiles. There are two types of system generated cellular interference:

a. Co-channel interference

b. Adjacent channel interference

a. Co-channel Interference

We have studied frequency reuse concept used in cellular technology. It means that in a given coverage area, there are several cells that use the same set of frequencies. These cells are called co-channel cells and the interference between signals from these cells is called ***co-channel interference***.

Co-channel interference can be reduced by physically separating co-channel cells by a minimum distance to provide sufficient isolation. When the size of each cell is approximately the same and the base station transmits the same power, the co-channel interference ratio is independent of the transmitted power. It is a function of the radius of the cell (R) and the distance between centers of the nearest co-channel cells (D). If the ratio D/R is increased, the spatial separation between co-channel cells relative to the coverage distance of a cell increases. This will reduce interference. The parameter, Q, is defined as the co-channel reuse ratio, related to the cluster size.

For a hexagonal geometry,

$$Q = \frac{D}{R} = \sqrt{3N}$$

Higher the value of Q, smaller is the level of co-channel interference.

b. Adjacent Channel Interference

Interference due to signals which are adjacent in frequency is called as adjacent channel interference. It occurs due to improper filter design of receiver which allows nearby frequencies to enter into the passband. The near-far effect is observed when a nearby transmitter captures the receiver of the subscriber. The effect can also occur when a mobile close to a base station transmits on a channel and this channel is closed to the channel used by a weak mobile. In such cases, the base station finds difficulty in locating the desired mobile user.

Adjacent channel interference can be reduced by proper filter design and channel assignments. In a given cell, if the frequencies between two channels are separated by a maximum, the adjacent channel interference reduces considerably. Even some channel allocation schemes avoid the use of adjacent channels in neighbouring cell sites.

3.5 Block Diagram of Mobile Handset

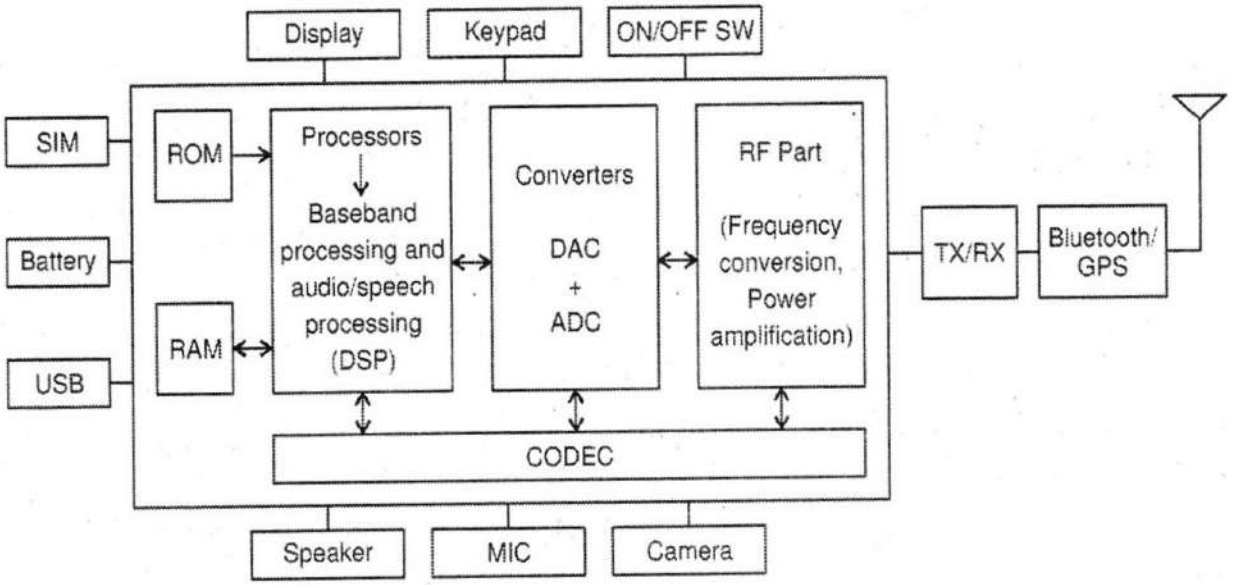


Figure 1.8: Mobile handset

A mobile handset is essentially a two-way radio, consisting of a radio transmitter and a radio receiver. When user talks / texts using mobile phone, basically phone converts voice / text messages into an electromagnetic signal, which is then transmitted via radio waves to the nearest cell tower.

The architecture of the mobile device consists of Hardware and Software.

A. Hardware

Figure 1.8 shows hardware architecture of mobile handset. Basic components of mobile device are:

a. CPU
b. Memory (RAM and ROM)
c. Digital Signal Processors (DSP)
d. D/A and A/D converters
e. Frequency converter and RF power amplifiers
f. I/O peripherals such as speaker, mic, camera, keypad, display, USB, GPS, bluetooth and wifi
g. SIM
h. Transmitter and receiver circuits
i. Antenna
j. Battery

Functioning of each of the above is explained in subsequent paragraphs.

- **Processor:** Heart of the mobile handset is **processor**. The processors used in smartphones are quite different from those used in a PC or laptop because they have different design constraints. Here, one has to balance power consumption against performance and cost. New smart phones have more than one processor (such as quad-core, octa-core processors). Processor controls all other I/O peripheral devices such as display, keypad, bluetooth etc. The radio signals are handled by baseband processor which in turn communicates with other processors to use their functionalities. Power and audio processors control the functioning of speaker and microphone with the help of application processor.
- **Memory:** The device needs **memory** to store OS as well as data. Modern handsets have a large volatile memory (SDRAM) of 8 GB and larger non-volatile storage, typically more than 64 GB.
- **Peripheral devices:** Mobile device needs many I/O peripheral devices through which the end-user interacts with the smartphone. The OS needs to have the driver

software installed for each device. Typical peripheral devices are already listed above.

- **SIM - Subscriber Identification Module**, widely known as SIM card, is a small integrated microchip that securely stores the information which is used to identify and authenticate subscriber on the network. It contains a unique serial number, International Mobile Subscriber Identity (IMSI) number, security authentication and ciphering information, temporary information related to the local network and two passwords: a Personal Identification Number (PIN) for ordinary use and Personal Unblocking Key (PUK) for PIN unlocking.
- **Transmitter and receiver circuits:** The receiver hardware receives incoming signal and generates interrupts for the radio interface in OS. After the reception, a physical layer handshake takes place. Thus the incoming audio, video and data are processed by the modem processor. This data is given to display, speaker etc. through radio OS components.

  Similarly during transmission, the audio / video data from microphone / camera etc. is written into the memory by the radio OS components. These data are then processed by the modem processor as per the transmission protocol.
- **Antenna:** Cell phones contain at least one radio antenna to transmit / receive radio signals. An antenna is a metallic element which converts electric signal into electromagnetic signal. The antennas are of specific sizes and shapes for transmitting and receiving specific frequencies. Some phones (such as iPhone) have multiple transmitting or receiving antennas. In addition to cellular antenna, smartphones also have Wi-Fi, bluetooth and /or GPS antennas.
- **Battery:** It provides the power for the functioning of all components. A modern handset typically uses a lithium-ion battery whereas older handsets used nickel-metal hydride batteries.

  The average phone battery lasts 2-3 years at best. Battery life can be extended by draining it regularly, not overcharging it and keeping it away from heat.

B. **Software:** *Feature* phones have basic software options while smartphones have advanced software platforms. Since 2011, mostly Android OS is used.

4. Overview of Cellular Telephony Generations

The evolution of mobile communication has witnessed rapid progress in technology and in the services, it is providing. The cellular concept was first developed in 1960s and 1970s. The worldwide cellular and personal communication subscriber surpassed 700 million users till 2000 and still exponential growth is being observed.

The evolution of mobile communication system is progressing through different generations. Next generation cellular networks are being designed to facilitate high speed data communication traffic in addition to voice calls. New standards and technologies are being implemented to allow wireless networks to replace fiber optic or copper wires. To support higher data rate, increase channel capacity, to accommodate more number of users to provide reliable and secure services, the advance digital modulation techniques, multiplexing and multiple access techniques are developed.

4.1 2G Cellular Network

First generation (1G) cellular systems was relying on FDMA / FDD and analog frequency modulation technique. Second generation (2G) was first introduced in the early 1990s and started using digital modulation techniques. New multiple access techniques such as TDMA and CDMA were introduced.

A. Three most popular TDMA standards of second generation are:

i. GSM developed supported eight time slotted users for each 200 kHz radio channel and has been deployed widely by service providers in Europe, Asia and Australia and South America.

ii. Interim Standard 136 (IS136) was developed which supported three time slotted users for each 30 kHz radio channel. It became popular in North America, South America and Australia.

iii. Pacific digital cellular standard known as Japanese TDMA standard was developed which was similar to IS-136.

B. Popular CDMA standard of second generation includes Code Division Multiple Access (IS-95) i.e. CDMA1. It supported 64 users that are orthogonally coded and simultaneously transmitted on each 1.25 MHz channel.

In many countries, 2G wireless networks are designed and deployed for conventional mobile telephone service to increase capacity. Above mentioned standards represent the first set of wireless air interface standards. It uses digital modulation and digital signal processing in the handset and the base station. However, circuit-switched data modems used by 2G has limit data users to a single circuit-switched voice channel. So data transmission in 2G are generally limited to the data throughput rate of an individual user. This standard is able to support limited internet browsing and short messaging capabilities (SMS) using a circuit switched approach.

4.2 2.5G Cellular Network

To support modern internet applications, throughput data rate of 2G needs to be increased. So new data centric standards were developed under 2.5G technology. It allowed existing 2G equipments to be modified and to upgrade software to support higher data rate transmissions for web browsing, e-mail traffic, mobile commerce and location-based mobile services. The 2.5G technologies also support a popular new browsing format language, called Wireless Application Protocol (WAP). WAP allows standard webpages to be viewed in a compressed format specifically designed for small, portable handheld wireless devices.

2.5G cellular network witnesses three upgradations:

i. High Speed Circuit Switched Data (HSCSD)

ii. General Packet Radio Service (GPRS)

iii. Enhanced Data Rates for GSM Evolution (EDGE)

These options provide remarkable increase in internet access speed over 2G-GSM and IS-136 technology.

4.3 3G Cellular Network

3G systems have advance features of wireless access. The advantages of this system are:

i. Multi-megabit internet access

ii. Communications using Voice Over Internet Protocol (VOIP)

iii. Voice-activated calls

iv. Un-parallel network capacity

v. 'Always-on' access

The eventual 3G evolution for CDMA systems leads to CDMA2000 and wideband CDMA (W-CDMA). W-CDMA is based on the network fundamentals of GSM, as well as mixed version of GSM and IS-136 through EDGE.

CDMA2000 and W-CDMA remained popular in early years of 21st century. It provides higher data rates in new bands. New radio spectrum bands defined in 3G network system are 2500-2690 MHz, 1710-1885 MHz and 806-960 MHz.

3G W-CDMA (UMTS)

The Universal Mobile Telecommunications System (UMTS) standard is designed in 1996. Several wideband CDMA proposals were merged into a single W-CDMA standard and then called as UMTS. It is backward compatible with the second generation GSM. It provided new CDMA interface with additional capacity and bandwidth. It retained the network structure and bit level packaging of GSM data.

The 3G W-CDMA standard had been designed for "always-on" packet-based wireless service. Due to this, the same wireless network can be shared by computers, telephones, entertainment devices for connection to the internet, anytime, anywhere.

Features of W-CDMA

i. Supported data rates upto 2.048 Mbps per user, thus allowing high quality data.

ii. Services provided to consumers - multimedia, streaming video and broadcast-type.

iii. Public and private network features.

iv. Provided video conferencing and Virtual Home Entertainment (VHE).

v. Ensured broadcasting, mobile commerce, games, interactive video and virtual private networking.

vi. Required a minimum spectrum allocation of 5 MHz and supported 100-350 simultaneous voice calls.

vii. Wider bandwidth of W-CDMA demanded a change of RF equipment at each base station. So installation became expensive.

4.4 4G Cellular Network

The 4G system was originally put forward by DARPA, the US Defense Advanced Research Project Agency. It was designed primarily for data and IP-based protocols. It has distributed architecture and end-to-end Internet Protocol (IP). It was five times faster than 3G network and can provide speeds of upto 100 Mbps. All mobile models released after the year 2013 support this network which offers connectivity for tablets, laptops and smartphones.

Features of 4G

i. Better latency

ii. Higher voice quality

iii. Easy access to instant messaging services and social media

iv. Quality streaming

4G-LTE

In 2009, first release Long Term Evolution (LTE) was deployed in Oslo, Norway and Sweden. It is a wireless communication with high speed.

LTE is comprised of following three main components:

i. The User Equipment (UE)

ii. The Evolved UMTS Terrestrial Radio Access Network (E-UTRAN)

iii. The Evolved Packet Core (EPC)

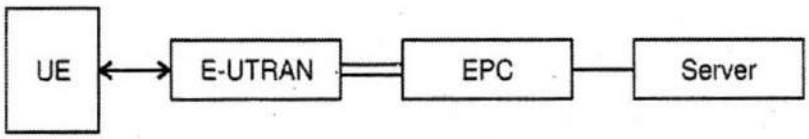


Figure 1.9: LTE

i. **User Equipment** is nothing but mobile equipment of LTE and is same as the one used by UMTS and GSM.

ii. **E-UTRAN** handles radio communications between the mobile and the evolved packet core. It consists of evolved base stations. LTE mobile communicates with just one base station and one cell at a time.

iii. **EPC** performs the function of mobility handling, IP address allocation, packet filtering and also takes care of security. It communicates with packet data networks in the outside world such as the internet, private corporate networks or the IP multimedia subsystems.

4.5 5G Cellular Network

The primary goal of previous generations of mobile networks has been to simply offer fast, reliable mobile data services to network users. 5G has broadened the scope to offer a broad range of wireless services delivered to the end user across multiple access platforms and multi-layer networks.

Features of 5G

i. Dynamic, coherent and flexible framework of multiple advanced technologies.

ii. 5G architecture utilizes Radio Access Networks (RAN).

iii. Created additional data access points.

iv. No need of having complex infrastructure or proximity base station.

v. Architecture is much more service oriented.

vi. Frequency spectrum is in between 30 GHz - 300 GHz.

vii. Multi-Access Edge Computing (MEC) is an important element of 5G architecture. It is an evolution in cloud computing. This has created a shortcut between the user and the host during content delivery.

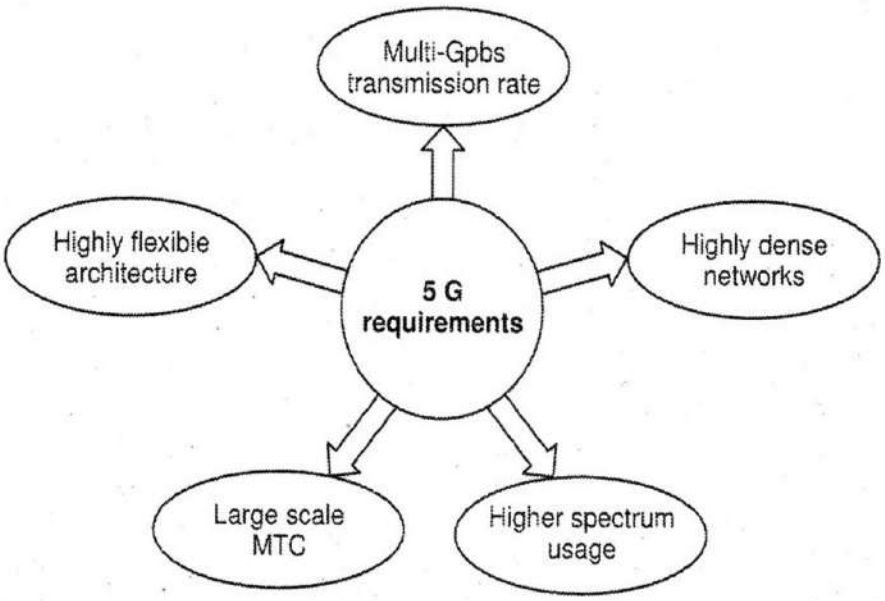


Figure 1.10: Key requirements for 5G

4.6 Comparative Study of Generations of Mobile Communication

Figure 1.11 represents comparative study of generations of mobile communication

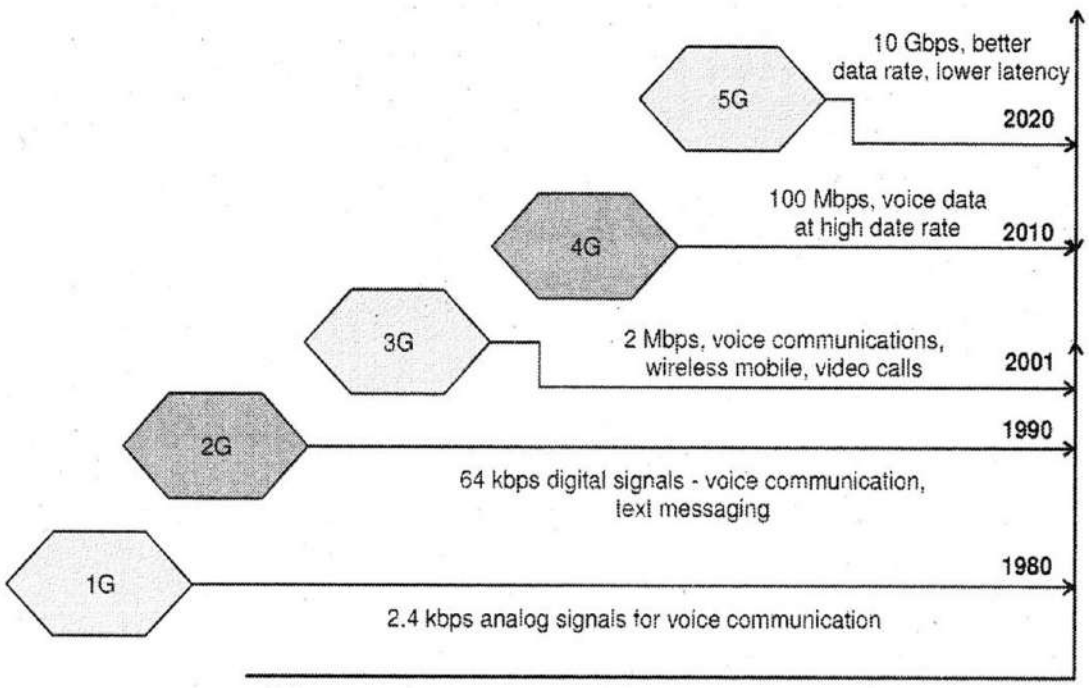


Figure 1.11: Overview of Generation of Mobile Communication

5. GSM (Global System for Mobile)

5.1 Introduction

The core data network that provides the main control and interfacing of the whole mobile network is GSM system. To establish the communication between two mobile devices is the basic task of mobile network system. To accomplish this task, a number of function needs to be performed such as:

- identifying the called person
- determining the location
- routing the call and ensuring that the connection is sustained as long as the communication lasts.
- After the completion of transmission, the connection is terminated and (normally) the calling user is charged for the service he/she has used.

In a fixed telephone network, the above operations are relatively easy, because the locations of source and destination are permanent from the network's point of view. In a mobile network, however, the establishment of a call is far more complex task as the wireless (radio) connection enables the users to move with steady network services anywhere. In practice, the network has to find solutions to three problems before it can even set up a call:

i. Where is the subscriber?

ii. Who is the subscriber?

iii. What does the subscriber wants?

In other words, the subscriber has to be **located** and **identified** to provide him/her with the requested **services.** These three operations are carried out by GSM.

5.2 The Architecture of GSM

The operations of GSM to locate the subscriber, to identify him/her and to provide the service are carried out by GSM using its architecture shown in *figure 1.12.*

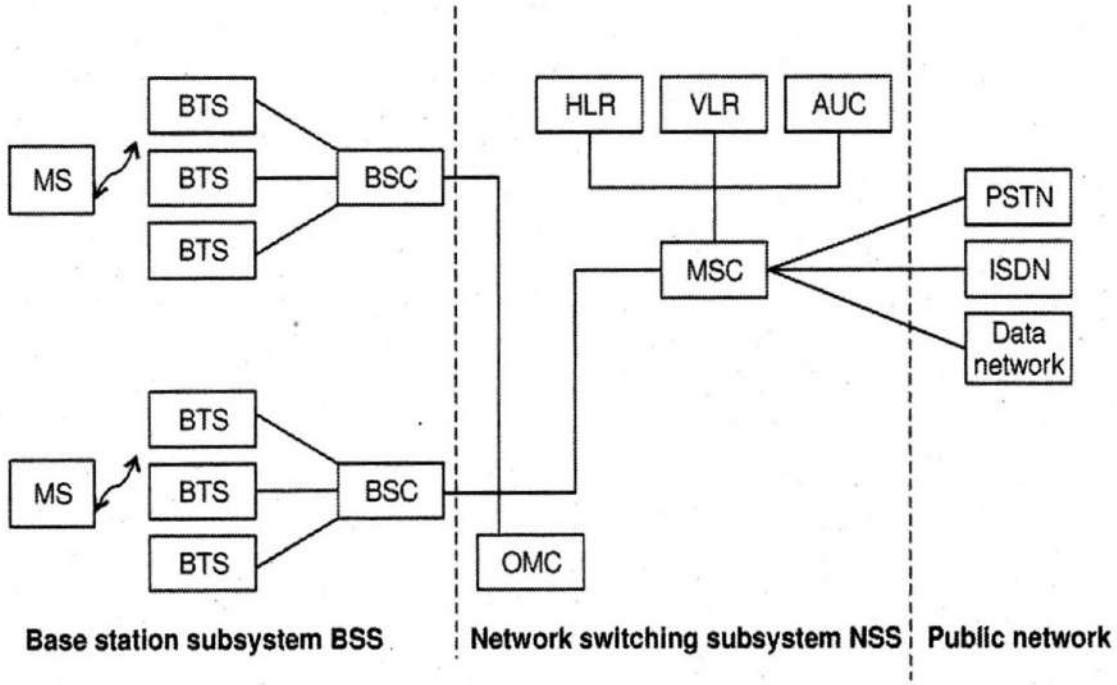


Figure 1.12: GSM System Architecture

The GSM architecture consists of

i. Mobile Station

ii. Base Station Subsystem (BSS)

iii. Network Switching Subsystem (NSS)

iv. Network Management Subsystem (NMS)

v. OMC (Operation and Maintenance)

The calls are originated and terminated at Mobile Station. The network establishment for calls is the responsibility of the subsystems NSS and BSS. The NMS controls the whole GSM network while OMC takes care of maintenance of the GSM network.

Each block functioning is explained in detail here.

A. Mobile Station (MS)

In GSM, the Mobile station is nothing but user equipment supported by necessary software for communication. It is a combination of mobile equipment (ME) and subscriber data card i.e. SIM (Subscriber Identity Module) card. Therefore, MS = ME + SIM.

Mobile equipment handles functions of radio transmission, speech encoding/decoding, error detection/correction and access to the SIM. SIM card is a removable subscriber's identification token storing the IMSI (International Mobile Subscriber Indentity), a unique key shared with the mobile network operator and other data. The SIM card also contains tools needed for authentication and ciphering.

B. Network Switching Sub-systems (NSS)

The Network Switching Subsystem (NSS) contains the network elements MSC, VLR, HLR, AUC, EIR. The main functions of NSS are:

i. *Call control*: This identifies the subscriber, establishes a call, and clears the connection after the conversation is over.

ii. *Charging*: This collects the charging details about a call/service and transfers it to the Billing Centre.

iii. *Mobility management*: This maintains information about the subscriber's location.

iv. *Signaling*: This applies to interfaces with the BSS and PSTN.

v. *Subscriber data handling*: This is the permanent data storage in the HLR and temporary storage of relevant data in the VLR.

Now let us study blocks of NSS units.

a. **Mobile Services Switching Centre (MSC):** The MSC acts as a bridge between a mobile network and a fixed network. So it is also called as Gateway MSC. The MSC performs following tasks:

- Call control: Identifying type of call, the destination and origin of call etc.
- Locating a particular mobile station
- Charging Data Collection

b. **Visitor Location Register (VLR):** VLR is a database which contains information about subscribers which are currently present in MSC's service area. It stores

- Identification numbers of the subscribers
- Security information for authentication of the SIM card and for ciphering
- Details of the services that the subscriber can use

c. **Home Location Register (HLR):** HLR is a huge database which stores administrative information of the mobile subscriber. HLR also keeps track of the current location of its customers, service restrictions and supplementary services.

d. **Equipment Identity Register (EIR):** The EIR is a list of all valid/non valid/stolen mobiles on the network. If a mobile has been reported stolen or not approved, then it may not be allowed to operate in the network. The equipments are identified by their unique IMEI number.

The EIR contains three lists:

- A mobile equipment in the *white list* is allowed to operate normally.
- If we suspect that a mobile equipment is faulty, we can monitor it. It is then placed in the grey list.
- If the mobile equipment is reported stolen, or it is otherwise not allowed, it is placed in the black list.

e. **Authentication Centre (AuC):** The AuC is a database containing a copy of the secret key present in each of the user's SIM cards. This is used to enable authentication and encryption over the radio link. The AuC uses a **Challenge - Response** technique, where it will send a random number to the mobile station; the mobile station encrypts this and returns it. The AuC will now decrypt the received number and if it is successfully decrypted to the number originally sent, then the mobile station is authenticated and admitted to the network.

C. Base Station Subsystem (BSS)

Base Subsystem is responsible for managing the radio network. BSS consists of the following elements:

a. Base Station Controller (BSC)

b. Base Transceiver Station (BTS)

c. TC (Transcoder)

a. **Base Station Controller:** Important tasks of BSC are:

- Connection Establishment between MS and NSS.
- Initialization of handovers while going from one cell to another

c. **Home Location Register (HLR):** HLR is a huge database which stores administrative information of the mobile subscriber. HLR also keeps track of the current location of its customers, service restrictions and supplementary services.

d. **Equipment Identity Register (EIR):** The EIR is a list of all valid/non valid/stolen mobiles on the network. If a mobile has been reported stolen or not approved, then it may not be allowed to operate in the network. The equipments are identified by their unique IMEI number.

The EIR contains three lists:

- A mobile equipment in the *white list* is allowed to operate normally.
- If we suspect that a mobile equipment is faulty, we can monitor it. It is then placed in the grey list.
- If the mobile equipment is reported stolen, or it is otherwise not allowed, it is placed in the black list.

e. **Authentication Centre (AuC):** The AuC is a database containing a copy of the secret key present in each of the user's SIM cards. This is used to enable authentication and encryption over the radio link. The AuC uses a **Challenge - Response** technique, where it will send a random number to the mobile station; the mobile station encrypts this and returns it. The AuC will now decrypt the received number and if it is successfully decrypted to the number originally sent, then the mobile station is authenticated and admitted to the network.

C. Base Station Subsystem (BSS)

Base Subsystem is responsible for managing the radio network. BSS consists of the following elements:

a. Base Station Controller (BSC)

b. Base Transceiver Station (BTS)

c. TC (Transcoder)

a. **Base Station Controller:** Important tasks of BSC are:

- Connection Establishment between MS and NSS.
- Initialization of handovers while going from one cell to another

- Routing of information from BTS to NSS
- Controlling BTS and TC control

b. **Base Transceiver Station (BTS):** BTS is the network element responsible for minimizing the transmission problems. Tasks of *BTS* are given below:

- Ciphering: Transmitted speech and data are encrypted and decrypted for protection.
- Speech processing: For error free connection speech data is processed (coding, interleaving, and burst formatting etc.).

c. **TC-Transcoder:** It compresses the digital speech. It also enables DTX (Discontinuous transmission), during a call when there is no conversation. It reduces the interference and save MS battery.

D. Network Management Subsystem (NMS)

The NMS monitors various functions and elements of the network. It mainly performs three types of functions:

i. **Fault Management:** The system maintains the current and previous status of alarm events.

ii. **Configuration Management:** It maintains information about the operation and configuration status of the network elements. It's functions include the management of the radio network, software and hardware management of the network elements, time synchronization and security operations.

iii. **Performance Management:** In performance management, the NMS collects data from individual network elements and stores it in a database. The database is used to analyze the performance of the network and suggests for improvement.

5.3 Handovers in GSM

The process of handover within any cellular system is of great importance. It is a critical process and if performed incorrectly handover can result in discontinuation in service or drop of calls. Within the GSM system, four types of handovers can occur.

i. **Intra-BTS Handover:** This form of GSM handover occurs if it is required to change the frequency being used by a mobile because of interference, or any other reason. In this type of GSM handover, the mobile remains attached to the same base station transceiver, but changes the frequency.

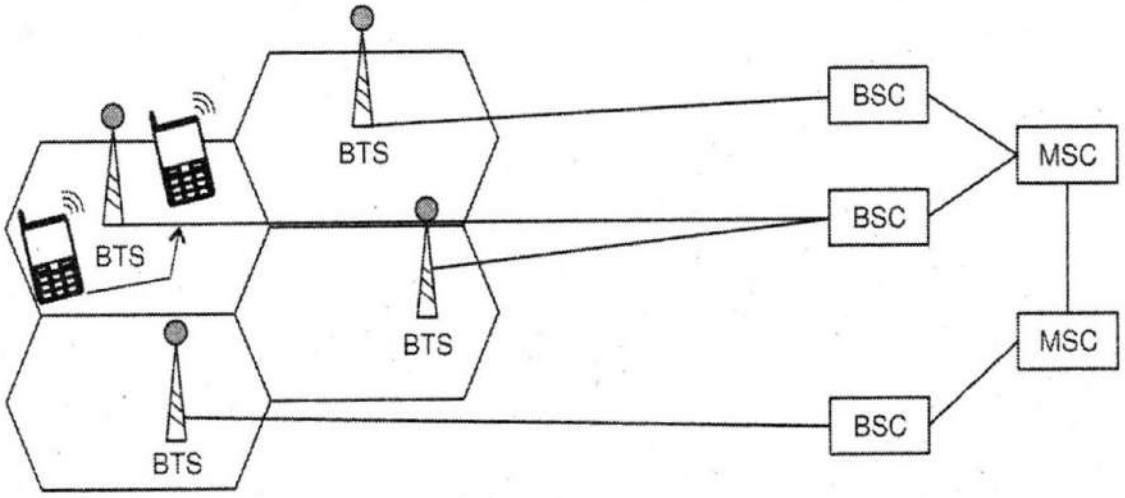


Figure 1.13: Intra-BTS Handover

ii. **Inter-BTS Intra BSC Handover:** This occurs when the mobile moves out of the coverage area of one BTS but into another controlled by the same BSC. In such situation, a new channel and slot is assigned to the mobile, before releasing the old BTS from communicating with the mobile.

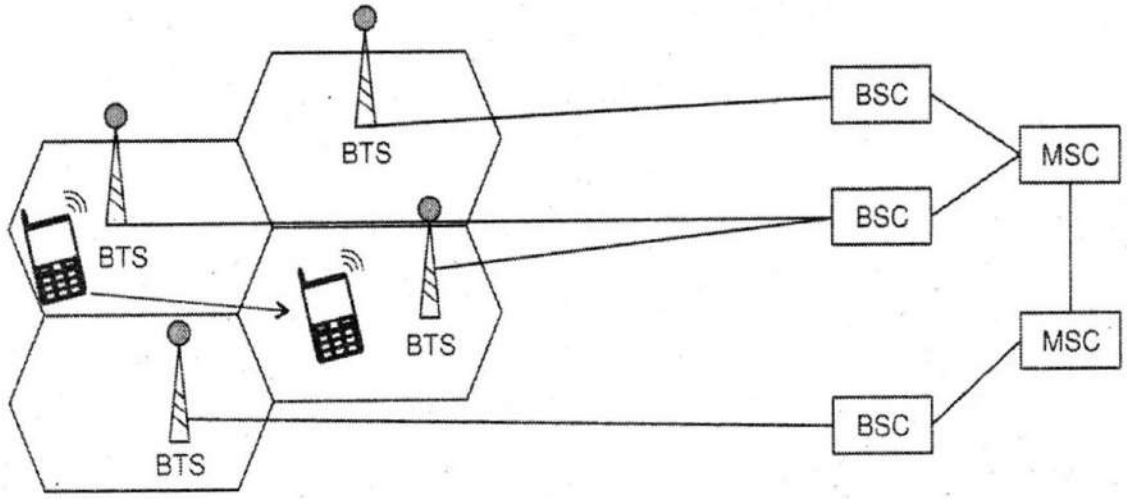


Figure 1.14: Inter-BTS Intra BSC Handover

iii. **Inter-BSC Handover:** When the mobile moves out of the range of cells controlled by one BSC to another. For this handover is controlled by the MSC.

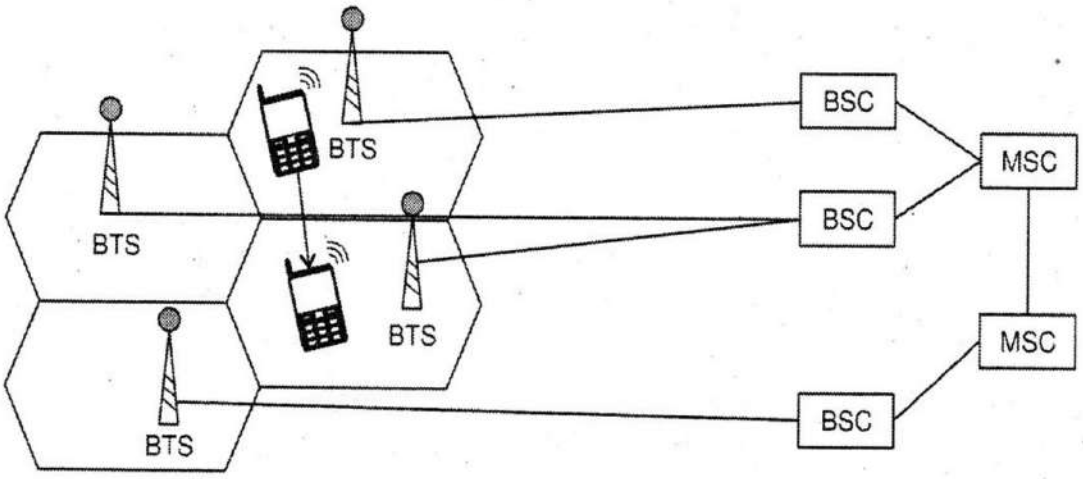


Figure 1.15: Inter-BSC Handover

iv. **Inter-MSC Handover:** This form of handover occurs when changing between networks. The two MSCs involved negotiate to control the handover.

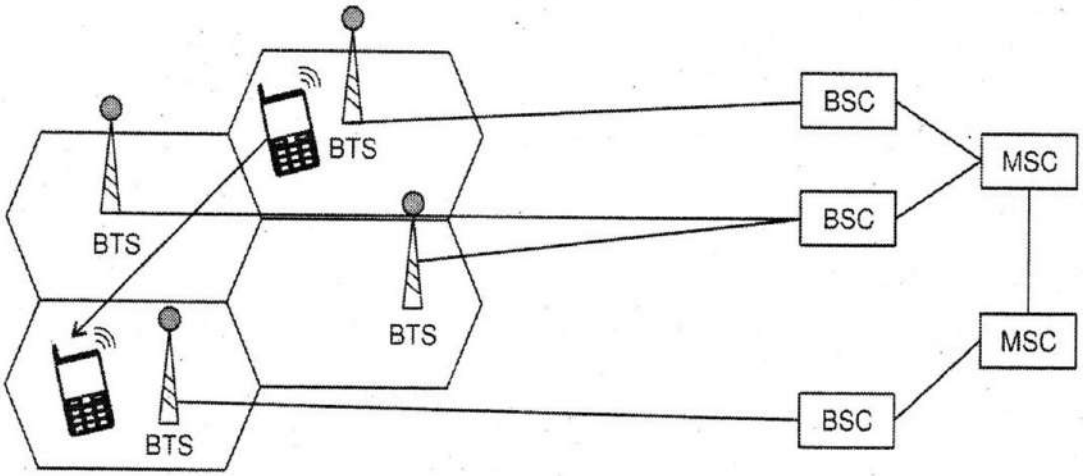


Figure 1.16: Inter-MSC Handover

6. General Packet Radio Service (GPRS)

6.1 Introduction

GPRS is a packet switching technology that enables data transfers through cellular network. The GPRS network acts in parallel with the GSM network and it provides packet switched connections to the external networks.

GPRS was established by European Telecommunication Standards Institute. It provided a packet data capability for the 2G cellular systems. GPRS provides all the functionality of a GSM network.

Depending upon the functionality, GPRS devices are of different kinds and shapes. According to functionalities the GPRS devices are classified as:

i. **Class A:** These devices can operate simultaneously with GPRS and with GSM networks.

ii. **Class B:** These devices can be registered for both the GSM and GPRS networks. But they can't be operated simultaneously on both the networks. The device must shift between the two modes.

iii. **Class C:** These devices operate exclusively on GPRS services.

6.2 GPRS Network Architecture

GPRS is not a completely separate network. GPRS architecture consists of GSM architecture and GPRS support nodes. It uses base transceiver and base transceiver station controller of GSM architecture.

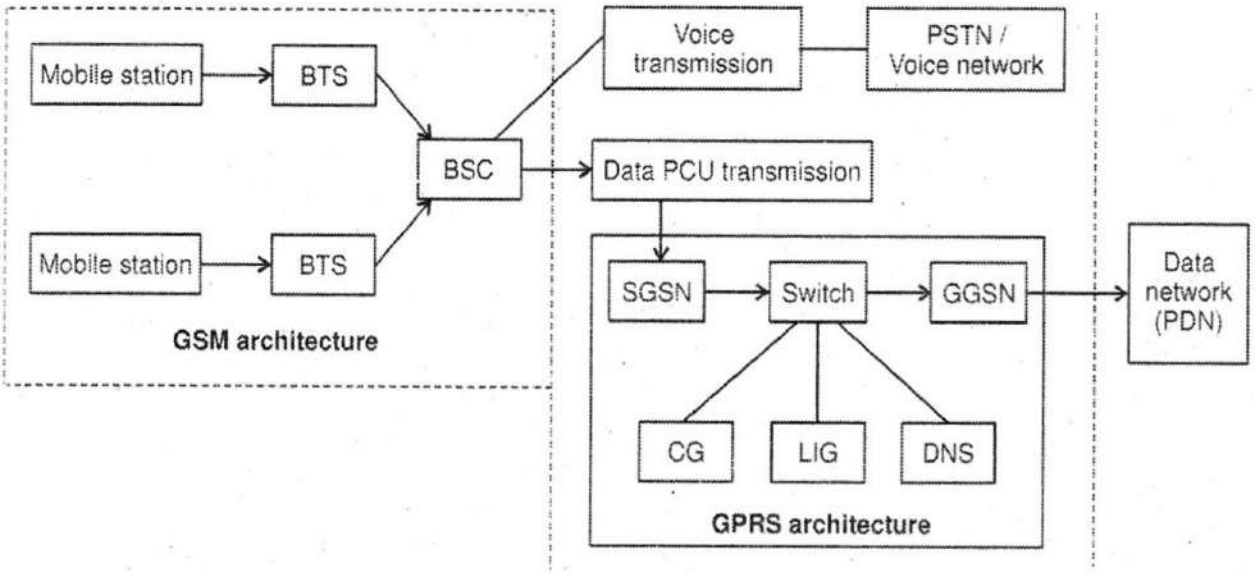


Figure 1.17: GPRS Architecture

GPRS architecture has two support nodes:

i. Serving GPRS Support Node (SGSN)

ii. Gateway GPRS Support Node (GGSN)

Following paragraphs explain functioning of each block.

1. **Serving GPRS Support Node (SGSN):** SGSN is responsible for routing, handover and compression, authentication, registration and IP address assignment. It connects network to the GPRS device. It functions as:

   a. When mobile device is moving through different cells, the SGSN finds out the BSC and does not allow the interruption / drop of call.

   b. When the user moves to a segment which is managed by different SGSN, it will perform a handoff to the new SGSN. During this process, if any packets are lost, then they are retransmitted.

   c. The SGSN converts mobile data into IP and is connected to GGSN via a tunneling protocol.

2. **Gateway GPRS Support Node (GGSN):** The GGSN provides the interface between the user device and external packet switched network. It functions as a gateway, router and firewall. GGSN stores International Mobile Subscriber Identity (IMSI) of mobile device, charging information and address of SGSN.

GGSN also receives the packets send from the other mobile device and routes them to the correct SGSN for final delivery to the mobile device.

3. **Charging Gateway (CG):** It's basic function is to introduce a single logical link to the operator's billing system and reduces the number of physical link and connections required.

4. **Lawful Interception Gateway (LIG):** In many countries, the traffic through GPRS network is monitored by Law Enforcement Agencies (LEA). So LIG captures the data and forward it to LEA. Often this interception of user data requires a court order.

5. **Domain Name System (DNS):** To make a connection via GPRS to an external network, selection of Access Point Name (APN) is required. The two general access points are net and wap. Net would indicate a connection directly to the Internet and wap a connection to a Wireless Access Protocol (WAP) gateway.

6. **Border Gateway (BG):** It acts as the backbone which connects different network operators together. This backbone is referred to as an inter-PLMN backbone or Global Roaming Exchange (GRX).

Benefits of GPRS

i. Resources are reserved only when needed.

ii. Connection set up times are reduced.

iii. Enables new service opportunities.

Exercises

A. Multiple choice questions

1. Which of the following is not a characteristic of cellular telephone system?
   a. Accommodate a large number of users
   b. Large geographic area
   c. Limited frequency spectrum
   d. Large frequency spectrum

2. What is the responsibility of MSC in cellular telephone system?
   a. Connection of mobile to base stations
   b. Connection of mobile to PSTN
   c. Connection of base station to PSTN
   d. Connection of base station to MSC

3. What is the shape of the cell present in the cellular system?
   a. Circular
   b. Square
   c. Hexagonal
   d. Triangular

4. What is handoff?
   a. Forward channel
   b. Switching technique
   c. Roamer
   d. Guard channel

5. What is meaning of frequency reuse?
   a. Increased capacity
   b. Limited spectrum is required
   c. Same spectrum may be allocated to other network
   d. Number of base stations is reduced

6. The interference between the neighbouring base stations is avoided by _____.
   a. Assigning different group of channels
   b. Using transmitters with different power level
   c. Using different antennas
   d. Using different base stations

7. 3G W-CDMA is also known as_____.
   a. UMTS
   b. DECT
   c. DCS-1800
   d. ETACS

8. _____detected short waves in 1920.
   a. Edwin Armstrong
   b. Albert Einstein
   c. Galileo Galilei
   d. Marconi

9. The interference between the neighboring base stations is avoided by_____.
   a. Assigning different group of channels
   b. Using transmitters with different power level
   c. Using different antennas
   d. All of the above

10. Radio capacity may be increased in cellular concept by_____.
   a. Increase in radio spectrum
   b. Increasing the number of base stations and reusing the channels
   c. Both a and b
   d. None of the above

11. Hexagon shape is used for radio coverage for a cell because_____.
   a. It uses the maximum area for coverage
   b. Fewer number of cells are required
   c. It approximates circular radiation pattern
   d. All of the above

12. Circular shape is not used for radio coverage for a cell because_____.
   a. It's coverage area is small
   b. Fewer number of cells are required
   c. Problem of "Hole" occurs
   d. None of the above

13. The advantage/s of using frequency reuse in cellular telephony system is/are_____.
   a. Increased capacity
   b. Limited spectrum is required
   c. Same spectrum may be allocated to other network
   d. All of the above

14. In Handoff_____.
    a. Process of transferring the call to the new base station
    b. Transfers the call
    c. New channel allocation is done
    d. All of the above

15. Frequency reuse distance depends upon_____.
    a. Radius of the cell
    b. Distance between the centers of the co channel cells
    c. Frequency allocation of nearest cells
    d. Both a and b

16. The 2G cellular network uses_____.
    a. TDMA/FDD
    b. CDMA/FDD
    c. Digital modulation formats
    d. All of the above

17. 2G CDMA standard – CDMA1 supports up to_____.
    a. 8 users
    b. 64 users
    c. 32 users
    d. 116 users

18. 2G standards support_____.
    a. Limited internet browsing
    b. Short Messaging Service
    c. Both a and b
    d. None of the above

19. The minimum spectrum allocation required for W-CDMA is_____.
    a. 5 MHz
    b. 2 MHz
    c. 500 KHz
    d. 100 KHz

20. What are the three main parts of a GSM Architecture or Structure?
    a. Mobile Station
    b. BSS - Base Station Subsystem
    c. NSS - Network and Switching Subsystem
    d. All the above

21. What are the main parts of a Mobile Station in a GSM Network?
    a. MT - Mobile Terminal
    b. SIM - Subscriber Identity Module
    c. Both a and b
    d. None

22. What are the main parts of a BSS (Base Station Subsystem) in a GSM network?

a. BTS - Base Transceiver Station
b. BSC - Base Station Controller
c. a and b
d. None

23. Each Mobile Terminal is identified by a unique _____. number.

a. IMEI
b. SIM
c. IMSI
d. None

24. IMEI stands for_____.

a. Internal Mobile Equipment Identity
b. International Mobile Equipment Identity
c. Intra Mobile Enable Identity
d. None

25. Each SIM is identified by a unique _____. number.

a. IMSI
b. IMEI
c. MSDN
d. None

26. IMSI stands for _____.

a. Internal Mobile Subscriber Identity
b. International Mobile Subscriber Identity
c. Investigating Mobile Subscriber Identity
d. None

27. What is the main function of NSS?

a. Establishing communication between mobile and landline numbers.
b. Providing eligible services to the subscriber
c. Providing parameters for Authentication and Encryption
d. All

28. A BTS is also called _____by general public

a. Mobile tower
b. Exchange
c. Charging Point
d. None

29. The only element that personalises a Mobile Station is _____.

a. Back cover
b. SIM
c. Screen guard
d. None

30. The functions of an MSC are_____.

a. Charging the call or billing
b. Signalling with outside systems
c. Logical radio link control
d. All

31. An Equipment Identity Register (EIR) contains _____ lists.

a. White list or Valid list
b. Grey or Monitored list
c. Black or Prohibited list
d. All

32. The actual network needed for establishing calls in GSM is composed of the _____.

a. NSS and BSS
b. NSS and NMS
c. NSS and OMC
d. BSS and NMS

33. Identification numbers of the valid subscribers are stored in _____element of GSM architecture.

a. HLR
b. VLR
c. EIR
d. MSC

34. The origin and destination of a call is identified by _____element of GSM architecture.

a. NSS
b. VLR
c. MS
d. MSC

35. _____is an element of BSS in GSM architecture.

a. BSC
b. NMS
c. EIR
d. VLR

36. Fault management of GSM architecture is handled by_____.

a. BSS
b. NMS
c. MSC
d. NSS

37. GPRS stands for_____.

a. General Packet Repair Service
b. General Packet Radio Service
c. Graphics Packet Radio Service
d. None

38. Class -A Mobile Station supports _____.

a. Only GPRS
b. Only GSM
c. GSM and GPRS Simultaneously
d. GSM and GPRS one at a time.

39. Choose a correct abbreviation below.
    a. SGSN - Serving GPRS Support Node
    b. GGSN - Gateway GPRS Support Node
    c. IP - Internet Protocol
    d. All of the above

40. In a GPRS network, SGSN is the equivalent of _____ system in GSM.
    a. BSC
    b. MSC
    c. VLR
    d. GMSC

41. GPRS Roaming from one SGSN to another SGSN is offered by ?
    a. GMSC
    b. GGSN
    c. HLR
    d. VLR

42. What are the functions of GGSN of a GPRS NETWORK_____?
    a. Charging (Billing), Filter user traffic
    b. Routing mobile originated traffic, GTP Tunneling to SGSN
    c. Interface external networks
    d. All

43. A BG(Border Gateway) connects to _____using Tunneling.
    a. Same operator's GPRS network
    b. Different operator's GPRS network
    c. Same or different operator GPRS N/W
    d. None

44. Which system in a GPRS architecture collects all Charging (Billing) records for final processing?
    a. SGSN
    b. GGSN
    c. CH (Charging Gateway)
    d. None

45. Which are the blocks of Mobile handset ?
    a. Processor
    b. Memory
    c. DSP
    d. all of above

B. Answer in one or two lines

1. What is the medium used in wireless Communication system?
2. Why circular or square shape of cell are not suitable?
3. Draw structure of individual cell.
4. Draw seven cell cluster for cellular telephony network,
5. Give relation between total available frequency spectrum, bandwidth of singal user, and number of users that can communicate simultaneously in a cell.
6. Define the following w.r.t cellular system
   a. Femtocell b. Picocell
   c. Microcell d. Macrocell
7. What is cell splitting?
8. State frequency reuse concepts of cellular telephony system.
9. How frequency reuse distance is calculated?
10. What is "Handoff" in cellular system? why it is required?
11. What are two types of interferences occurring in cellular systems?
12. How co-channel interference can be reduced?
13. How to reduce adjacent channel interference?
14. Name components of mobile handset.
15. What is purpose of memory inside mobile handset?
16. What is need of multiple antennas in the mobile handset?
17. What is UMTS?
18. W-CDMA is a feature of which generation of cellular netwok.
19. What is 4G-LTE?
20. "GSM architecture is must for cellular networking" – Comment.
21. What are different blocks of GSM architecture?

22. What is mobile station?
23. Which are elements of base station subsystem of GSM?
24. Give function of following blocks of NSS of GSM
    a. Visitor Location Register(VLR)
    b. Home Location Register(HLR)
    c. Equipment Identity Register(EIR)
    d. Authentication Centre(AuC)
25. Mention four types of handover occurring in GSM.
26. Write the following type of handover will occur in GSM
    a. Intra-cell handover
    b. Inter-cell handover of Intra-BSC handover
    c. Inter-BSC handover
    d. Inter- MSC handover
27. GPRS uses GSM architecture-Comment.
28. Which are different blocks of GPRS architecture?
29. What is function of charging Gateway block of GPRS?
30. What are the benefits of GPRS?
31. Define following types of GPRS devices
    a. Class A
    b. Class B
    c. Class C
32. Which class supports only GPRS services?
33. In which type of class, GSM and GPRS services can be used simultaneously?
34. Draw GPRS architecture.

C. Answer in detail

1. What are advantages of wireless communication?
2. Explain seven-cell cluster of cellular telephony system.
3. What is frequency reuse concept of cellular telephony system.
4. Why "handoff" is necessary in cellular telephony system?
5. How "handoff" is achieved?
6. What is co-channel interference in cellular system?
7. Explain adjacent channel interference.
8. Draw block diagram of mobile handset.
9. Describe functioning of any five blocks of Mobile handset.
10. Explain CDMA and TDMA technologies of 2G cellular network.
11. Which are advantages of 3G cellular network?
12. What are features of 3G W CDMA (UMITS)?
13. Write features of 4G cellular network.
14. Write short note on 4G –LTE.
15. Compare 1G, 2G, 3G,4G cellular network.
16. Explain Mobile Station (MS) of GSM.
17. What are functions of Network switching subsystem of GSM?
18. Which are three different lists maintained by EIR of GSM?
19. Write role of base station subsystem of GSM.
20. Mention any three tasks performed by BTS of GSM.
21. Write three functions performed by Network Management Subsystem (NMS) of GSM.
22. What are different types of handover of GSM?

23. Draw GPRS architecture.

24. Explain functioning of Serving GPRS Support Node (SGSN).

25. Explain role of Lawful Interception Gateway (LIG) and Domain Name System (DNS) in GPRS architecture.

Answers

1. d	2. b	3. c	4. b
5. c	6. a	7. a	8. d
9. a	10. b	11. d	12. c
13. d	14. d	15. d	16. d
17. b	18. c	19. a	20. d
21. c	22. c	23. a	24. b
25. a	26. b	27. d	28. a
29. b	30. d	31. d	32. a
33. c	34. d	35. a	36. b
37. b	38. c	39. d	40. b
41. b	42. d	43. b	44. c
45. d			

Unit 2

Short Range Wireless Technologies and Location Tracking

1. Introduction

Many wireless technologies developed so far are now standardized and are widely used for number of applications. Some of them are developed for specific applications while others are flexible and generic. We are familiar with various types of wireless communication systems such as

i. Television and Radio Broadcasting

ii. Satellite Communication

iii. Radar

iv. Mobile Communication System

v. Global Positioning System (GPS)

vi. Infrared Communication

vii. WLAN (Wi-Fi)

viii. Bluetooth

Most of the wireless standards we use daily are considered to be short-range communication standards. These characterize a wide range of scenarios, technologies and requirements. There is no formal definition of such systems though one can always classify short-range systems

according to their typical reach or coverage. The range varies widely with frequency, power level, antenna structures as well as many environmental conditions. Short-range systems involve transfer of information from millimeters to a few hundreds of meters. However, short-range communication systems are not only systems providing wireless connectivity in the immediate proximity, but in a broader perspective they also define technologies used to build service access in local areas. The short-range systems include Near Field Communications (NFC) for very close connectivity (range in the order of millimeters to centimeters), Radio Frequency Identification (RFID) ranging from centimeters upto a few hundred meters. Other examples are standards like Wi-Fi, Bluetooth, ZigBee, Z-Wave which ranges from a few feet upto 100 meters or so.

An important factor in the widespread penetration of short-range devices into the office and in the home is the most popular applications based on the industry standards. While designing short range communication applications, the following criteria are considered:

i. Communication architecture

ii. Energy awareness

iii. Signaling and traffic channels

iv. Scalability and connectivity

v. Medium access control and channel access

vi. Service discovery

vii. Security and privacy and authentication

viii. Flexible spectrum

In this chapter, we will study very widely used short range communication applications. At the end of this chapter, working of GPS architecture is explained.

2. Bluetooth

Wireless has become a remarkable and attractive feature for almost every new electronic product. It adds flexibility, convenience, and remote monitoring and control without expensive wiring and cabling. The range of applications is staggering, from simple toys to consumer electronic products to industrial automation.

Bluetooth is a short range, low cost and power efficient wireless technology standard used to exchange data between point-to-point and point-to-multipoint connections. It operates in the unlicensed 2.4 GHz band and uses frequency hopping technique. It was originally conceived as a wireless alternative to RS-232 data cables. It connects handheld devices like printers, mobiles, laptops and other accessories in the 10 m range.

In 1997 Jim Kardach of Intel developed a system that would allow mobile phones to communicate with computers. He proposed the name "Bluetooth" for the newly invented device in the honor of 10th-century Danish King, Harald Bluetooth. At the time of this proposal, he was reading Frans G. Bengtsson's historical novel *The Long Ships* about Vikings and Harald Bluetooth.

2.1 Bluetooth Architecture

The architecture of Bluetooth defines two types of network:

i. Piconet

ii. Scatternet

The basic unit of networking in bluetooth is a **piconet** and a collection of interconnected piconets is called **scatternet.**

i. Piconet is a type of bluetooth network that contains one primary node called as master device and one or more slave devices. One piconet can have maximum seven slave devices.

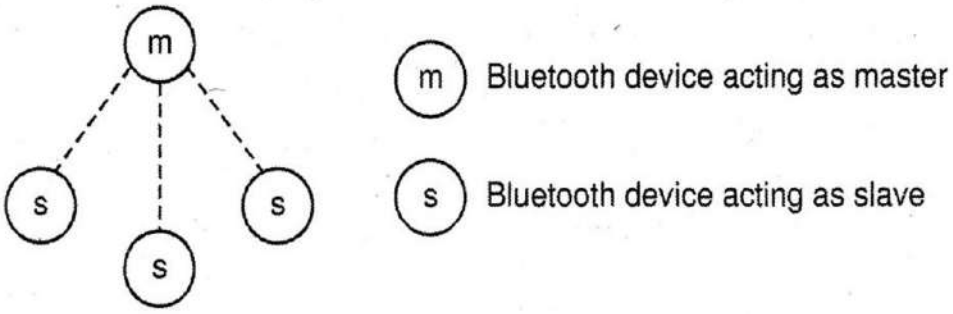


Figure 2.1: Piconet

ii. Bluetooth uses Frequency Hopping sequence with a carrier spacing of 1 MHz for wireless communication. Master decides frequency hopping sequence and timing required for transmission of all slaves. For this, master device uses his own device address.

iii. Slave has to take permission from master for communication. Then it can communicate through master only.

iv. The Bluetooth network consisting of one or more piconets is known as scatternet. A device in one piconet may also exist as part of another piconet and may function as either a slave or master. This forms a **scatternet**. In one scatternet there can be minimum two and maximum ten piconets.

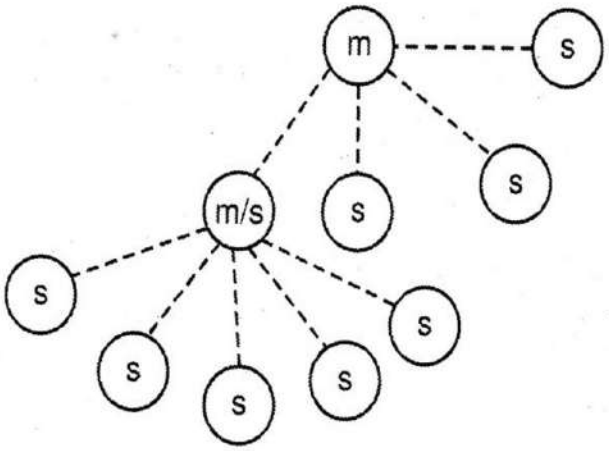


Figure 2.2: Scatternet

v. The advantage of the piconet / scatternet scheme is that it allows many devices to share the same physical area and make efficient use of the bandwidth.

vi. Different logical channels (different hopping sequence) can simultaneously share the same 80 MHz bandwidth.

vii. Collision will occur when devices in different piconets, happen to use the same hop frequency at the same time.

viii. As the number of piconets in an area increases, the number of collisions increases and performance degrades.

ix. In short, the physical area and total bandwidth are shared by the scatternet. The logical channel and data transmission are shared by a piconet.

2.2 Classes of Bluetooth

Based on output power and coverage area, there are three classes of bluetooth transmitters:

i. **Class 1:** This class provides the greatest coverage distance. In this class, power control is mandatory. It provides 1 mW power output for minimum range and 100 mW output power for maximum range.

ii. **Class 2:** This class outputs 2.4 mW at maximum and 0.25 mW at minimum. Here power control is optional.

iii. **Class 3:** This class outputs lowest power. Nominal output is 1 mW.

2.3 Bluetooth Frequency Spectrum

i. Most of the countries in Europe, Asia and U.S. use unlicensed 2.4 GHz - 2.4835 GHz band within ISM (Industrial, Scientific and Medical) band.

ii. It uses 1 MHz bandwidth for each channel. Typically upto 80 different frequencies are used for a total bandwidth of 80 MHz.

iii. Power control is used to keep the devices from emitting more RF power than required.

iv. Modulation for bluetooth is Gaussian FSK, with a binary one represented by a positive frequency deviation and binary zero represented by a negative frequency deviation from the center frequency.

2.4 Bluetooth Protocol Stack

Bluetooth has a layered protocol architecture. It consists of four layers:

i. Core protocol

ii. Cable replacement protocol

iii. Telephony control protocol

iv. Adopted protocol

Let us study functioning of each layer.

i. **Core protocol:** It forms a five-layer stack having the following elements:

   a. *Radio*: Takes care of frequency, hopping sequence, modulation scheme, transmit power.

   b. *Baseband*: Responsible for establishing connection within a piconet, addressing, packet format, timing and power control.

   c. *Link Manager Protocol (LMP)*: Handles link setup between bluetooth devices and ongoing link management. It takes care of security aspects such as authentication and encryption.

   d. *Logical link control and adaption control (L2CAP)*: Adapts upper layer protocols to the baseband layer.

   e. *Service Discovery Protocol*: Device information, services and the characteristics of the services can be queries to enable the establishment of a connection between two or more bluetooth devices.

ii. **Cable replacement protocol:** RFCOMM is the cable replacement protocol. It is a virtual serial port that is designed to make a replacement of cable technologies with the minimum of modification of existing devices. EIA-232 is a widely used serial port interface standard for bluetooth.

iii. **Telephony control protocol:** TCSBIN (Telephony Control Specification - Binary) is a bit-oriented protocol of bluetooth. It defines the call control signaling for the establishment of speech and data calls between bluetooth devices. It also takes care of mobility feature of group of bluetooth devices.

iv. **Adopted protocol:** Bluetooth architecture has adopted existing standard, protocols wherever possible and invented only necessary protocols. The adopted protocols are:

   - PPP: (Point-to-Point Protocol)
   - TCP/UDP/IP: Foundation protocol of TCP/IP protocol
   - OBEX: Object exchange protocol
   - WAE/ WAP: Wireless Application Environment / Wireless Application Protocol

2.5 Bluetooth Frame Structure

The Bluetooth packet consists of three fields:

i. Access code: 72 bits in length

ii. Header: 54 bits in length

iii. Payload format: 0 to 2745 bits in length

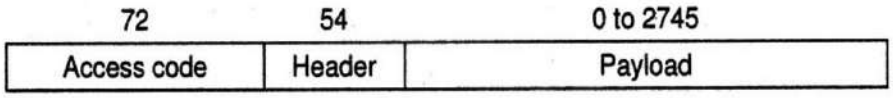


Figure 2.3: Bluetooth packet format

i. **Access code:** Access code is of maximum 72 bits. It is used for timing synchronization, offset compensation and enquiry.

- The fields of access code are further subdivided as: Preamble, SYNC Word and Trailer.
- Preamble and trailer fields are of 4-bits each while SYNC word is of 64-bits.
- LSB and MSB of SYNC word decides Preamble and Trailer fields.
- If LSB in SYNC word is 0, then 4-bit preamble is 0101 and if LSB in SYNC word is 1, then 4-bit preamble is 1010.
- If the MSB of the SYNC word is 1, then the trailer is 0101 and if MSB is 0 then the trailer is 1010.

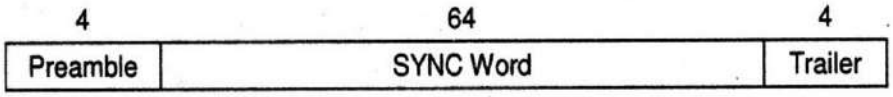


Figure 2.4: Bluetooth Access code format

- There are three types of access codes:
  - *a.* *Channel Access Code*: Identifies a piconet.
  - *b.* *Device Access Code*: Used for paging and its subsequent responses.
  - *c.* *Inquiry Access Code*: Used for inquiry purposes.

ii. **Header:** This field identifies packet type and carries protocol control information. It consists of six fields:

a. *AM_ADDR (Active Mode Address)*: 3-bit AM_ADDR (since max. seven active slaves) is temporarily address assigned to the slave in piconet.

b. *Type*: Identifies the type of packet.

c. *Flow*: Provides a 1-bit flow control mechanism. When a packet with Flow = 0 is received, the station receiving the packet must temporarily halt the transmission. When a packet with Flow = 1 is received, transmission may resume.

d. *ARQN*: Provides a 1-bit acknowledgement mechanism. In case of successful reception, ARQN = 1 is returned. ARQN = 0 indicates no reception and relevant packet is retransmitted.

e. *SEQN*: Provides 1-bit sequential numbering schemes.

f. *Header Error Control (HEC)*: An eight bit error detection code used to protect the packet header.

iii. **Payload:** Payload contains user's voice or data. It's format is decided by the baseband specifications. The payload format has three fields:

a. Payload header: It can be 8-bits or 16-bits depending upon whether packets are single-slot or multi-slot respectively. Payload header consists of three sections:

- L-CH: Identifies logical channel.
- Flow: Used to control flow at the L2CAP level.
- Length: The number of bytes of data in the payload.

b. Payload body: Actual user information is present in Payload body.

c. CRC: 16-bit CRC code is used for all data payloads for error detection and correction.

3. ZigBee

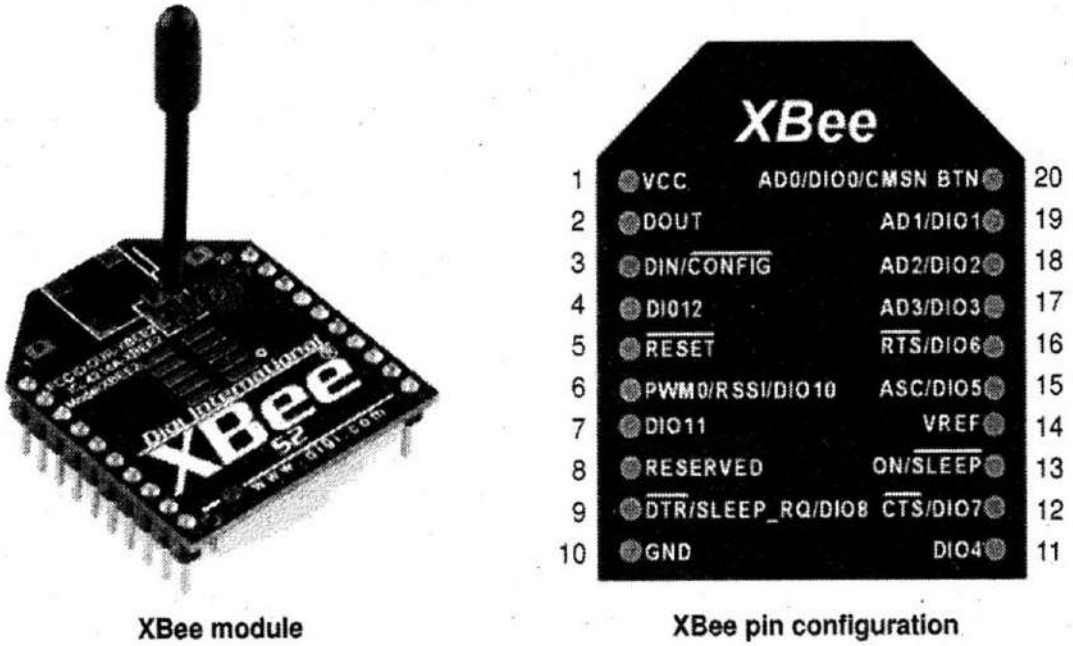
3.1 Introduction

Currently, numerous high data rate communication standards are available but none of these meet the sensors' and control devices' communication standards. Several embedded applications, industrial control, home automation and IoT applications etc. Demand low power communication standard. ZigBee is a wireless technology specially developed for such applications and for wireless personal area networks (WPANs). It is the product from ZigBee alliance. ZigBee is a specification that's been around for more than a decade, and it's widely considered an alternative to Wi-Fi and bluetooth for applications including low-powered devices that don't require a lot of bandwidth - like your smart home sensors.

Maximum data transfer rate of ZigBee is just 250 kbps which is much lower than the lowest speed of Wi-Fi. In spite of having low data transfer rate than Wi-Fi, attractive features like low-cost and low-power consumption make ZigBee more suitable for applications of wireless IoT networks and in automation industries. Another advantage is that it's protocol was designed as 'assemble and forget', meaning once you set it up, it can last for months.

The ZigBee standard operates on the IEEE 802.15.4 physical radio specification and operates in unlicensed bands including 2.4 GHz, 900 MHz and 868 MHz. The ZigBee technology range for transmission covers mainly 10 - 100 meters based on the power output and on environmental characteristics.

Standard ZigBee module is shown in figure 2.5.



XBee module XBee pin configuration

Figure 2.5: Standard module of ZigBee

3.2 ZigBee Architecture

We will study ZigBee architecture in two parts: ZigBee devices and ZigBee technological architecture.

A. ZigBee Devices

ZigBee devices are commonly known as ZigBee nodes. Each node can send and receive data. However depending upon functionality, the nodes are categorized as:

a. ZigBee coordinator
b. Router
c. End device

The number of coordinators, routers and end devices depends on the type of network topology (star, tree and mesh). The role and function of each type of node is described below:

a. Coordinator: Every ZigBee network must have at least one coordinator. The job of the coordinator is to handle and store the information including security keys.

b. **Router:** ZigBee routers act as intermediate devices that permit data to pass to and fro through them to other devices.

c. **End device:** End devices are low-power or battery-powered devices, which talk to the coordinator or a router. They can't relay data from other devices. These have limited functionality to communicate with the parent nodes so that the battery power is saved.

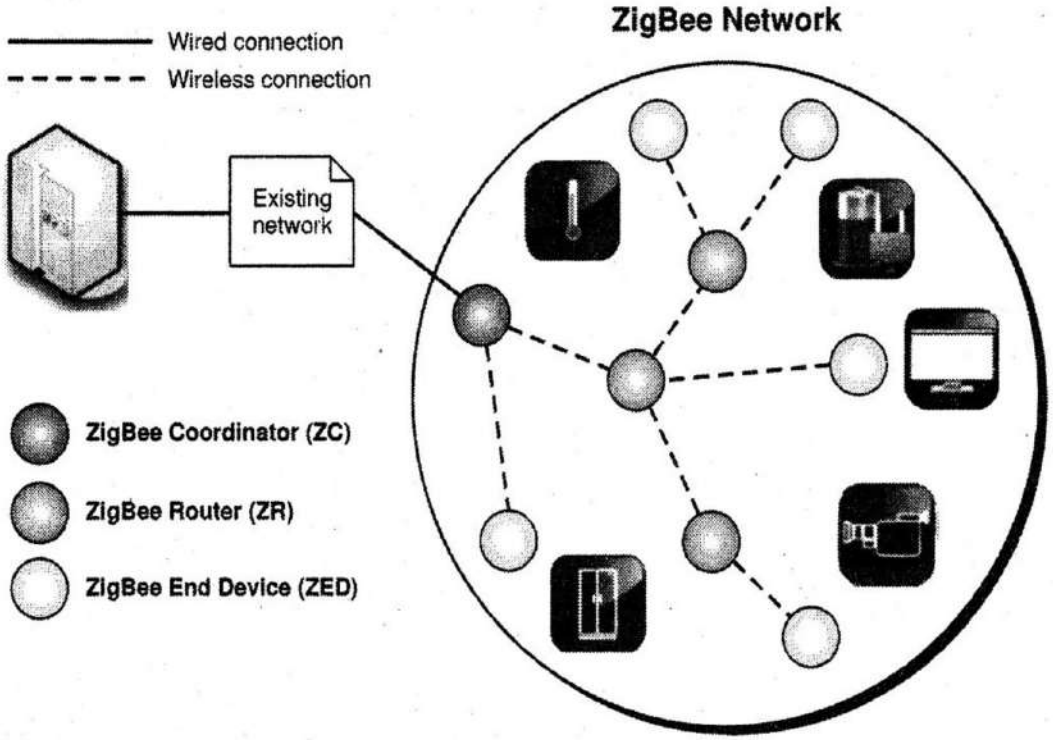


Figure 2.6: ZigBee Devices

B. ZigBee Architecture

ZigBee protocol architecture is of five layers viz. physical layer, MAC layer, network layer, application support sublayer and application layer. Out of these it's physical and MAC layers are same as that of IEEE 802.15.4. It has it's own other three layers.

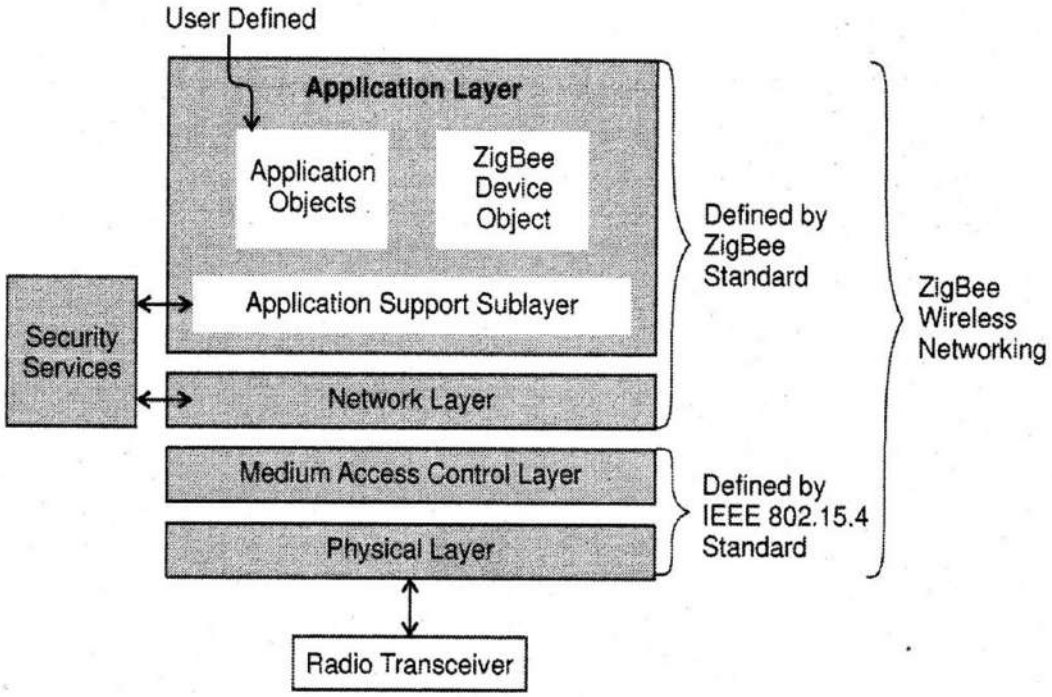


Figure 2.7: ZigBee Architecture

i. **Physical layer:** This layer does modulation and demodulation operations upon transmitting and receiving signals respectively.

ii. **MAC layer:** This layer is responsible for reliable transmission of data by accessing different networks with the carrier sense multiple access collision avoidances (CSMA-CA). This also transmits the beacon frames for synchronizing communication.

iii. **Network layer:** This layer takes care of all network-related operations such as network setup, end device connections and disconnections to network, routing, device configurations, etc.

iv. **Application support sub-layer:** This layer enables the services necessary for ZigBee device objects and application objects to interface with the network layers for data managing services. This layer is responsible for matching two devices according to their services and needs.

v. **Application framework:** It provides two types of data services as key-value pair and generic message services. The generic message is a developer-defined structure, whereas the key-value pair is used for getting attributes within the application objects. ZigBee Device Object provides an interface between application objects and the APS layer in ZigBee devices. It is responsible for detecting, initiating, and binding other devices to the network.

3.3 ZigBee Topologies

ZigBee supports several network topologies; however, the most used configurations are star, mesh, and cluster tree topologies. Any topology consists of one or more coordinators, routers and end devices.

i. **Star topology:** The star topology consists of one coordinator and several end devices. Coordinator initiates and manages all the devices in the network. End devices can only communicate with the coordinator. Any data exchange between end devices must go through the coordinator. This topology is used in industries where all the endpoint devices are needed to communicate with the central controller. This topology is simple and easy to deploy. But disadvantage of this topology is the operation of the network depends on the coordinator of the network, and because all packets between devices must go through coordinator, the coordinator may become bottlenecked. Also there is no alternative path from the source to the destination.

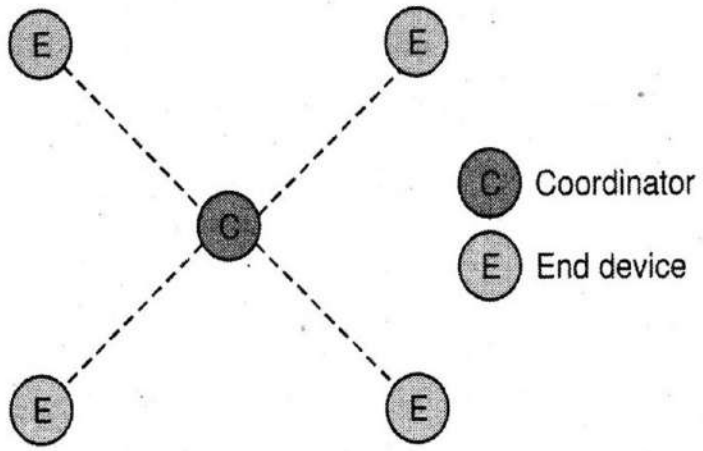


Figure 2.8: ZigBee - Star topology

ii. **Tree Topology:** In this topology, the ZigBee network coverage is extended with several routers. It has a central node acting as coordinator, several routers, and end devices as shown in *figure 2.9.* The end devices can communicate either with routers or with the coordinator.

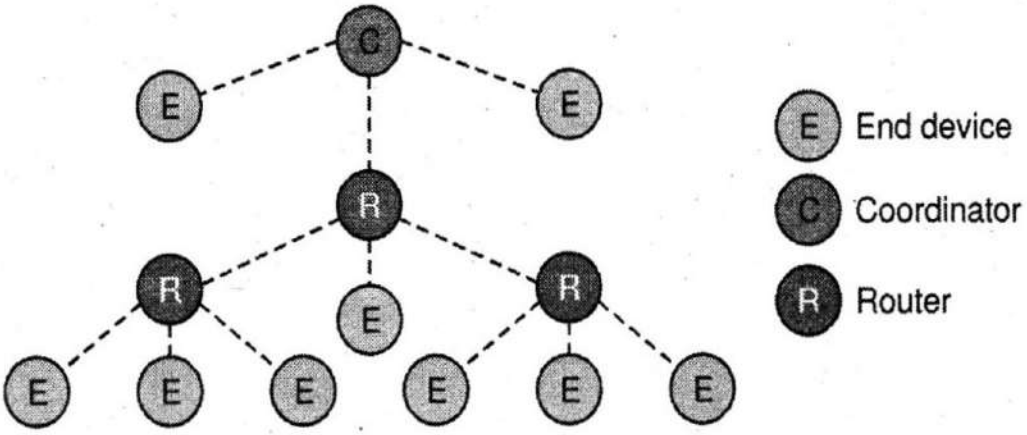


Figure 2.9: ZigBee -Tree topology

The end nodes that are connected to the coordinator or the routers are called children. Only routers and the coordinator can have children. Each end device is only able to communicate with its parent (router or coordinator). The coordinator and routers can have children and, therefore, are the only devices that can be parents. An end device cannot have children and, therefore, may not be a parent. A special case of tree topology is called a cluster tree topology.

The disadvantages of tree topology is that if one of the parents becomes disabled, the children of the disable parent cannot communicate with other devices in the network.

iii. **Cluster tree topology:** A cluster tree topology is a special case of tree topology in which a parent with its children is called a cluster, as shown in *Figure 2.10.* Each cluster is identified by a cluster ID. ZigBee does not support cluster tree topology, but IEEE 802.15.4 does support it.

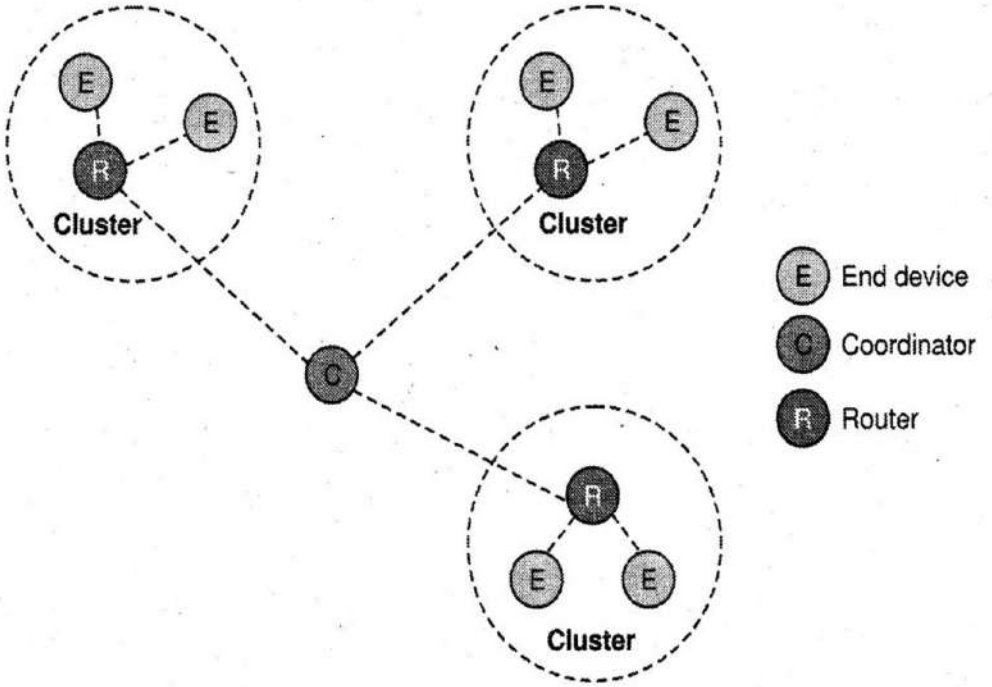


Figure 2.10: ZigBee - Cluster topology

iv. **Mesh topology:** Mesh topology, also referred to as a peer-to-peer network, consists of one coordinator, several routers, and end devices, as shown in *figure 2.11.*

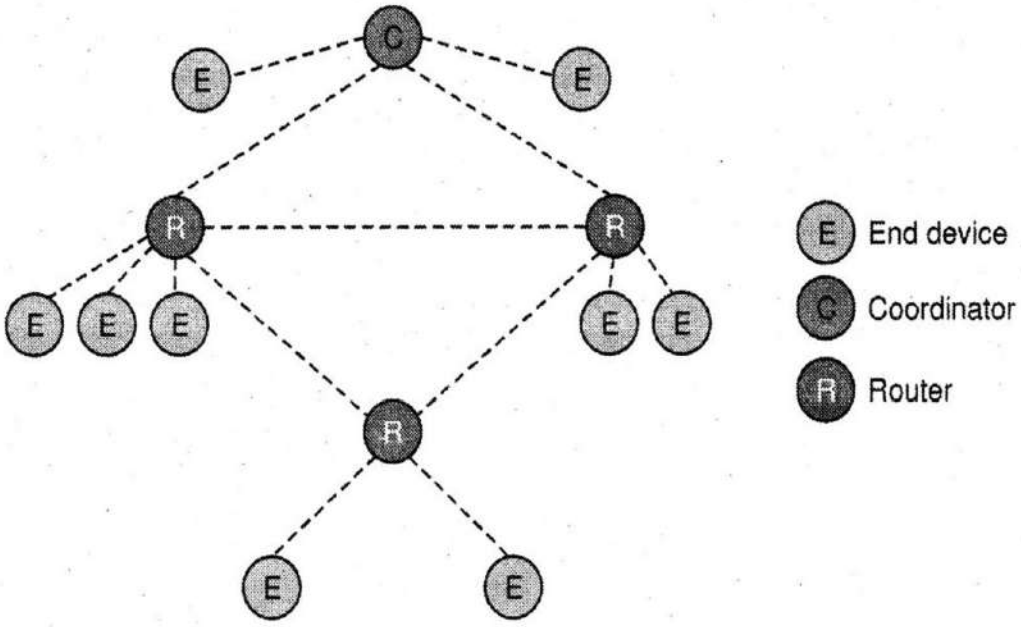


Figure 2.11: ZigBee - Mesh topology

The following are the characteristics of a mesh topology:

A mesh topology is a multihop network; packets pass through multiple hops to reach their destination. The range of a network can be increased by adding more devices to the network. It can eliminate dead zones. A mesh topology is self-healing, meaning during transmission, if a path fails, the node will find an alternate path to the destination. Adding or removing a device is easy. Any source device can communicate with any destination device in the network.

Compared with star topology, mesh topology requires greater overhead. Mesh routing uses a more complex routing protocol than a star topology.

3.4 ZigBee Technology Advantages and Disadvantages

Advantages

The advantages of ZigBee include the following:

i. This network has a flexible network structure.
ii. Battery life is good.
iii. Power consumption is less.
iv. Very simple to fix.
v. It supports approximately 6500 nodes.
vi. Less cost.
vii. It is more reliable.
viii. Network setting is very easy and simple.
ix. The network is scalable and it is easy to add/remove ZigBee end device to the network.

Disadvantages

The disadvantages of ZigBee include the following:

i. It needs the system information to control ZigBee based devices for the owner.
ii. It is less secure than Wi-Fi. So highly risky to be used for official private information.
iii. The high replacement cost once any issue happens within ZigBee based home appliances.
iv. The transmission rate of the ZigBee is less.

v. It does not include several end devices.

vi. It is not used as an outdoor wireless communication system because it has less coverage limit.

vii. Similar to other types of wireless systems, ZigBee communication system is prone to bother from unauthorized people.

3.5 Applications

ZigBee is a low-cost, low-power, wireless network standard targeted at battery-powered devices. So it is used in wireless control and monitoring applications. ZigBee chips are typically integrated with microcontrollers.

Thus, ZigBee protocols are intended for embedded applications requiring low power consumption and tolerating low data rates. The resulting network will use very little power. Individual devices must have a battery life of at least two years. ZigBee is not for situations with high mobility among nodes. Hence, it is not suitable for adhoc radio networks where high data rate and high mobility is needed.

The typical applications of ZigBee technology include the following:

i. **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, surveillance, and so on.

ii. **Industrial automation:** In manufacturing and production industries, a communication link continuously monitors various parameters and critical equipments using ZigBee. ZigBee considerably reduces communication cost as well as optimizes the control process for greater reliability.

iii. **Wireless Sensor Networks (WSN):** A wireless sensor network consists of sensors which are densely distributed to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. The sensor data is transmitted to network coordinator which is heart of the wireless personal area network. In the modern scenario, wireless networks contain sensors as well as actuators. WSN is composed of ZigBee coordinator, ZigBee router and ZigBee end device. The sensor nodes send the information to the coordinator, the coordinator collects all sensors data, stores the data in memory, processes it, and routes the data to appropriate node.

iv. **Medical data collection:** With wireless medical monitoring systems, patients' information such as blood pressure, heart rate and electrocardiogram can be sent instantly to specialized medical centers to store and process properly.

v. **Smoke and intruder warning:** The conflagration of fire is still a serious problem caused by humans, and houses are at a high risk of fire. People have developed smoke alarms which only have one sensor to detect fire. Smoke is emitted in several forms in daily life. A single sensor is not a reliable way to detect fire. Therefore intelligent smoke alarm systems using many sensors are developed. It uses ZigBee transmission to build a wireless network to identify smoke.

vi. **Building automation:** Building automation systems using ZigBee technology control various components within a building's structure, such as heating, ventilation, air conditioning etc. It improves system efficiency, reduces costs and increases safety.

vii. **Smart metering:** ZigBee application in smart metering includes energy consumption response, pricing support, security over power theft, etc.

viii. **Smart grid monitoring:** ZigBee operations in the smart grid involve remote temperature monitoring, fault locating, reactive power management, and so on.

3.6 Comparison of ZigBee and Bluetooth

The following table compares ZigBee and Bluetooth

	Bluetooth	ZigBee
i.	The frequency range of Bluetooth ranges from 2.4 GHz - 2.483 GHz.	The frequency range of ZigBee is 2.4 GHz.
ii.	It has 79 RF channels.	It has 16 RF channels.
iii.	The modulation technique used in Bluetooth is GFSK.	ZigBee uses different modulation techniques like BPSK, QPSK & GFSK.
iv.	Bluetooth includes 8-cell nodes.	ZigBee includes above 6500 cell nodes.
v.	Bluetooth uses IEEE 802.15.1 specification.	ZigBee uses IEEE 802.15.4 specification.
vi.	The network range of Bluetooth ranges from 1-100 meters based on radio class.	The network range of ZigBee is upto 70 meters.
vii.	The protocol stack size of a Bluetooth is 250 kbytes.	The protocol stack size of a ZigBee is 28 kbytes.
viii.	Bluetooth uses rechargeable batteries.	ZigBee doesn't use rechargeable batteries.
ix.	Bluetooth requires less bandwidth.	As compared with Bluetooth, it needs high bandwidth.

4. Z-Wave

The Z-Wave protocol was developed by Zensys, a Danish company in 1999. It is a wireless communication protocol used primarily for home automation. Since it is low-energy protocol, it is useful for wireless control of residential appliances and other devices, such as lighting control, security systems, A/C, windows, locks etc. The advantage of this protocol is that a Z-Wave system can be controlled via the Internet from a smart phone, tablet or simply from computer or a Z-Wave gateway or central control device serving as both the hub controller and portal to the outside. Today, worldwide, over 50 million Z-Wave products are in use. Advanced Z-Wave technology does not interfere with Wi-Fi, Zigbee, or other 2.4 GHz wireless technologies in a similar band.

4.1 Z-wave Architecture

The Z-wave architecture has two types of devices. One device is acting as controller and is called as master device. Other devices connected to master device are called as slaves.

Z-wave comes with pre-programmed Network ID (called as HomeID) that is assigned to each slave. Slave does not assign a preprogrammed ID. Slaves are added to the network through a process called "inclusion".

Z-wave architecture uses a mesh network. Z-wave devices forms a mesh network, where signals intended for one device are received, amplifies and repeated by other Z-wave devices.

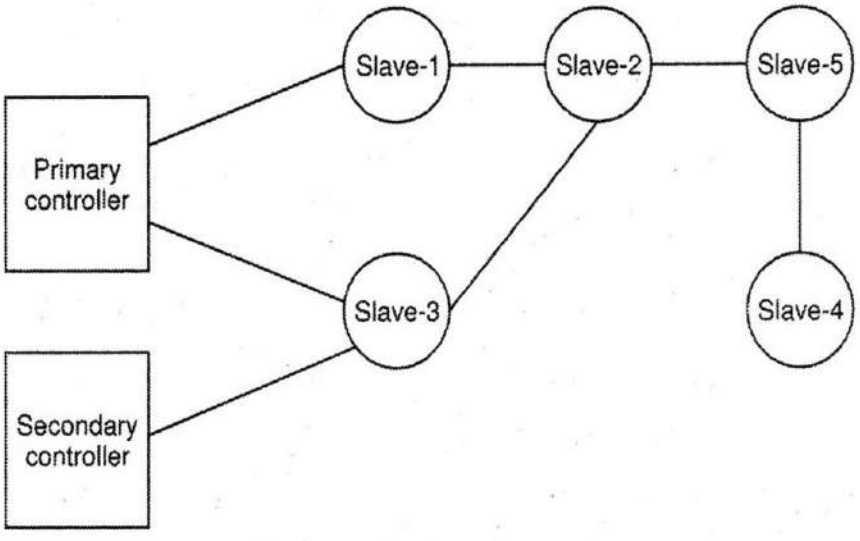


Figure 2.12: Z- Wave Network

4.2 Z-wave Protocol

The Z-wave protocol layers main function is to communicate very short messages of few bytes long from a control unit to one or more Z-wave nodes. It is a low bandwidth and half duplex protocol to establish reliable wireless communication. Z-wave protocol stack need not have to take care of large amount of data as well as any kind of time critical or streaming data.

Z-wave protocol stack has 5 layers namely

i. Physical layer

ii. MAC layer

iii. Transport layer

iv. Network layer

v. Application layer

vi. The security layer is not defined in Z-wave open protocol specifications. The major functions of these protocol layers are:

i. **Physical layer:** The physical layer in Z-wave does many functions. It takes care of modulation and RF channel allocation. It inserts known pattern (called as 'preamble') into data which is used for synchronization at receiver.

ii. **MAC layer:** MAC layer as the name suggests takes care of medium access control among slave nodes based on collision avoidance and backoff algorithms. It takes care of network operation based on Home ID, Node ID and other parameters in the Z-wave frame.

iii. **Transport layer: Details of transport layer are explained below.**

   a. It takes care of transmission and reception of frames, ACK frame transmission and insertion of checksum.

   b. Z-Wave transport layer is mainly responsible for retransmission, packet acknowledgment, waking up low power network nodes and packet origin authentication.

   c. The z-wave transport layer has four basic frame types for transferring commands in the network. The frame format for all four types of frames is mentioned below.

   d. Transport Frame = {HomeID, Source NodeID, Header, length, Data byte (0 to X), Checksum}

e. The four frame types of transport layer is explained below:

- *Singlecast frame type:* These type of frames are transmitted to one specific Z-wave node. The frame is acknowledged so that transmitter will know whether the frame is received or not. If this frame or its ACK is lost or damaged then the singlecast frame is retransmitted.
- *ACK frame type:* It is singlecast frame where in data payload part does not exist.
- *Multicast frame type:* These frames are transmitted to more than one node i.e. max. of 232 nodes. This type of frame does not support acknowledgement concept. Hence this type is not used for reliable communication.

d. Broadcast frame type: These frames are received by all the nodes in a network and they are not Acknowledged by any nodes.

iv. Network layer: The function of network layer is frame routing from one node to the other node, topology scan and routing table updates. Both the controllers as well as slave nodes participate in frame routing.

The **Z-wave network layer** is responsible for the following tasks:

a. Transmission of a frame with correct repeater list

b. Scanning of network topology

c. maintenance of routing table in the controller

v. Application layer: Takes care of control of payloads in the frames received or to be transmitted.

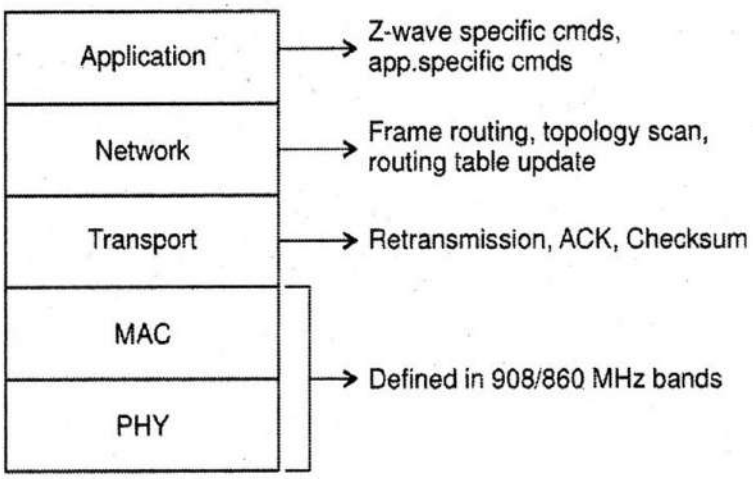


Figure 2.13: Z-wave protocol

4.3 Features of Z-Wave

i. **Secure:** Due to a unique ID assigned to each Z-wave device in a network, a gateway can never control another gateway's connected devices.

ii. **Low communication latency:** Z-wave is designed for reliable, low-latency transmission of small amounts of data (100 kbit/s maximum).

iii. **Low power:** Z-wave requires very less power so Z-wave devices can operate for up to seven years on a single battery.

iv. **Interference free:** With Z-wave, there is no interference from Wi-Fi, Zigbee, or other 2.4 GHz wireless technologies.

v. **Interoperable:** All Z-wave certified products can work with any past, present, or future Z-wave product.

5. RFID

5.1 Introduction

RFID, i.e., radio-frequency identification is a short range wireless communication technology. It is sometimes referred to as a contact-less technology and is often used in object tracking applications.

RFID is grouped under the broad category of automatic identification technologies. Some of the auto identification technologies that you are aware of include bar codes, optical character readers and some biometric technologies, such as retinal scans. These are used to reduce the amount of time and labor needed to input data manually and to improve data accuracy. Bar code system is often used to scan a label or tag to capture the data. RFID is often visualized as next generation of barcoding. It is like a barcoding system in which *tags*, or *labels* attached to the objects. Then digital data from a tag or label is captured by a device remotely and is stored in a database. RFID has several advantages over barcode systems. The main advantage is that for barcode reading optical scanner must be aligned with barcode while RFID tag can be read from far distance.

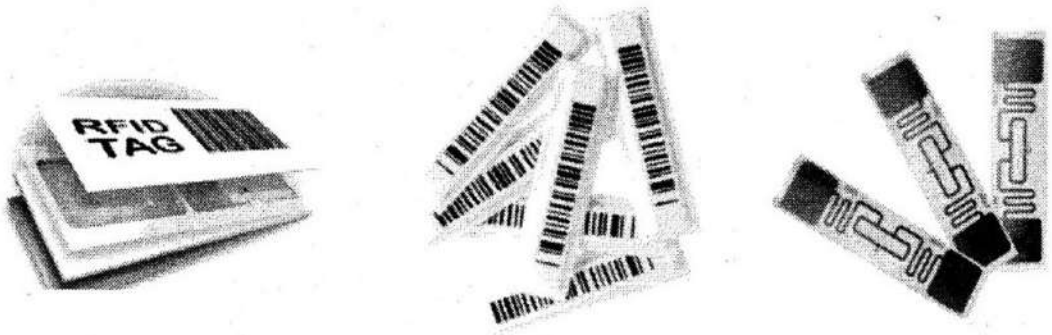


Figure 2.14: RFID tags on objects

5.2 Working of RFID System

An RFID system has four elements:

i. RFID Tag

ii. RFID Reader

iii. Communication Network

iv. Workstation

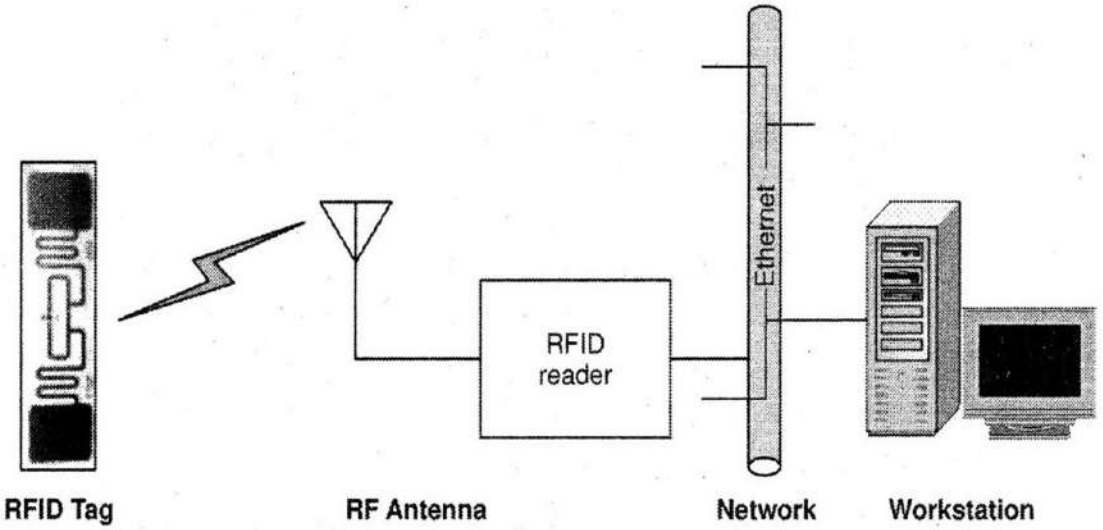
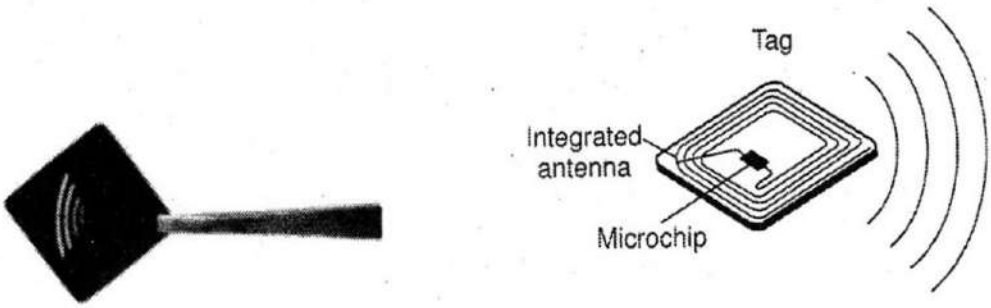


Figure 2.15: RFID System

i. **RFID tag:** An RFID tag is a tiny radio device on which the information required by user is present.



(a) RFID Tag (b) RFID Tag Structure

Figure 2.16: RFID Tag

The tags are made up of three elements: a microchip, an antenna and a substrate. The tag is nothing but a simple silicon microchip (typically less than half a millimeter in size) attached to a small flat aerial and mounted on a substrate. The whole device is then encapsulated in different material (such as plastic) depending upon its intended usage. The finished tag can be attached to an object, typically on an item, box or pallet and read remotely to ascertain its identity, position or state.

A microchip has a fixed or programmable logic for storing and processing of transmitted information. Tag also performs modulation and demodulation of radio-frequency (RF) signals which are transmitted and received by an RFID antenna.

The tag information is stored in a non-volatile memory. The information may be only a unique tag serial number or may be product-related information such as a stock number, lot or batch number, production date, or other specific information. Memory may be read-only where a factory-assigned serial number is used as a key into a database. In read/write type of memory, the system user can write object-specific data into the tag. Field programmable tags are also available which are write-once, read-multiple type.

ii. **RFID reader:** The reader, sometimes called an interrogator or scanner receives RF data from the tag via antennas. A reader may receive data from multiple antennas that are responsible for sending and receiving radio waves.

iii. **Communication network:** The data flow from the reader and the workstation is managed by existing communication network. The networking methodology can be implemented in

several different ways, depending on the frequency band used by the tag. The coverage range of RFID tag is dependent upon the transmitted power and frequency used for communication.

iv. **Workstation:** The data received from communication network is then passed to a workstation. It has dedicated software or middleware for RFID system to filter the data and route it to the correct application to be processed into useful information.

5.3 Types of RFID Tags

RFID tags are of two types:

i. Passive RFID tag

ii. Active RFID tag

i. **Passive RFID tag:** A passive tag has no power source or own transmitter, instead it uses the radio energy transmitted by the reader for it's operation. It is cheaper and smaller in size than active tag. However the power required to activate the passive tag is much higher than an active tag for signal transmission. The working of the passive tag is as follows:

   a. When passive RFID tag is scanned by a reader, the reader transmits energy to the tag.

   b. Tag receives the power and it's chip is activated.

   c. It transmits the signal back to the reader through the antenna.

   d. The reader then transmits this information back to an computer for interpretation.

ii. **Active RFID tag:** Active tag has its own transmitter and power supply. It periodically transmits RF signal. Active RFID tags use one of two main frequencies - either 433 MHz or 915 MHz - to transmit information. The working of active tag is as follows:

   a. Active tag is periodically sending the radio signals through it's antenna.

   b. It's signals are readable from several hundreds of feet away by reader.

   c. The reader then transmits this information to an RFID computer for interpretation.

d. When within range of one another, even a reader can first send out a signal to the tag which then responds back with the relevant information.

As active tag is sending out data frequently, their battery tends to deplete quicker. Once battery dies, the tag will not function unless and until battery is replaced. So the battery of an active RFID tag should be such that it would supply enough power to last for 3-5 years.

Comparison on Active and Passive RFID

Parameter	Active RFID	Passive RFID
Tag power source/battery	System uses battery powered RFID tags that continuously emits their own signals.	System uses tags with no internal power supply. Energized from the reader via RF.
Availability of tag power	Continuous	Only within field of reader
Required signal strength from reader to tag	Low	High(must power the tag)
Application characteristics	• Dynamic business process • Unconstrained asset movement • Security / sensing • Data storage / logging	• Rigid business process • Constrained asset movement • Very simple security/sensing • Limited data storage
Sensor capability	Ability to continuously monitor and record sensor input; data/time stamp for sensor events.	Ability to read and transfer sensor values only when tag is powered by reader; no date/time stamp.
Data storage	Large read/write data storage (128 kB) with sophisticated data search and access capabilities available.	Small read/write data storage (*example*:128 bytes).
Available signal strength from tag to reader	High	Low
Communication range	Long range	Short or very short range (3 m or less)
Multi-tag collection	Single reader can collect information from 1000s tags within range.	Single reader can collect information from 100 tags within 3 meters range.
Cost	Expensive	Cheaper than active RFID tag.

5.4 Limitations of RFID System

RFID systems aren't ideal compared to other tracking labels for a number of reasons. Some problems with RFID are listed as follows:

i. Security and technological issues: Because an RFID tag cannot distinguish between readers, the information can be read by almost anyone once it has left the original supply chain. Because RFID readers are so portable, and the range of some tags so great, many scanners can easily gather information. This means that anyone can collect potentially sensitive information without a person's knowledge.

ii. Another security concern for consumers is that RFID tags can be linked to individual credit cards, creating the potential for financial theft and fraud.

iii. Technology-wise, RFID tags are problematic because of lack of global or industrial standards. Since they operate on radio frequency, RFID tags and their systems can also easily become jammed or disrupted, reducing their usability.

iv. Some signaling issues can occur with RFID inventory systems, including collision - when signals from two or more readers overlap. Interference may be caused by metal, water, or other magnetic fields in the surrounding area.

v. Setting up of an RFID system is time-consuming, critical and costly.

5.5 RFID Frequency

RFID tags use three main frequencies for communication in LF, HF and UHF bands. These are :

i. **LF range:** 125 - 134 kHz, Detection range is 10-15 cm

ii. **HF range:** 13.56 MHz, detection range is 1.5 meters

iii. **Ultra High Frequency (UHF):** 433 MHz, 865 - 960 MHz, detection range is upto 12 meters.

The different applications use different frequency ranges which are listed in following table:

Frequency spectrum	Range	Data speed	Typical application
LF: 120–150 kHz	10-15 cm	Low	Animal identification, factory data collection
HF: 13.56 MHz	1.5 m	Low to moderate	Smart cards non-compliant memory cards ISO-compatible microprocessor cards
UHF: 433 MHz	1 - 100 m	Moderate	Defense applications, with active tags
UHF: 865 - 868 MHz (Europe) 902–928 MHz (North America)	1 - 12 m	Moderate to high	EAN, various standards; used by railroads

5.6 RFID Applications

RFID applications can be categorized into two types: firstly, short range applications where the reader and tag must be in close proximity (such as in access control) and secondly, medium to long range application, where the distance may be greater (such as reading across a distribution centre).

Some of the typical applications are listed below.

i. Inventory management

ii. Asset tracking

iii. Personnel tracking

iv. Controlling access to restricted areas

v. ID Badging

vi. Supply chain management

vii. Counterfeit prevention (e.g., in the pharmaceutical industry)

6. GPS (Global Positioning System)

6.1 Introduction

Most of us use GPS every single day. It has become an inseparable part of our life. It can be Google map or any other GPS based navigation application.

Global positioning system is a navigation system based on a satellite communication. It has created the revolution in navigation and position location. It is mainly used in positioning, navigation, monitoring and surveying applications. The major advantages of satellite navigation are real time positioning and timing synchronisation.

GPS is built by U.S. Department of Defense. It became fully operational since 1995. It was initially developed for military use for accurate targeting, location awareness and monitoring etc. In 1970, there was an urgent demand for improving long-distance positioning.

Traditional LORAN (Long Range Navigation) system suffers from electronic effects of weather and in particular atmospheric effects related to sunrise and sunset and has got limited capacity. So GPS based on satellite navigation system got developed.

6.2 GPS Architecture

GPS is based on network of satellites that continuously transmit coded information through radio signals. The receivers interpret the information transmitted from the satellite to identify the locations on earth accurately.

GPS architecture has three segments:

i. Space/Satellite segment (GPS satellites)

ii. Control segment (Ground control stations)

iii. User segment (GPS receivers)

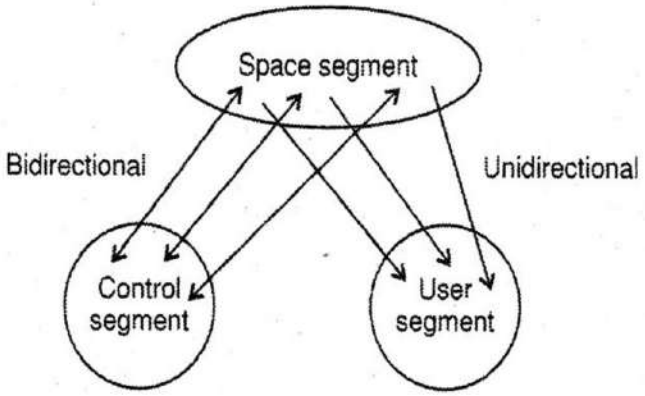


Figure 2.17: GPS Segments

i. **Space segment (GPS satellites):** Complete operational GPS space contains twenty four satellites at the altitude of approximately 20,000 km. These satellites form six groups and in each group there are four satellites (i.e. 6*4 = 24). The group of four satellites is called as one constellation. Any two adjacent constellations are separated by 60° in longitude. The orbital period of each satellite is approximately equal to twelve hours. Hence everyday all satellites revolve around the earth twice. At any instant, the GPS users will get the signals from at least four satellites.

ii. **Control segment:** The control segment consists of a master station and several monitoring stations. The monitor stations continuously monitor the GPS satellite signals. These signals are then sent to the master control station. Here operational specifications are checked and revised. Then the control signals are transmitted back to the GPS satellites through ground antennas.

This segment also takes care of the deviation of the satellites from the orbit and GPS timing.

iii. **User segment:** The user segment comprises of the GPS receiver, which receives the signals from the GPS satellites and determines the locations.

6.3 GPS Receiver

Note that, in GPS system, there is only one-way transmission from satellite to users. Hence, the individual user does not need the transmitter, but only a GPS receiver.

The block diagram of GPS receiver is shown in *figure 2.18.*

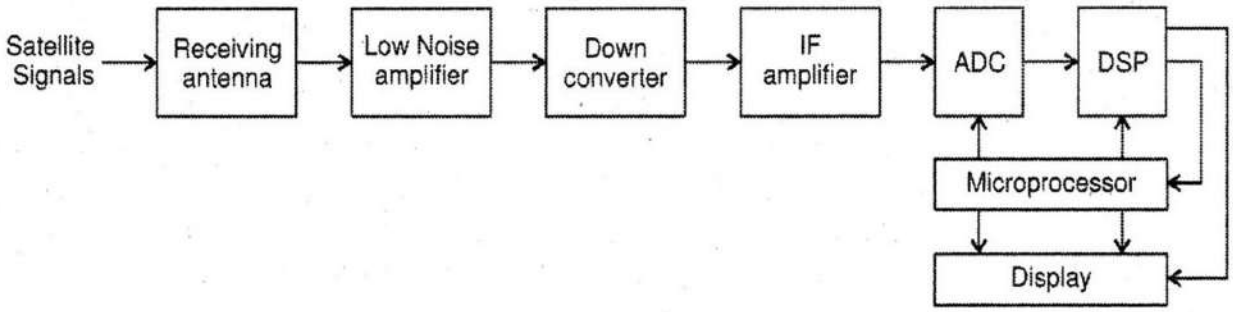


Figure 2.18: Block diagram of GPS receiver

The function of each block present in GPS receiver is mentioned below:

i. **Receiving antenna:** Receiving antenna of GPS system is mainly circularly polarized and receives the satellite signals.

ii. **Low noise amplifier:** The received satellite signals are weak. So they are amplified using low noise amplifier.

iii. **Down converter:** It converts the frequency of received signal to an Intermediate Frequency (IF) signal.

iv. **IF amplifier:** It amplifies the intermediate signals.

v. **ADC:** It accomplishes the job of converting an analog signal to digital signal. Basically, it does sampling and quantization of received signal.

vi. **DSP:** It generates the C/A code (C/A code is explained in next section).

vii. **Microprocessor:** It performs the calculation of position and provides the timing signals in order to control the operation of other digital blocks. It sends the useful information to display unit in order to display it on the screen.

6.4 How GPS Determines a Position

Three segments of GPS work in unison resulting in accurate and reliable operation of the positioning system.

It is based on the 'trilateration' principle. This technique determines the position by measuring distances to points at known coordinates.

In GPS, the four satellites are used to determine the position of the receiver on the earth. Three satellites trace the location while the fourth satellite is used to confirm the location.

The positioning system uses two main factors in determining the position:

i. Position of the user using Trilateration Principle

ii. Pseudorange Calculation

i. **Position of the user using Trilateration Principle:** To calculate the 2-D position (latitude and longitude) of a point or to track movement, a GPS receiver must be locked onto the signal of atleast three satellites. A single satellite tracks a general location of the point of interest on the earth's surface. This location information is spread over a large area. Data from a second satellite, when added to this information, allows the GPS to narrow the location. This will be the point where the two areas of satellite data overlap. Adding data from a third satellite provides more accurate position of the point.

The distance is measured using the equation:

$$\text{Distance} = \text{Travel time} \times \text{Speed of light}$$

Here travel time is the time taken by the signals to reach the receiver.

The fourth satellite is used to re-confirm and enhance the position of the user. The receiver determines the 3-D position, i.e., latitude, longitude and altitude of the point using the information from the fourth satellite. Precision increases with increase in the number of satellites in the vicinity.

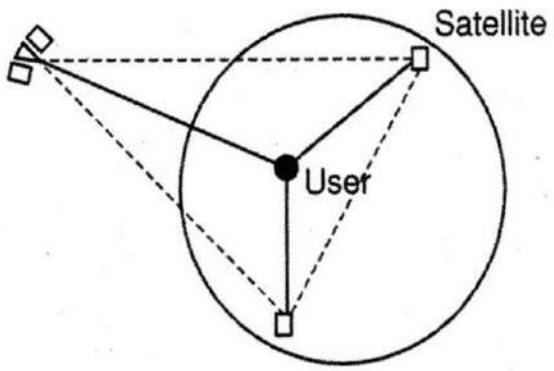


Figure 2.19: Trilateration principle

ii. **Pseudorange Calculation:** We have seen that GPS satellite rotates twice a day around the earth. It transmits signals on the same two carrier frequencies F_1 and F_2. F_1 is

1575.42 MHz and F_2 is 1227.60MHz. Transmission uses spread spectrum technology and it uses two codes -

a. Coarse and Acquisition code (C/A)

b. Precise code (P)

The signal F_1 is modulated with 1.023 Mbps pseudo random bit sequence. This code is called as *Coarse Acquisition Code or C/A code* and it is used by the public. C/A code consists of identification of each satellite and navigation information. The C/A code pattern is used by the user to search the specific satellite to compute the distance to each satellite using time frames.

The signal, F_2, is modulated with 10.23 Mbps pseudo random bit sequence. This code is called as Precise Code or P Code and it is used in military positioning systems. The P code gives better measurement accuracy as compared to C/A code since the bit rate of P code is greater than the bit rate of C/A code.

6.5 GPS Errors

i. There are many sources of possible errors that will degrade the accuracy of positions computed by a GPS receiver. The travel time taken by the GPS satellite signals can be changed by atmospheric effects. *For example*, the speed of the GPS signal when travelling through the ionosphere and troposphere is different than the speed of the GPS signal in space.

ii. Another source of error is noise or distortion of the signal which causes electrical interference or errors inherent in the GPS receiver itself.

iii. Information about satellite orbits will cause errors in determining the positions.

iv. Small variations in the electronic clock of the satellites can translate to large position errors. A clock error of 1 nsec translates to 1 feet or 0.3 m user error on the ground.

v. A multipath effect occurs when signals transmitted from the satellites bounce back from a reflective surface before reaching to receiving antenna. During this process, the receiver gets the signal in a straight line path as well as the delayed path. The effect is similar to a ghost.

6.6 Advantages of GPS

i. GPS satellite-based navigation system is an important tool for military, civil and commercial users.

ii. Vehicle tracking systems, GPS-based navigation systems can guide us with turn by turn directions.

iii. Very high speed.

6.7 Disadvantages of GPS

i. The highest accuracy requires line-of-sight from the receiver to the satellite.

ii. GPS satellite signals are too weak as compared to phone signals. So it doesn't works well in indoor, underwater, under trees etc.

6.8 Applications of GPS

i. To create digital maps.

ii. To determine position locations, e.g., you need to guide CAB driver about your positon locations so that he can pick you up.

iii. To navigate from one location to another, e.g., will guide you the path when you are travelling to an unknown location.

iv. To determine the distance between two different points.

Exercises

A. Multiple choice questions

1. Bluetooth is the wireless technology for
   a. local area network
   b. personal area network
   c. both (a) and (b)
   d. none of these

2. In the piconet of bluetooth one master device
   a. can not be slave
   b. can be slave in another piconet
   c. can be slave in the same piconet
   d. none of these

3. A scatternet can have maximum
   a. 10 piconets
   b. 20 piconets
   c. 30 piconets
   d. 40 piconets

4. The bluetooth supports
   a. point-to-point connections
   b. point-to-multipoint connection
   c. both (a) and (b)
   d. none of these

5. An interconnected collection of piconet is called
   a. scatternet
   b. mininet
   c. micronet
   d. none of these

6. Bluetooth transceiver operates in _____band?
   a. 101 MHz
   b. 2.3 GHz
   c. 2.4 GHZ
   d. 2.6 GHz

7. Bluetooth uses
   a. orthogonal frequency division multiplexing
   b. time division multiplexing
   c. frequency hoping spread spectrum
   d. None of these

8. Bluetooth architecture has _____ layers
   a. 5 b. 6
   c. 7 d. 4

9. What is the IEEE specification used for Bluetooth?
   a. 802.15 b. 802.14
   c. 802.10 d. 802.16

10. Bluetooth standard is named after _____
   a. King Ronaldo Bluetooth
   b. Pope Vincent Bluetooth
   c. King Herald Bluetooth
   d. Pope Francis Bluetooth

11. Which modulation scheme is used by Bluetooth?
   a. QPSK b. QAM
   c. FSK d. GFSK

12. RFID stands _____.
   a. Radio-Frequency Indication
   b. Radio-Frequency Identification
   c. Radio-Frequency Interconnection
   d. None of the above

13. Which of the following is not RFID type?
   a. Ultra-Low frequency b. Low frequency
   c. High frequency d. Ultra-High frequency

14. Which of the following businesses benefit and implemented RFID?
   a. Logistics and Transportation b. Building and Construction
   c. IT d. All the above

15. The information on read-only chips _____ be changed.
   a. Can b. Cannot
   c. Sometimes can d. None of the above

16. There are _____ basic types of chips available on RFID tags.
   a. Two b. Three
   c. Four d. Five

17. Which one of the following statements is true?
    a. RFID tags require laser scanning.
    b. A passive RFID tag does not use an antenna.
    c. An active RFID tag does not require a power source.
    d. Normally passive RFID tags store ID numbers.

18. Which of the following RFID tag has battery?
    a. Active
    b. Passive
    c. Active and Passive
    d. None of the above

19. Basic elements of RFID system are _____
    a. RFID tag
    b. RFID reader
    c. RFID Computer system
    d. All of the above

20. Which of the following statements about radio frequency identification (RFID) is not true?
    a. Companies may be required to upgrade hardware and software to accommodate the massive amounts data that are being produced by RFID systems.
    b. RFID systems transmit radio signals over long distances.
    c. RFID systems use tiny tags with embedded microchips containing data about an item and its location.
    d. RFID systems provide a powerful technology for tracking the movement of goods throughout the supply chain.

21. What is the use of the RFID Module?
    a. Object Identification
    b. To provide 3G Connectivity
    c. To measure temperature
    d. To measure Wi-Fi strength

22. Zigbee network layer supports the following topologies except:
    a. tree
    b. bus
    c. star
    d. mesh

23. In a Zigbee network, a single device that controls the network is called _____.
    a. master
    b. server
    c. coordinator
    d. pointer

24. Devices being controlled in a zigbee network are known as _____.
    a. end devices
    b. clients
    c. slaves
    d. coordinators

25. Which of the following is not a characteristic of a Zigbee network?
    a. Low Power Consumption
    b. High data rates
    c. Easy installation
    d. Unlicensed radio bands

26. Which of the following layers are defined by the Zigbee Stack?
    a. Network layer
    b. Physical Layer
    c. Application Support Layer
    d. Medium Access Layer

27. What is the typical range of transmission distance in a ZigBee network?
    a. 5 m
    b. 50 m
    c. 500 m
    d. 5 km

28. To determine the accurate position of the object, GPS receiver must receive signals from - _____satellites?
    a. 1
    b. 2
    c. 3
    d. 4

29. What does GPS stand for?
    a. Going Places Sometimes
    b. Global Positioning System
    c. Government Positioning Satellites
    d. Global Positioning Satellites

30. What is the total number of GPS satellites?
    a. 4
    b. 6
    c. 10
    d. 24

31. What kind of information does a GPS satellite transmit to the GPS receiver?
    a. The orbital information for all the other GPS satellites in the fleet
    b. The time the message was sent
    c. The location of the GPS satellite
    d. All of these

32. What is the approximate time taken by the GPS for one complete orbit?
    a. 11 minutes
    b. 45 minutes
    c. 5 hours
    d. 12 hours

33. What is the reason for sending two transmissions in the same band?
    a. Redundancy
    b. Ionosphere refraction corrections
    c. Multiplexing
    d. Reducing traffic

34. Accuracy of the position through can be influenced by_____

a. Refraction b. Reflection
c. Signal strength d. Position of satellite

35. Basic principle of GPS positioning is

a. Analytical resection b. Triangulation
c. Trilateration d. Graphical resection

36. In case of GPS positioning, positions of _____ are considered to be objects at known positions

a. Receivers b. Satellites
c. Controllers d. Signals

37. The most significant error in GPS is_____

a. Ionosphere error b. Cycle slip
c. receiver clock d. User

B. Answer in one or two lines

1. Name any two short range wireless technologies.
2. What is advantages of bluetooth technology.
3. What is operating frequency band of bluetooth technology?
4. Define piconet and scatterenet for Bluetooth technology.
5. Draw piconet and scatternet architecture.
6. How Bluetooth devices are classified according to output power?
7. Which spread spectrum technology is used in bluetooth?
8. What is the bandwidth of one channel of bluetooth?
9. Which modulation technique is used in bluetooth?
10. Draw bluetooth packet format.
11. What is maximum length of access code and state its different fields.
12. What are advantages of ZigBee?
13. What is IEEE standard on which ZigBee is operated?

14. How ZigBee devices/nodes are classified?
15. Name the layers of ZigBee architecture.
16. Name the ZigBee topologies.
17. Mention any four disadvantages of ZigBee.
18. What is difference between RFID and bar code?
19. Name the components of RFID tag.
20. Which are two types of RFID tags?
21. What is active RFID tag?
22. What is passive RFID tag?
23. Mention any two limitations of RFID.
24. Which frequency bands are normally used by RFID.
25. State any two applications domains of RFID.
26. Who has developed Z-wave protocol?
27. State five layers of Z-wave protocol?
28. Give frame format of transport frame.
29. Give any two features of Z- wave.
30. Which are applications of GPS?
31. Which are three segments of GPS?
32. Which are block of GPS receiver?
33. Which two principles are used by GPS to determine position?
34. Name the two codes used on psedorange calculations.
35. Which are main error sources of GPS to locate position?
36. Mention any two advantages of GPS system.
37. Mention any two disadvantages of GPS system.

C. Answer in detail

1. Explain piconet of Bluetooth.
2. Explain scatternet of Bluetooth.
3. Explain Bluetooth protocol stack.
4. In detail explain core protocol of bluetooth.
5. Which protocols are adopted by bluetooth architecture.
6. Explain Bluetooth frame structure.
7. Explain ZigBee devices architecture.
8. Draw and explain ZigBee architecture.
9. Explain following topologies used in ZigBee
   i. Star ii. Tree
   iii. Cluster tree iv. Mesh
10. What are advantages and disadvantages of ZigBee system?
11. Write application domain of ZigBee. Explain any one in detail.
12. How Zigbee is useful in Wireless Sensor Network(WSN).
13. Compare Bluetooth and Zigbee.
14. Explain working of RFID system.
15. Write note on RFID tag.
16. Explain passive RFID tag.
17. Explain active RFID tag.
18. Compare active and passive RFID tags.
19. Which are limitations of RFID systems?
20. Explain Z-wave architecture.
21. Write in detail transport layer of Z-wave.
22. Which tasks are performed by network layer of Z-wave?
23. Write any four features of Z-wave.

24. Explain three segments of GPS.
25. Write note on space/ satellite segment of GPS.
26. Draw and explain GPS receiver.
27. How GPS determines a position of an Object?
28. How trilateration principle is used for position detection in GPS?
29. Explain pseudorange calculation method for position detection in GPS.
30. Which are sources of errors in locating correct position using GPS.

Answers

1.	b	2.	b	3.	a	4.	c	5.	a
6.	c	7.	c	8.	a	9.	a	10.	c
11.	d	12.	b	13.	b	14.	d	15.	b
16.	a	17.	c	18.	b	19.	d	20.	a
21.	a	22.	b	23.	c	24.	a	25.	b
26.	a and c	27.	b	28.	d	29.	b	30.	d
31.	d	32.	d	33.	b	34.	d	35.	a
36.	b	37.	c						

Unit 3

IoT Architecture

1. Introduction to IoT

For last five decades, growing applications in wireless communication have been witnessed since the evolution of Internet. The internet has undergone severe changes since its first launch "ARPANET" in 1960s.

The reach of internet is growing faster than ever before. The internet is not just limited to desktop, laptops, smartphones, but new internet connected devices has been introduced to the general public. The things you used to read in the science fiction novels are now becoming real because of the new upcoming technology "INTERNET OF THINGS". The Internet of Things (IoT) has gradually transformed the way daily tasks are completed. The technology has made our lives more comfortable and secure. Smart home, smart city, smart medical wearable gadgets are all *examples* of IoT. Let us consider an *example* of smart home for instance. People can start their cooling devices, lights, various appliances remotely through their mobile phones or can be programmed for automatic On/Off.

Below are some of the *interesting applications of IoT system*:

i. In morning, when you open your eyes, you noticed that alarm rings at 6.15 am while you have set it for 6.00 am. You must be wondering how it could happen without human intervention. But it's possible in IoT world. The clock has checked the train timing online

and got the information that your train is delayed by 15 minutes. So it lets you sleep a little longer.

ii. In your kitchen, a blinking light reminds you it's time to take your tablets if you forget to take it on time.

iii. Your umbrella handle is lit up automatically and has indicated you to carry it with you as umbrella has received weather reports which has predicted rainfall.

iv. Refrigerator place an order to shopkeeper for eggs after noticing that egg-tray is empty.

v. In advance, one will receive intimation on mobile by car indicating the less fuel level in the tank and warns you about need of refilling it.

There are such 'N' numbers of *examples* of the internet of things in our daily lives. In all these *examples*, we have used the internet to send/receive the information. Note that in each case the gadget that was connected to the internet wasn't a computer, tablet or a mobile phone but an object or a thing like alarm clock, tablet, umbrella, refrigerator and car. These things are designed for a specific purpose.

So let us study details of interesting and upcoming technology: *Internet of Things!!*

2. What is Internet of Things?

Let us see the technical definition of IoT. It is a global network of interconnecting devices that interact with each other and with user using different communication methods.

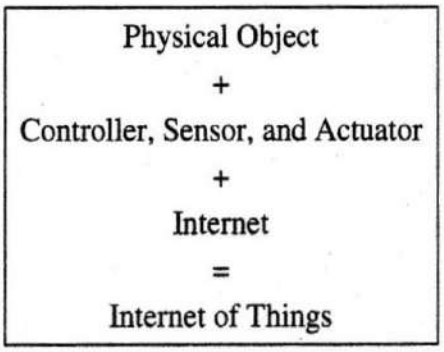
There are basically three components of IoT:

i. Physical object

ii. Controller, sensor and actuators

iii. Internet

Thus very simple equation of IoT is:



An equation for the Internet of Things

In previous courses of electronics subjects, you have separately studied these three components. Integration of proper devices will make an IoT system.

3. Evolution of IoT

As stated earlier, history of IoT started with ARPANET. During recent years, one of the most familiar name scaling new heights and creating a benchmark is Internet of Things (IoT). It has transformed Things (objects) of the real world into smarter devices.

Since its invention, IoT technology has paved a journey so successful that today IoT is one of the topmost business drivers. Let us have a look at how the evolution of IoT happened over a period of time along with the timelines:

i. **Year 1999:** The term Internet of Things (IoT) was framed by Kevin Ashton, MIT in 1999. He linked objects to the internet using the RFID tags.

ii. **Year 1999:** In the same year, Device to Device (D2D) communication concept was coined by Bill Joy.

iii. **Year 2000:** LG Internet Digital DIOS invented the first internet connected refrigerator in the world. It had used a LAN port for IP connectivity.

iv. **Year 2001:** David Brock MIT, proposed a new object identification scheme for unique identification and tracking of objects throughout the product life cycle using the internet.

v. **Year 2003:** The 'Project JXTA-C', enabled a web of things. The aim of the project was to assign a unique number for every object to replace the unique barcode system in the world.

vi. **Year 2005:** Single-board micro-controller was developed at Italy.

vii. **Year 2008:** Various industrialists formed the IPSO Alliance to promote technology related with connected devices. This was a major jump towards implementation of IoT on larger scale.

viii. **Year 2011:** The most recent version of Internet Protocol was released. Launching of new protocol IPv6 was a turning point for IoT.

ix. **Year 2013-14:** IoT devices started using sensors to accurately sense the surrounding environment parameters. This allowed people to control home lighting, garage doors from their phones.

x. **Year 2014:** Dublin became the first IoT city. Smart Dublin installed hundreds of smart bins, sensors for monitoring flood levels and sensors for monitoring sound level of city.

xi. **Year 2017 onwards:** Billions of IoT devices got installed for military, healthcare, agriculture, industrial automation, transportation etc. purposes.

Figure 3.1 shows percentage of 10 most widely used IoT applications.

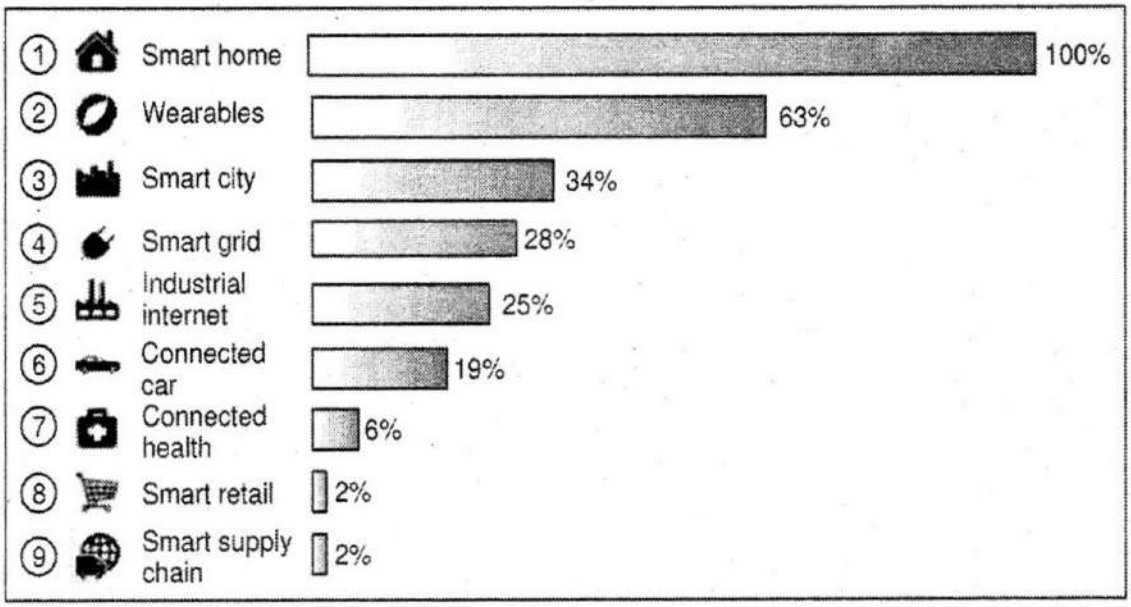


Figure 3.1: Popularity of IoT applications

Future of IoT

It is predicted that over zettabytes of IoT devices will be connected to the internet till 2025. Though it's difficult to predict exact number, we can all agree that the IoT industry will continue to grow and progress with continued innovation.

4. M2M and IoT

In previous sections, we have learned about basis of IoT and its evolution. Another term which is often used synonymously with IoT is Machine-to-Machine (M2M). Though IoT and M2M are often used interchangeably, there are certain differences between M2M and IoT. These are discussed in this section.

4.1 M2M

Machine-to-Machine (M2M) refers to networking of machines (or devices). It's main purpose is remote monitoring, control and data exchange. Architecture of M2M system consists of:

i. M2M area network

ii. Communication network

iii. Application domain

Now let us study these in detail.

i. **M2M area network**: It comprises of machines which are also called as M2M nodes. These have hardware modules for sensing, actuation and communication.

ii. **Communication network**: It provides connectivity to remote M2M area networks. The communication network can be either wired or wireless. It uses IP-based networks. Various communication protocols used are ZigBee, Bluetooth, M-bus, 6LoWPAN, IEEE 802.15.4 etc.

To enable the communication between remote M2M area networks, M2M gateways are used. Gateway performs translations from/to native protocols to/from Internet Protocol (IP).

v. **Year 2003:** The 'Project JXTA-C', enabled a web of things. The aim of the project was to assign a unique number for every object to replace the unique barcode system in the world.

vi. **Year 2005:** Single-board micro-controller was developed at Italy.

vii. **Year 2008:** Various industrialists formed the IPSO Alliance to promote technology related with connected devices. This was a major jump towards implementation of IoT on larger scale.

viii. **Year 2011:** The most recent version of Internet Protocol was released. Launching of new protocol IPv6 was a turning point for IoT.

ix. **Year 2013-14:** IoT devices started using sensors to accurately sense the surrounding environment parameters. This allowed people to control home lighting, garage doors from their phones.

x. **Year 2014:** Dublin became the first IoT city. Smart Dublin installed hundreds of smart bins, sensors for monitoring flood levels and sensors for monitoring sound level of city.

xi. **Year 2017 onwards:** Billions of IoT devices got installed for military, healthcare, agriculture, industrial automation, transportation etc. purposes.

Figure 3.1 shows percentage of 10 most widely used IoT applications.

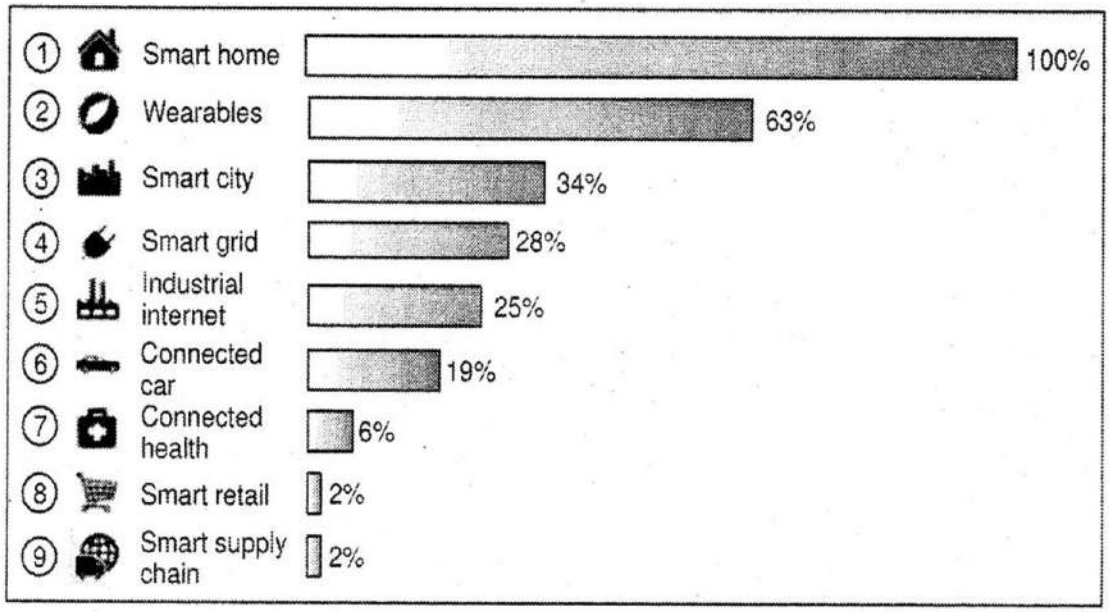


Figure 3.1: Popularity of IoT applications

Future of IoT

It is predicted that over zettabytes of IoT devices will be connected to the internet till 2025. Though it's difficult to predict exact number, we can all agree that the IoT industry will continue to grow and progress with continued innovation.

4. M2M and IoT

In previous sections, we have learned about basis of IoT and its evolution. Another term which is often used synonymously with IoT is Machine-to-Machine (M2M). Though IoT and M2M are often used interchangeably, there are certain differences between M2M and IoT. These are discussed in this section.

4.1 M2M

Machine-to-Machine (M2M) refers to networking of machines (or devices). It's main purpose is remote monitoring, control and data exchange. Architecture of M2M system consists of:

i. M2M area network

ii. Communication network

iii. Application domain

Now let us study these in detail.

i. **M2M area network**: It comprises of machines which are also called as M2M nodes. These have hardware modules for sensing, actuation and communication.

ii. **Communication network**: It provides connectivity to remote M2M area networks. The communication network can be either wired or wireless. It uses IP-based networks. Various communication protocols used are ZigBee, Bluetooth, M-bus, 6LoWPAN, IEEE 802.15.4 etc.

To enable the communication between remote M2M area networks, M2M gateways are used. Gateway performs translations from/to native protocols to/from Internet Protocol (IP).

iii. **Application domain:** M2M has various application domains such as smart metering, home automation, industrial automation, smart grids etc. Application domain of M2M designs, architecture for data collection, storage and analysis according to application requirement.

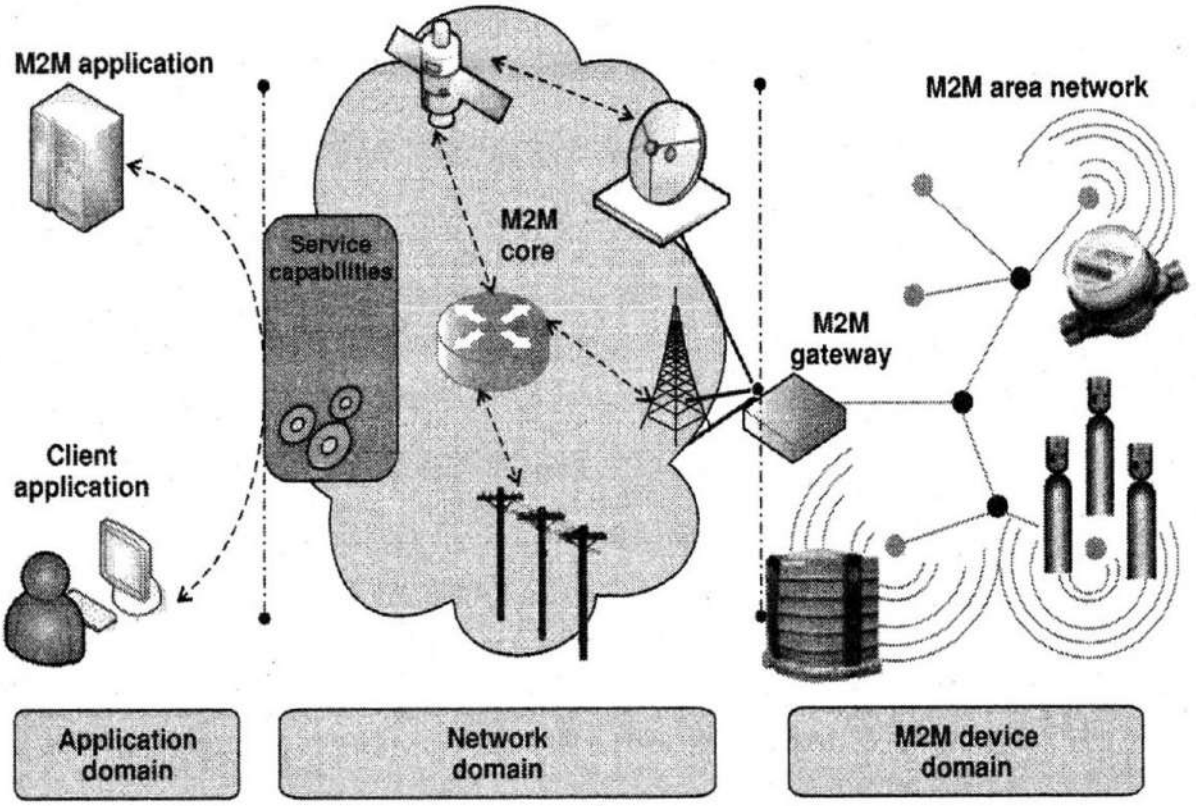


Figure 3.2: M2M system architecture

4.2 Differences between IoT and M2M

Though both M2M and IoT involve networking of machines and devices, they differ in the underlying technologies, system architectures and types of applications. Major differences are listed below:

Parameter	M2M	IoT
Communication Protocol	Commonly used protocols are mainly below network layer protocols such as ZigBee, Bluetooth, PLC, 6LoWPAN, IEEE 802.15.4, Z-Wave.	Protocols used are of above network layer protocols such as HTTP, Web Sockets, MQTT, DDS, AMQP etc.
Machines in M2M vs Things in IoT	Typically have homogenous machine types within an M2M area network.	"Things" in IoT are heterogeneous physical objects having unique IP/MAC addresses.[e.g. smart home includes IoT devices of various types such as fire alarms, door alarms, lighting control devices etc.]
Hardware vs Software emphasis	Emphasis of M2M is more on hardware with embedded modules.	The emphasis of IoT is more on software.
Data collection and analysis	M2M data is collected in point solutions and often in on-premises storage infrastructure.	The data in IoT is collected in cloud (either public or private or hybrid).
Applications	Application domains include diagnosis applications, service management applications and on premises enterprise applications.	Since cloud is used for massive data collection, cloud-based real-time and batch data analysis frameworks can be used. So IoT is used in applications in education, healthcare, finance, retail, supply-chain, manufacturing and other industries.

5. IoT Architecture

Widespread use of IoT demands a reliable architecture for successful implementation of IoT applications. Typically, the seven layer architecture used for IoT has the following layers:

i. Physical devices and controllers (The "Things" in IoT)

ii. Connectivity (Communication and Processing units)

iii. Edge computing (Data Element Analysis and Transformation)

iv. Data Accumulation (Storage)

v. Data Abstraction (Aggregation and Access)

vi. Application (Reporting, Analytics, Control)

vii. Collaboration and Processes (Involving people and business processes)

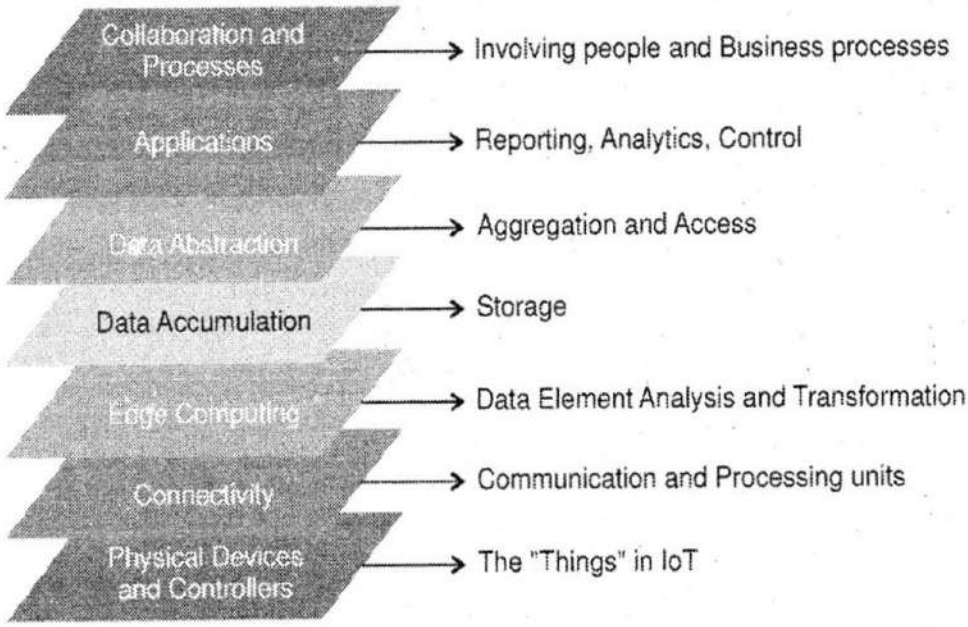


Figure 3.3: Seven layer architecture of IoT

i. Layer 1: Physical Devices

The first layer is covered with the "Things" in the IoT. It has controllers and physical equipments which are used to control devices and to send/receive data.

ii. Layer 2: Connectivity

This layer is responsible for communication between devices via multiple networks. It executes the following tasks:

a. Set up a connection with the first layer devices

b. Deliver the data throughout the network

c. Implement different device compatible protocols

d. Used for routing and switching

e. Serves as an added protection measure for the network

iii. Layer 3: Edge Computing

This is an important layer of IoT architecture which takes care of data formatting. It performs the following tasks:

a. Filter the data

b. Clean up the data

c. Aggregate the data

d. Provide evaluation for validation so that the data can be processed by the fourth layer.

e. Reformat the data so that it can help in more complex and higher level computations.

f. Used for expanding and decoding

g. Compress the data to reduce traffic

h. Generate events for any alerts

iv. Layer 4: Data Accumulation

The real-time data coming from the sensor is constantly changing. After data is filtered through the layer 3, a lot of data is decreased. Data accumulation layer maintains the data in an accessible format.

v. Layer 5: Abstraction

The objective of this layer is to render data along with its storage with such a strategy that can help developers to write easier applications.

vi. Layer 6: Application

It processes data in order to ensure that it is accessible for everyone. It is associated with both the physical and software layer. It is used for data interpretation to create reports.

vii. Layer 7: Collaboration and Processes

Seventh layer offers action or response that can help against the provided data. For *example*, this action can be an electromechanical device's actuation after a trigger from the controller.

6. Role of Cloud in IoT

Apart from providing smarter solutions for homes and housing communities, IoT has also been used in business environments across various industries. However, with the amount of huge amount of data that is generated by IoT, a lot of strain is put on the internet infrastructure. This has made businesses and organizations look for an option that would reduce this load. Use of cloud in IoT system is the solution for this.

Today, cloud computing has more or less penetrated mainstreams of IT and its infrastructure. Many tech biggies such as Amazon, Alibaba, Google and Oracle are building machine learning tools with the help of cloud technology to offer a wide range of solutions to businesses worldwide.

6.1 Advantages of using Cloud in IoT

i. **Increased data storage:** Cloud acts as a large, virtually never ending storage for huge data generated in IoT applications. It also manages big data and has virtually unlimited computing capabilities.

ii. **Mobility:** The data stored and processed in the cloud server can be accessed from almost anywhere in the world. It means that it won't be bound by any infrastructural or network limitations. Mobility is very essential when it comes to IoT projects requiring real-time monitoring and management of connected devices. It allows developers to implement projects without delay.

iii. **Provides security and privacy:** Cloud has made IoT more secure with preventive, detective and corrective controls. It has enabled users with strong security measures by providing effective authentication and encryption protocols.

iv. **Scalability:** What exactly does scalability mean as it pertains to the Internet of Things? Scale, by definition, refers to the capability of a system, network, or process to handle a growing amount of work, or its potential to be enlarged in order to accommodate that growth.

Cloud-based IoT system is easily scalable. It's possible to add another virtual server or more cloud space to implement new techniques. Furthermore, IoT cloud platform services offer flexibility in case you want to scale down the number of IoT-enabled devices. On the

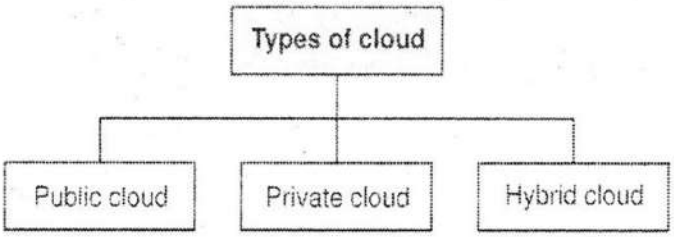
other hand, scaling up of IoT system without cloud requires purchasing of hardware and upgradation of configuration. This would increase developing time and cost.

v. **Removes entry barrier for hosting providers:** Today, many innovations in the field of IoT need plug-and-play hosting services. With the cloud, most hosting providers allow their clients a ready-to-roll model.

Thus cloud computing and IoT work towards increasing the efficiency of everyday tasks and both have a complementary relationship. On one hand, IoT generates lots of data while on the other hand, cloud computing paves way for this data to travel. It is essential that both cloud and IoT form cloud-based IoT applications in a bid to make the most out of their combination. This alliance has led to the success of IoT.

6.2 Cloud Topologies

Cloud computing is dictated by some specific topologies. One has to select the proper one as per the application. Cloud topology can be broadly categorized as:



i. **Public Cloud:** In this topology, a third party owns and manages the entire infrastructure and the hardware of a business. User has to pay only for the consumed resources and need not worry about the hardware. Therefore, public cloud is the most cost effective topology for cloud server hosting.

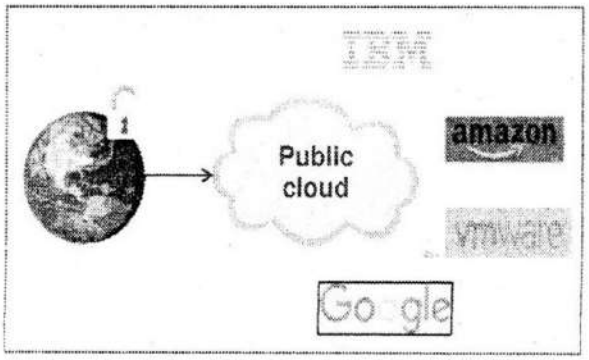


Figure 3.4: Public Cloud

The features of public cloud are:

a. High scalability
b. Pay as you use
c. Cost-effective
d. Easy deployments
e. Reliable
f. Continuous uptime
g. Zero maintenance

ii. **Private Cloud:** Private cloud can be of two types - dedicated private cloud and managed private cloud.

In *dedicated private cloud*, the hardware is placed at a data center. It is managed and owned by the user. Obviously, this is the most expensive setup. Therefore, dedicated private cloud is mostly used by large organizations.

In *managed private cloud*, the hardware is managed by a third party and is installed at an external location. Here, one can utilize the best of a dedicated private cloud's control and security while reducing complexity of creating a data center.

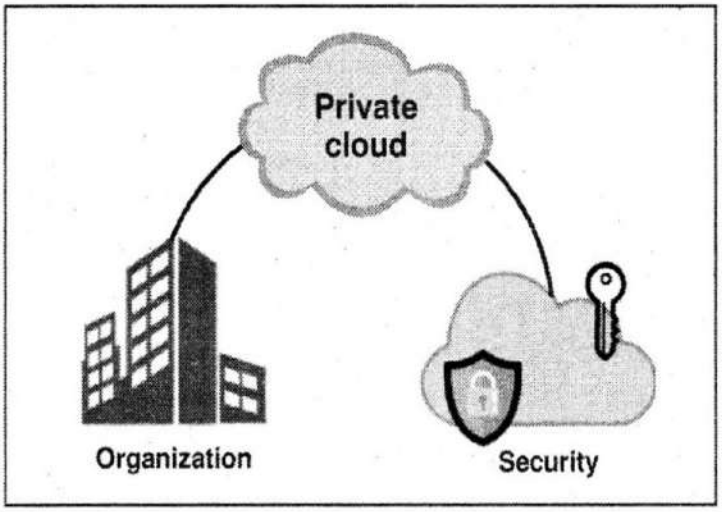


Figure 3.5: Private Cloud

The features of private cloud are:

a. Most secure
b. Good performance
c. High reliability
d. Less risky
e. Agility
f. Efficient

iii. **Hybrid Cloud:** Hybrid cloud is a combination of the public and private clouds. It combines control and security of private cloud and cost saving advantage of public cloud. It achieves this by using the public cloud for non-critical information while the private cloud is utilized for sensitive data.

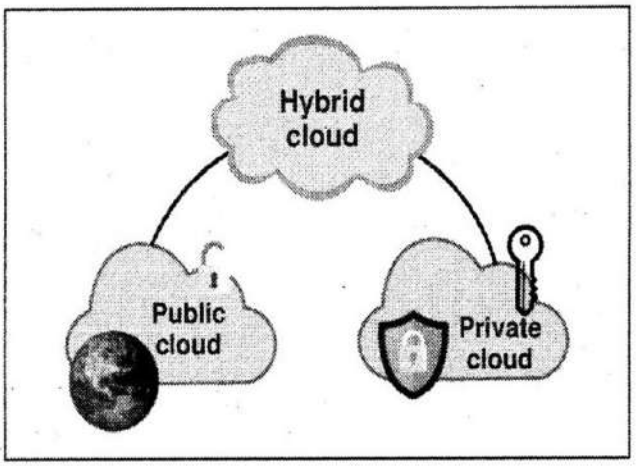


Figure 3.6: Hybrid cloud = Public Cloud + Private Cloud

The features of hybrid cloud are:

a. High scalability
b. Very secure
c. Improved cost
d. High reliability
e. Easy transition

6.3 Cloud Access

In the previous section, we have seen advantage of using Cloud in IoT. A cloud-based service can be utilized and consumed in different ways. There are three key service models in the cloud.

i. Infrastructure as a Service (IaaS)

ii. Platform as a Service (PaaS)

iii. Software as a Service (SaaS)

i. IaaS (Infrastructure as a Service): It is the most basic level of cloud based solutions. In this model, outsourcing of infrastructure elements is allowed. e.g., storage, networking, load balancers and virtualization. If anyone wants to deploy cloud application, he/she has to install images of the operating system along with the concerned application software. In IaaS, the user is responsible to maintain, update and patch the operating system and install the required application software. Cloud provider will charge the concern depending upon the usage of provided resources.

Advantage: IaaS offers high level control by which one can select the basic components of infrastructure. The pooling of storage and computing resources can allow with easy and quick scaling.

e.g. Amazon EC2 and S3, Google Compute Engine, Windows Azure.

ii. PaaS (Platform as a Service): In PaaS, apart from providing an infrastructure, cloud providers also issue an on-demand computing environment to develop, test, run and collaborate with components such as web services, database management systems and software development kits for various programming languages. In PaaS, the lower level is not user headache. Security, load balancers, network topology and the infrastructure are managed by the cloud provider.

One can easily use PaaS platform to deploy his/her own applications and configure them to scale down or scale up own functionalities.

Advantages: User need not worry about managing operation system, running updates or upgrading the hardware. It is the responsibility of cloud provider.

e.g., AWS, Elastic Beanstalk, Heroku, Google App engine.

iii. SaaS (Software as a Service): SaaS providers offer fully functional web-based application softwares. SaaS provider is responsible to supervise everything, which

includes firewalls, load balancers and infrastructure. Runtime environments and operating systems like Java and .NET, business applications and even emails are handled by the provider. The user of SaaS service is known as tenant. The architecture is known as a multitenant architecture. The provider vertically partitions its servers.

Advantage: It does not need much investment for software licensing or servers. e.g., Microsoft Office 365.

Following is a diagrammatic representation of the above three service categories:

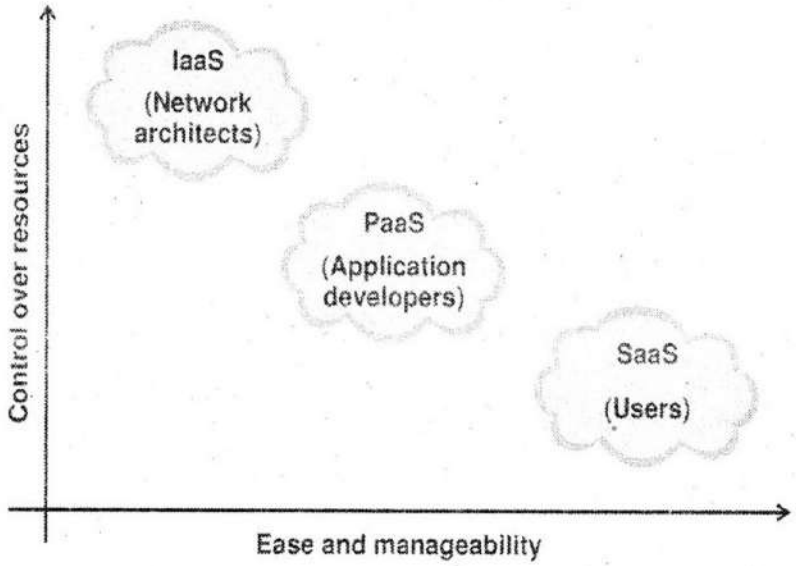


Figure 3.7: Cloud access Types

7. Communication Protocol used in IoT

Communication protocol is one of the important piece in IoT for seamless connectivity. The IoT system uses number of protocols intended to serve different purposes. Communication speed, reliability and connection durability affects the IoT system performance.

Following are the IoT protocols used at different architecture layers of IoT.

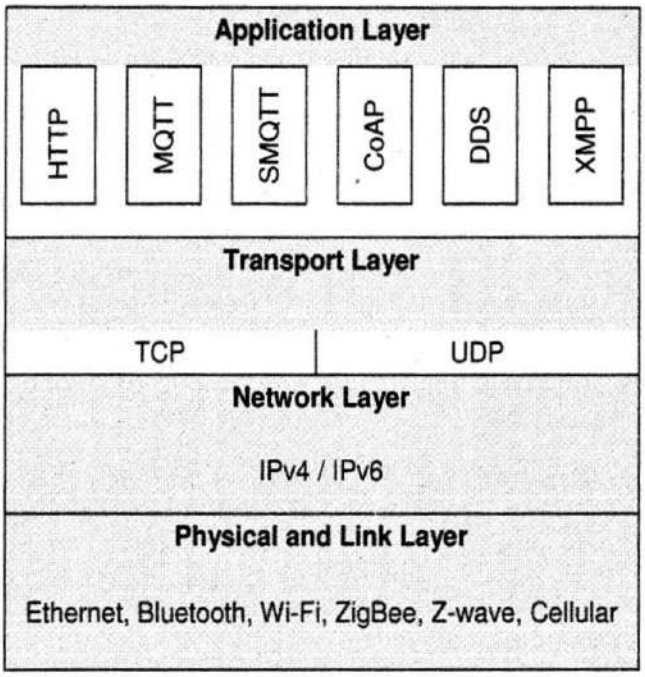


Figure 3.8: Communication protocol suite used in IoT

7.1 Physical and Link Layer Protocol

Developers and engineers can use a wide range of connectivity options with IoT systems and products. The network protocols used are Wi-Fi, ZigBee, Bluetooth, 3G/4G/5G cellular etc.

i. **Bluetooth**: It is one of the most important networking protocols used for wearable devices.

ii. **ZigBee**: It is used more in industrial set ups. ZigBee Remote Control (RF4CE) provides high security, scalability, robustness and low power consumption for complex systems along with a high number of nodes. It can increase the sensor networks and wireless control in the IoT and M2M applications.

iii. **Z-wave:** This low power RF communication protocol is used for the IoT automation system. It works with less than 1 GHz band, data rate of 100 kbits/s and can provide control of at least 232 devices.

iv. **Wi-Fi:** Widespread use of Wi-Fi devices at homes/offices, it is used for speedy transfer of huge data. However, it consumes large power for several IoT applications.

v. **Cellular:** Long distance communication applications of IoT use 3G/4G/5G cellular. The protocol is recommended for IoT systems that involves sensors and deals with low data bandwidth.

7.2. Network Layer

One of the prominent protocol used in IoT applications is Internet Protocol version 6 or IPv6. Exponential increase of interconnected users, platforms, devices and various other services has created a challenge of assigning unique identity to each. To overcome this, IPv6 came into existence in 1998. It allows IP address of 128 bits. This naturally gives us a massive amount of billions of unique IP addresses. However in IoT, one has to consider the power consumption of all the devices. The devices should be low power and very reliable, while still being capable of connecting to the Internet. To accomplish this, 6LoWPAN was put forward. The details of this are explained in subsequent sections.

7.3 Transport Layer

TCP (Transmission Control Protocol) and UDP (User Diagram Protocol) are the most widely used protocols for transportation.

i. TCP is connection oriented. Once a connection is established, data is transmitted between systems over a network in the form of packets. It includes error checking, guarantees the delivery and preserves the order of the data packets.

ii. UDP is a connectionless protocol. It is faster than TCP. However, it provides only basic error checking support so the delivery of data to the destination can't be guaranteed.

7.4 Application Layer

This is the highest layer of protocol where users are mostly interacting while prototyping an IoT projects. Commonly used protocols are: http, SMTP, MQTT, DNS, DHCP, CoAP etc.

i. **HTTP (Hyper Text Transfer Protocol)** is a simple widely used protocol for IoT devices when there is a lot of data to be published. It uses client/server model. It is not suitable in resource constraint environment because it is extremely heavy-weight and incurs a large parsing overhead.

ii. **MQTT (Message Queuing Telemetry Transport):** It is a light-weight messaging protocol designed for limited network bandwidth. It uses publish/subscribe mechanism for exchanging messages via a message broker. It was developed initially by IBM for M2M communication and is playing a crucial role in the IoT.

iii. **SMQTT (Secure Message Queue Telemetry Transport):** It is an encryption based light weight messaging protocol giving more security.

iv. **CoAP (Constrained Application Protocol):** It is specially designed for limited hardware. The hardware that does not support HTTP can use CoAP protocol. It is a light weight client-server based model and is used for communication between battery powered IoT devices.

v. **DDS (Data Distribution Service):** It is an M2M application layer protocol for real-time systems. Like MQTT, it is based on publish/ subscribe mechanism. It does not require any networking middleware and programming as it does not verify existence or location at the nodes and confirmation of the message delivery.

8. Cross Connectivity across IoT System Components

IoT connectivity is a term defining connection between all the points in the IoT ecosystem. The core modules of IoT ecosystem are:

Sensors, endpoints, analytics, data management, data communication and protocols.

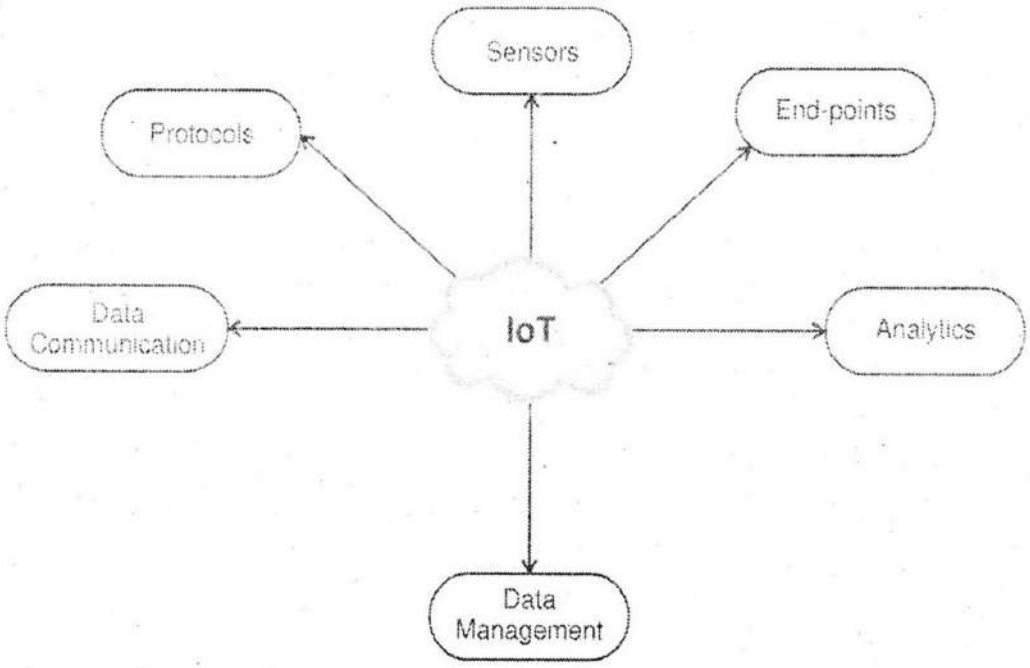


Figure 3.9: Core Model of IoT

IoT platforms operate and provide several data and intelligence features with the help of sensors. **Sensors** collect data and forward it to other IoT modules.

An **endpoint** is a physical device that executes a task or a function as a component of an IoT solution.

Data communication module communicates the data between various devices in IoT. The data is properly managed and analysed by **Data management and analytics module**.

Protocol is one of the important part of IoT system as without these various modules cannot understand each other's language and fail to communicate.

In all these processes, an **IoT gateway** plays a key role. The IoT gateways are programmed hardware devices which form the communication bridge for different technologies. It creates a bridge between the IoT sensors/ actuators and the internet. The IoT gateway aggregates all data, translates sensor's protocols, and pre-process the data before sending it.

An IoT gateway enables IoT communications, usually

i. Device to Gateway

ii. Gateway to Cloud

iii. Device to Cloud

i. **Device to Gateway:** Here application layer gateway is used as a channel between an IoT device and cloud service. In layman terms, it is an application software running on a local gateway device.

   This model is common in many consumer devices/smart gadgets. Most of the time, a smartphone is used as a local gateway. Connection is established by an application running on smartphone. The connection may be established using access point using router, switch or hub. Hub can also be used as a gateway especially in home/office automation system.

ii. **Gateway to Cloud:** This model is used for long range IoT applications. Here dedicated protocols are designed to send small amount of sensor data over a large distance. It uses wired LAN, WAN, cellular network or satellite links to establish faster connectivity between gateway to cloud.

iii. **Device to Cloud:** In this communication model, the IoT device establishes a direct connection with an Internet cloud service. An application software controls the transfer of data. The model uses Wi-Fi and wired Ethernet to connect an IP network with a device after which it finally establishes a connection with the cloud service. In this mode, IoT device must be uniquely identified, located and allocated an IP address. This method is cost effective as compared to the above two.

9. Network Technologies

The situation of network technologies is totally different in IoT network. Most IoT sensors are designed for a single job and they are typically small and inexpensive. This means that they often have limited power, processing capabilities and memory storage. They transmit only when there is something important. Because of the massive scale of these devices and the huge uncontrolled environments where they are usually deployed, the networks that provide connectivity also tend to be very lossy and support very low data rates. To meet the constrained nature of IoT systems, IoT requires a new breed of connectivity technologies that meet both the scale and constraint limitations.

LPLAN, LPWAN are types of wireless telecommunication networks designed to meet the above requirements.

9.1 Low Power Local Area Networking (LPLAN)

This networking is used for smart home/office applications. It's connectivity range as well as number of IoT devices that can be connected are limited. Therefore this is not widely used for IoT networking.

9.2 LPWAN (Low Power Wide Area Network)

The name itself is self-explanatory. It is a new type of technology which is developed in 2013 and is used in many IoT applications. The most prominent features of LPWAN are:

i. LPWAN provides long-range communication.

ii. LPWAN has less bit rate.

iii. LPWAN devices has low power consumption.

iv. LPWAN devices have good battery life as they transmit small packets of data at random intervals.

v. LPWAN offers better connectivity

Because of the above features, many businesses utilize LPWANs to establish their own secure networks and link their IoT devices. *For example,* in application of environment monitoring, many sensors can be deployed to monitor the air quality in an area or water level/purity of a river.

As IoT devices have good battery life, sensors can be deployed in buildings or hard to access areas and left there for a long time to transmit data. LPWAN facilitates a wide area of coverage which is never limited by proximity to the distance among the access points. This power saving translates into lower costs for the end users and companies who are using this technology.

Widely used LPWAN technologies are:

LoRaWAN, Sigfox, NB-IoT, Cat-M1

i. **LoRaWAN:** The LoRaWAN (Long Range WAN) is a low power wide area open access protocol designed for long distance communication. The protocol is defined by the LoRa Alliance. It is a cloud-based MAC layer protocol which manages communication between LPWAN gateways and end-node devices.

LoRaWAN network architecture is deployed in a star-of-stars topology in which gateways pass the messages between end-devices and central network server. LoRa devices define the physical layer and use spread spectrum modulation technique.

LoRaWAN operates in unlicensed ISM band and the band varies from country to country. In India, 865 MHz - 867 MHz band is allocated for LoRaWAN.

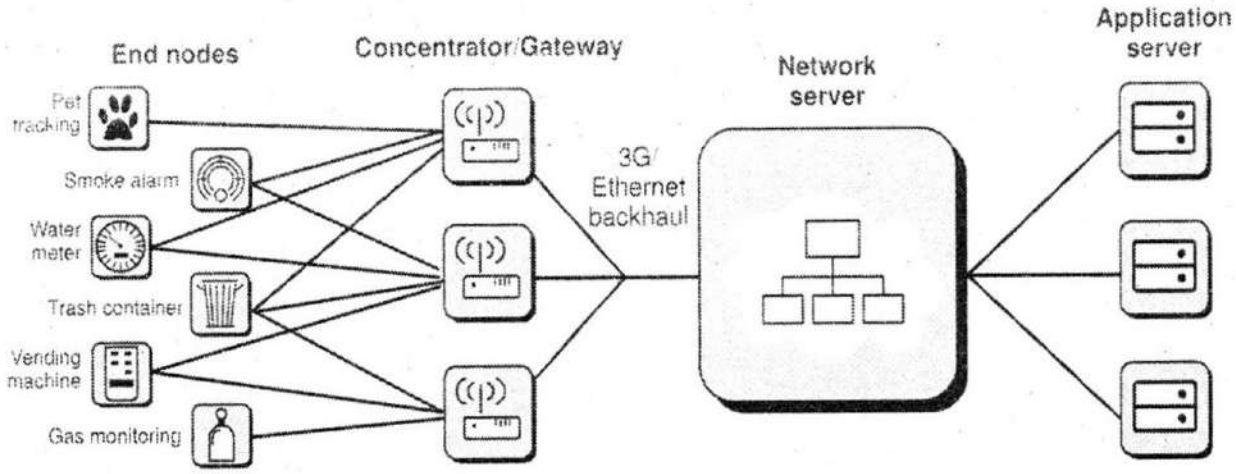


Figure 3.10: LoRaWAN Architecture

- End device, Node, Mote: An object with an embedded low-power communication device.
- Gateway: LoRaWAN nodes are associated with a specific gateway. Data from end devices is transmitted to all gateways and each gateway which receives a signal transmits it to a cloud based network server.
- Network server: Servers that route messages from End devices to the right application, and back.
- Application: A piece of software, running on a server.

ii. **Sigfox:** Sigfox is an LPWAN technology that offers an end-to-end IoT connectivity. Sigfox deploys its proprietary based stations connected to back-end servers. The end devices are connected to base stations using BPSK modulation.

Sigfox uses the frequency bandwidth efficiently and experiences very low noise levels. This ultimately results in low power consumption and high receiver sensitivity.

iii. **NB-IoT:** NB-IoT is a Narrow Band IoT technology released by 3GPP in 2016. It uses licensed frequency bands of 700 MHz, 800 MHz and 900 MHz.

The NB-IoT communication protocol functionalities are enhanced as per requirement of IoT applications. It allows connectivity of upto 100 k end devices per cell which can be expanded by adding more NB-T carriers. It uses FDMA technique and QPSK modulation technique.

NB-IoT devices consume large power as compared to Sigfox and LoRa and reduces NB-IoT end-device life time.

iv. **Cat-M1:** Cat-M1 is LPWAN technology which supports high data rates. It operates at 1.4 MHz bandwidth with higher device complexity/cost than NB-IoT. It uses modulation technique of OFDM. Wider bandwidth allows data rates upto 1Mbps and more accurate device positioning capabilities. It also supports voice calls and mobility of device. So many times wearable devices, smart vehicles, trackers and alarm panels prefer this technology.

9.3 Comparison of LoRaWAN, Sigfox, NB-IoT, Cat-M1

	LoRaWAN	Sigfox	NB-IoT	Cat-M1
i.	Long range	Long range	Short range	Long range
ii.	Low data rates	Moderate data rates	Moderate data rates	High data rates
iii.	Long battery life	Long battery life	Good battery life	Low battery life
iv.	Low cost	Low cost	Low cost	Medium cost
v.	Modulation technique used is chip spread spectrum	Modulation technique is BPSK	Modulation technique is QPSK	Modulation technique is OFDM
vi.	Unlicensed ISM frequency bands are used.	Unlicensed ISM frequency band is used.	Licensed LTE frequency band	Uses LTE specified frequency band
vii.	Connectivity of upto 50 k per cell	Connectivity of upto 50 k per cell	Connectivity of upto 100 k per cell	Connectivity of upto 50 k per cell

The IoT factors and technical differences of LoRaWAN, Sigfox, NB-IoT, Cat-M1 will determine their feasibility for specific applications. One technology cannot serve all IoT applications. One has to select the best fitting technology as per the application under.

Exercises

A. Multiple choice questions

1. IoT stands for?
   a. Introduction of Things
   b. Internet of Things
   c. Internet of Tracking
   d. Interaction of Things

2. The term "Internet of Things" was coined by?
   a. Kevin Ashton
   b. Guido van Rossum
   c. IBM
   d. Ross Ihaka

3. Which of the following is true about IoT?
   a. The term Things in the Internet of Things refers to anything and everything in day to day life.
   b. IoT has greater transparency, control, and performance.
   c. Both a and b
   d. None of the above

4. IoT is an advanced automation and analytics system which deals with?
   a. sensor, networking
   b. electronic
   c. cloud messaging
   d. All of the above

5. Which of the following is not an advantage of IoT?
   a. Improved customer engagement
   b. Security
   c. Reduced waste
   d. Enhanced data collection

6. The number of layers in the IoT Architecture?
   a. 5
   b. 6
   c. 7
   d. 8

7. Scalability of IoT means:
   a. Expandable/reducible in terms of scale or size.
   b. Measurable
   c. Increasing/decreasing monetary costs.
   d. All of these.

8. MQTT stands for:
   a. Message Queue Telemetry Transport
   b. Multiple Queue Telemetry Transport
   c. Multiple Query Transport Technique
   d. Message Query Transport Technique

9. M2M stands for:
   a. MAC to MAC communication
   b. Machine to MAC communication
   c. Machine to machine communication
   d. MAC to machine communication

10. Why is IPv6 preferred over IPv4 for IoT implementations?
   a. Larger addressing range
   b. More security
   c. Both a and b
   d. Neither a or b

11. Which one of these is the most important factor to be considered in an IoT implementation:
   a. Scalability
   b. Power efficiency
   c. Efficient and scalable addressing schemes
   d. All of these

12. Which of these is a part of the Sensing Layer of the IoT Service Oriented Architecture?
   a. Service integration
   b. Data storage
   c. Data sensing and actuation protocols
   d. Data Analytics

13. Gateway provides the connection between _____ and _____.
   a. Cloud and controller
   b. Network and cloud
   c. Network and controller
   d. Controller and device

14. CoAP is specialized in _____
   a. Internet applications
   b. Device applications
   c. Wireless applications
   d. Wired applications

15. Which layer is HTTP?
    a. Control layer
    b. Transport layer
    c. Service layer
    d. Application layer

16. Which is an open standard?
    a. HTTP
    b. CoAP
    c. XMPP
    d. MQTT

17. MQTT is _____ protocol.
    a. Machine to Machine
    b. Internet of Things
    c. Machine to Machine and Internet of Things
    d. Machine Things

18. Which protocol is lightweight?
    a. MQTT
    b. HTTP
    c. CoAP
    d. SPI

19. Which of the company is not a leader in cloud computing?
    a. Google
    b. Amazon
    c. Blackboard
    d. Microsoft

20. Examples of a public cloud include:
    a. Amazon Web Services
    b. Microsoft Azure
    c. Google Cloud Platform
    d. All of the above

21. Who is responsible for security in a public cloud service?
    a. The cloud provider is responsible for data protection
    b. An individual tenant is responsible for data protection
    c. Both the cloud provider and the tenant are responsible for data protection
    d. None of the above

22. Which cloud deployment model is managed by a cloud provider, has an infrastructure that is off site, and is accessible to the general public?
    a. Public cloud
    b. Private cloud
    c. Hybrid cloud
    d. None of the above

23. Which one is not an element of IoT?
    a. People
    b. Process
    c. Cloud
    d. Things

24. Which of the following is not the component of IoT Endpoint
    a. Sensor
    b. Gateway
    c. Communication Module
    d. MCU

25. _____ in IoT as one of the key characteristics, devices have different hardware platforms and networks.
    a. Sensors
    b. Heterogeneity
    c. Security
    d. Connectivity

26. Which of the following is one of the backend's built-in components of cloud computing?
    a. Security
    b. Application
    c. Storage
    d. Service

27. The _____ allows systems and services to be accessible within an organization.
    a. Private cloud
    b. Public cloud
    c. Community cloud
    d. Hybrid cloud

28. Which of the following is a type of Service Models?
    a. Public-as-a-Service
    b. Platform-as-a-Service
    c. Community-as-a-Service
    d. Public-as-a-Service

29. _____ provides the runtime environment for applications, development and deployment tools, etc.
    a. IaaS
    b. PaaS
    c. SaaS
    d. XaaS

30. Which of the following is the most complete cloud computing service model?
    a. PaaS
    b. IaaS
    c. CaaS
    d. SaaS

31. Which of the following is best known service model?
    a. PaaS
    b. IaaS
    c. SaaS
    d. all of the mentioned

32. _____provides virtual machines, virtual storage, virtual infrastructure, and other hardware assets.
    a. PaaS
    b. IaaS
    c. SaaS
    d. all of the mentioned

33. Which cloud is deployed when there is a budget constraints but business autonomy is most essential?
    a. Private cloud
    b. Public cloud
    c. Community cloud
    d. Hybrid cloud

34. _____cloud is one where the cloud has been organized to serve a common function or purpose by many organizations.
    a. Private cloud
    b. Public cloud
    c. Community cloud
    d. Hybrid cloud

35. Which is not a characteristic of SaaS?
    a. Multi device Support
    b. Web access
    c. One to many
    d. Offline Access

36. Which of the following is not the part of basic services offered by cloud.
    a. PaaS
    b. SaaS
    c. IaaS
    d. LaaS

B. Answer in one or two lines

1. What is IoT?
2. Define M2M.
3. Name communication protocol used in M2M.
4. Compare M2M and IoT with respect to any two points.
5. Which are different cloud topologies?
6. Define following:
    a. Private cloud
    b. Public cloud
    c. Hybrid cloud
7. State the need of cloud in IoT.
8. Name the seven layers of IoT architecture.

9. State any two features of private cloud.
10. State any two features of public cloud.
11. State how hybrid cloud is better than public and private cloud.
12. Name three key services in the cloud.
13. What is IaaS?
14. What is PaaS?
15. What is Saas?
15. State following clouds are of which type?
    a. Heroku
    b. Windows Azure
    c. Microsoft office
16. Name the protocols used in link layer of IoT layers.
17. Name the protocols used in link layer of IoT layers
18. What is bit length of IP address in IP.
19. What is long form of SMQTT, COAP, HTTP, DDS.
20. Define 'Things' in case of IoT.
21. What is requirement of network technology in IoT?
22. State four important features of LPWAN.
23. What is the frequency band of LoRaWAN?
24. What is Sigfox technology?
25. Give any one advantage of NB-IoT and Cat –M1 network technology.

C. Answer in detail

1. Write a note on evolution of IoT.
2. Describe M2M architecture.
3. Differentiate between M2M and IoT.
4. Describe seven layer of IoT architecture.
5. What is the role of edge computing layer in IoT architecture?
6. Explain role of cloud in IoT.

7. Describe following cloud topologies:
   a. Public cloud b. Private cloud c. Hybrid cloud
8. Explain features of public cloud.
9. Explain three services models of cloud access:
   a. Infrastructure as a Service (IaaS)
   b. Platform as a Service (PaaS)
   c. Software as a Service (SaaS)
10. Explain physical and Link layer protocol used in IoT.
11. Explain in detail Transport layer protocol of IoT.
12. Explain following IoT gateways.
    a. Device to Gateway b. Gateway to Cloud c. Device to Cloud
13. What is LPWAN technology?
14. Describe LoRaWAN.
15. Write note on Sigfox.
16. Describe NB-IoT and cat-M1.
17. Compare LoRaWAN, Sigfox, NB-IoT and Cat-M1 technologies.

Answers

1.	b	2.	a	3.	c	4.	d	5.	b
6.	c	7.	d	8.	a	9.	c	10.	c
11.	d	12.	c	13.	a	14.	a	15.	d
16.	b	17.	c	18.	a	19.	c	20.	d
21.	c	22.	a	23.	a	24.	b	25.	b
26.	a	27.	a	28.	b	29.	b	30.	d
31.	d	32.	b	33.	a	34.	b	35.	d
36.	d								

Unit 4

IoT Applications

1. Application Domains of IoT

The number of IoT devices and systems has been increasing all over the world. The range of IoT application domain is wide and encapsulates applications from home automation to more sophisticated environments, such as smart cities, manufacturing, supply chain, healthcare, education, retail, government and so on.

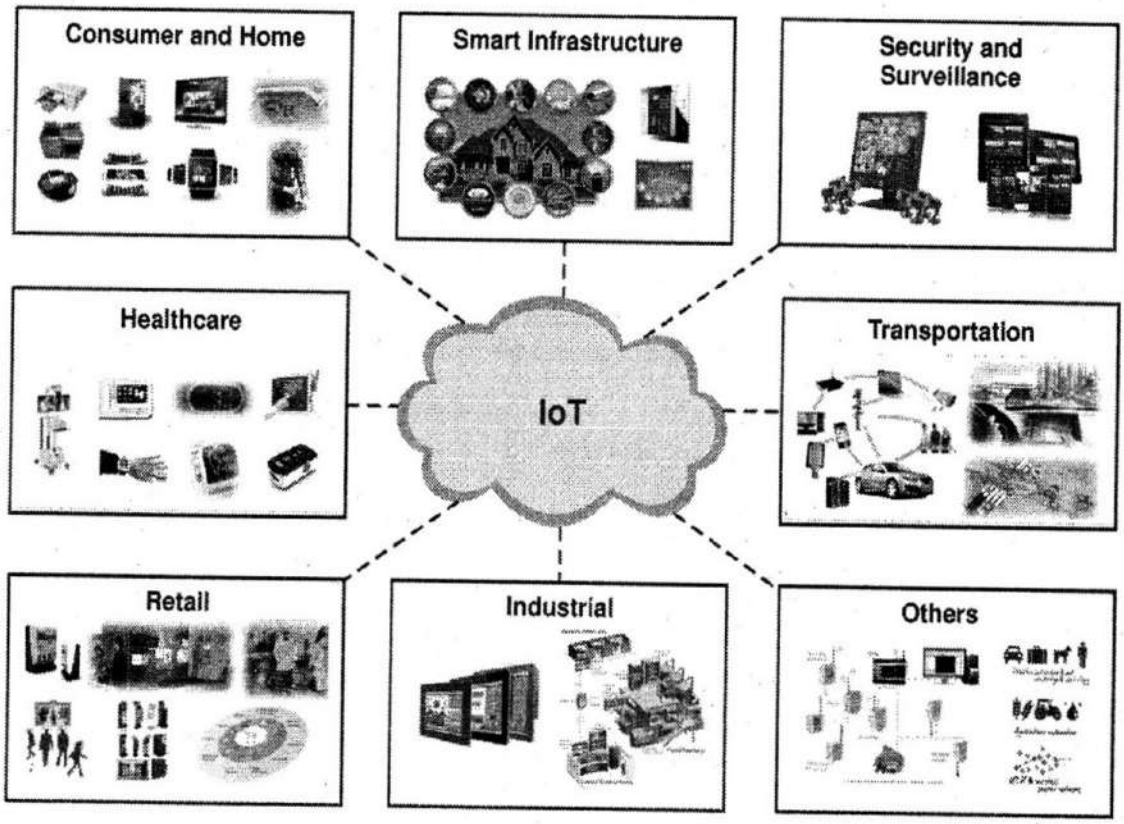


Figure 4.1: Day-to-day applications of IoT

Major application areas are categorized for your reference and are explained:

i. **Manufacturing and Logistic:** Using IoT systems, the retailer can optimize activities like automation in checking, real time stock monitoring and detection of expired stock. On demand information regarding goods can optimize the logistics of whole supply chain. Applications also include authentication of goods, anti-counterfeiting, inventory management service and support.

ii. **Smart Transportation:** Use of sensor network, GPS and wireless network are making vehicles and transportation system smart, safe and efficient. Vehicle tracking, traffic data collection for management, traffic rule enforcement systems, are going to be a part of an integrated network. Another emerging application is real time traffic monitoring using video sensors and it's use for traffic forecasting.

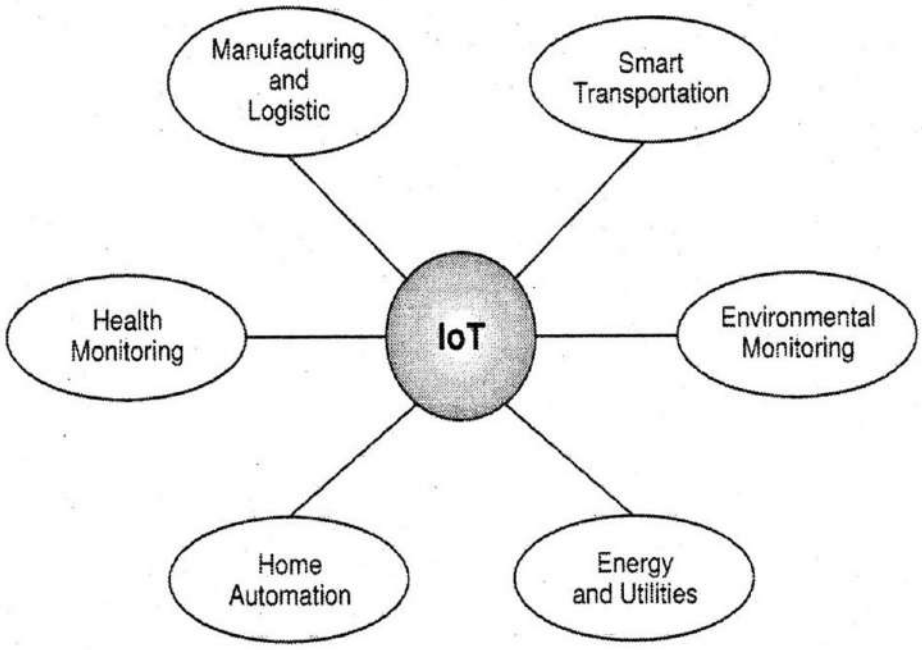


Figure 4.2: Application domains of IoT

iii. **Environmental Monitoring:** Weather forecasting and environmental monitoring is very important and valuable application of IoT. It is used to protect environment by monitoring air or water quality, atmospheric or soil conditions. It can even include areas like monitoring the movements of wildlife and their habitats. Development of IoT systems can also be used for early warning systems for tsunami or earthquake and used by emergency services to provide effective aid.

iv. **Energy and Utilities:** Smart electricity grid, water transmission grid, real time monitoring of water supply and electricity usage are some of the applications of IoT in this domain.

v. **Home Automation:** IoT home automation is slowly but steadily becoming a part of daily lives in the world. These days, there is a vast range of devices powered by IoT. These include thermostats, refrigerators, security systems and even dryers and kettles. All these things have sensors for data collection. The data is then used for monitoring, controlling and transferring information to other devices via the internet. This allows specific actions to be automatically activated whenever certain situation arises. In a simple *example*, consider a smart kettle. The kettle can be programmed to automatically turn off once it reaches a specific temperature. It might also send a notification to the user on the same.

vi. **Health Monitoring:** IoT has enabled tele-monitoring of the health conditions of a person especially the old age patients and informing doctors/relatives in case of emergency. One can have access to electronically stored patient records and medical history from anywhere.

The use of smart technology in healthcare has been advancing steadily with the invention of smart insulin pens, internet connected inhalers, asthma monitors, wearable devices like biosensors and smart watches. Use of such gadgets allows user to better manage and address their own health needs as well as to quickly access help if something goes wrong.

2. Challenges in IoT

The world is witnessing massive growth of IoT application. It is predicted that by 2025 there will be 79 Zettabyte IoT devices (one Zettabyte = one trillion Gigabytes). This has put up many challenges in front of IoT system researchers and developers. The major challenges are figured out in the diagram.

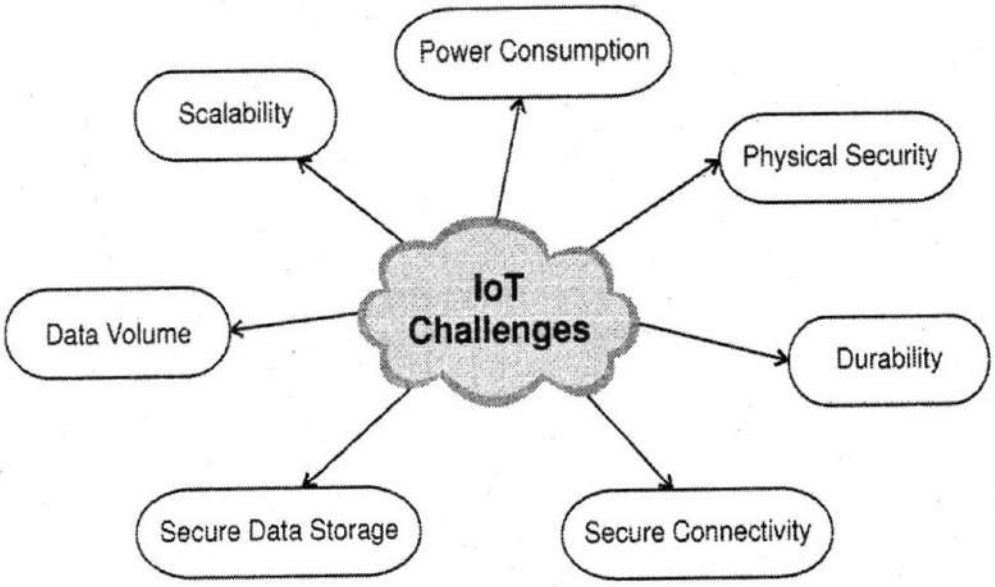


Figure 4.3: Challenges of IoT

i. **Power consumption:** All the IoT devices need power in order to work. Increasing number of IoT devices demands more power. Currently devices are using external sources like batteries, which do not have a long life and are not economical. This adds some functional

challenges as power sources need to be replenished. Replacements of batteries or rechargeable batteries are not feasible options. Also accessing continuous power from the power grid is not always possible.

There are two primary ways to avoid IoT power consumption issues:

a. Energy - harvesting technique, which captures energy from a device's surrounding environment.

b. Reduction in power use by implementing protocols that conserve power. Three *examples* of low-power consumption techniques are: the use of power saving mode, employing Extended Discontinuous Reception protocols and wake-up signals.

ii. **Physical security:** Security is one of the most important concern in IoT. Since billions of devices are connecting to each other and transferring a large amount of data, security becomes the biggest concern. The security challenges are related to security services like authentication, privacy, confidentiality and end-to-end security.

Main problem is any IoT device could be a possible attack target. Some devices are located in untrusted areas and attackers can gain physical access to them and even get control of the device.

iii. **Durability:** Durability is related with the ability of a system to work within specified limits without any maintenance. IoT system includes many "Things", sensors controllers, actuator and communication networking devices. All these components have aging, overheating effects or connection establishment issues. The IoT devices must sustain mechanical shocks, vibrations or environment condition.

Thus, overall durability of IoT system is dependent on durability of each and every component of the system.

iv. **Secure connectivity:** There is no standard platform and common architecture available for IoT applications. Because of lack of open collaborative platform for all the manufacturers, devices face problem of connectivity. IoT implementations are taking place in fragments. There are millions of connected devices and billions of sensors and their number is continuously increasing. All of them need secure and reliable connectivity.

v. **Secure data storage:** Data storage security involves protecting storage resources and the data stored on them - both on premises and in external data centers and cloud. IoT data is mostly unstructured and so can easily be stored in public cloud infrastructure. Al the

major cloud providers offer low-cost scalable storage systems based on object storage technology.

vi. **Data volume:** With the increase in density in IoT devices and the rapid increase in daily generation of the huge volume of data, the data volume became a problem in IoT. The statistics shows the overall data volume of connected IoT devices / connections over the years. The growth is exponential; it is because in almost all IoT applications, real-time data is generated from sensors surveillance cameras, drones, personal devices, gateways etc.

On this background, data management of IoT is gaining importance and researchers are focusing on finding solutions for tackling 'Big Data' generated. Data authentication, security and confidentiality also need to be taken care.

vii. **Scalability:** This is an upcoming challenge for major IoT implementations. A lot of data is getting generated through this connected architecture, which adds pressure on bandwidth. Hence, scalability becomes an issue where the network has to extend as we add more devices to it.

Secondly, scalability is limited by availability of hardware components as well. Main issue is with sensors used for IoT applications. Though many types of sensors are available in market, one has to think about durability, power requirement, robustness, sustainability of these when they are deployed as IoT devices.

One has to consider communication means (wire or wireless) and protocols (Bluetooth, ZigBee, RFID, Wi-Fi etc.). The IoT system is highly distributed, heterogeneous and pervasive. Dealing with such type of system, scalability is an important point in designing a secure and reliable IoT system.

3. Case Studies

In third chapter, we got familiar with IoT architecture and network technologies. In the first section of this chapter, we have seen various application domains of IoT. Now in this section, we will study three cases of IoT applications in different domains.

3.1 Case Study 1: Smart Irrigation System for Agricultural Field

IoT is nowadays widely used in agricultural domain for irrigation system or for green house control. Use of IoT in irrigation system optimizes the water and energy resources thus making system more efficient and cost effective.

Objectives

i. To design a smart irrigation system using IoT devices and soil moisture sensors.

ii. To determine the amount of moisture in the soil.

iii. If moisture level goes below a predefined threshold, release the flow of water through the irrigation pipes.

iv. To collect data of moisture levels in the cloud where it is analyzed to plan watering schedules.

System Architecture

To accomplish the above objectives, the system architecture has been designed. Basically moisture level of soil is measured at different locations and is used as input to the system. This input is compared with predefined threshold level required by field. It depends upon crop type, soil texture and growth status of crop. The switching of the water pumps is controlled remotely after processing of real time acquired data and predefined threshold level.

For simplicity, it is divided into four broad categories:

i. Data collection of soil / environment parameters

ii. Data transmission

iii. Data processing and intelligence

iv. Enabling of water pumps

Following figure shows block diagram, of IoT based Irrigation System:

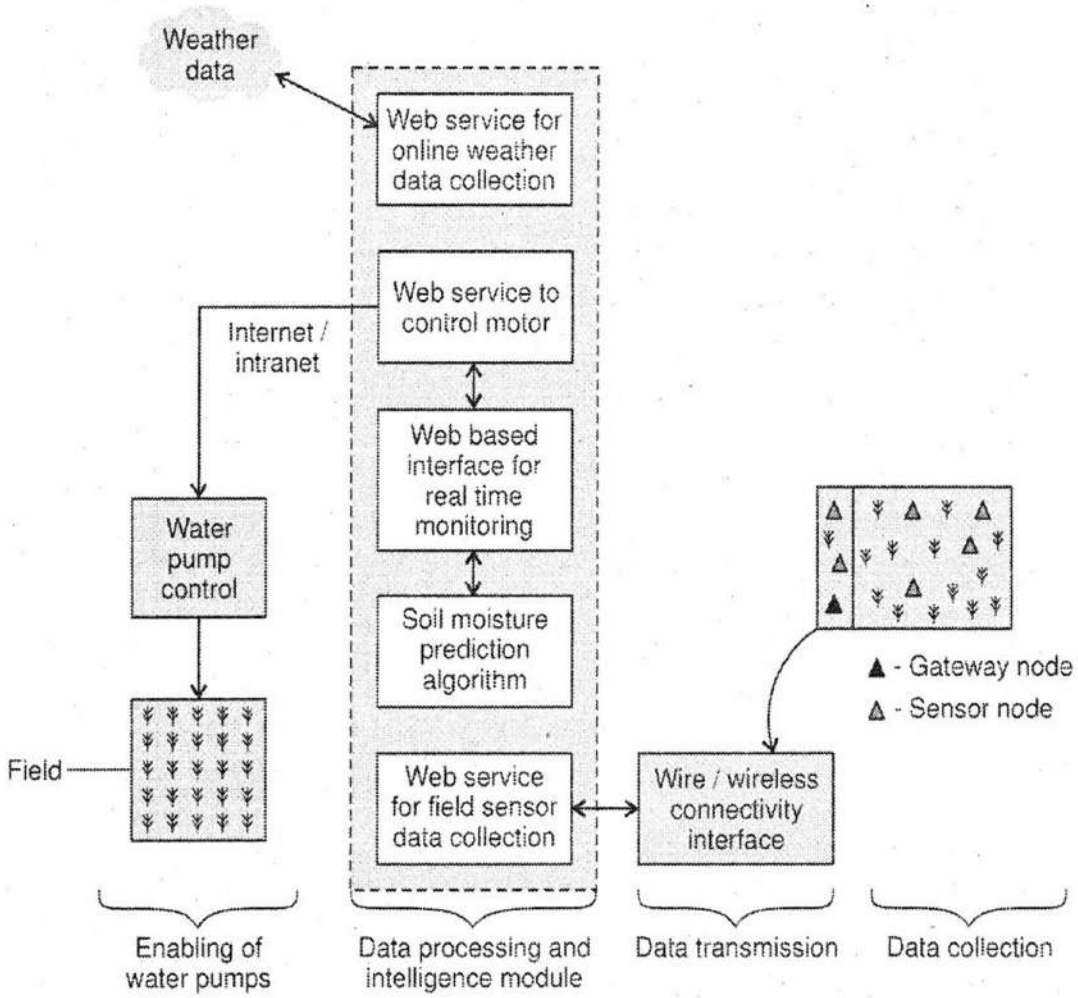


Figure 4.4: Smart irrigation architecture

The working of the system is as below:

i. **Data collection of soil parameters:** For irrigation system, we are interested in knowing soil moisture, air temperature and humidity in air. For sensing these parameters, we will require moisture, temperature and humidity sensors. For detection of moisture level of the field, only one sensor will not be sufficient. Many moisture sensors need to be deployed at different locations for monitoring soil moisture level. Number of sensors required and their location is dependent on the area of field and soil morphology. These IoT devices form a wireless sensor network and transmit data to network. For this low power ZigBee, Wi-Fi modules can be used.

ii. **Data transmission:** Real-time captured data of WSN is transmitted to server using suitable wireless protocol.

iii. **Data processing and intelligence:** This unit processes WSN data. It also collects weather forecasting data like cloudiness, UV index and precipitation. Algorithms like vector regression model and k-means clusting etc. are used to predict irrigation schedule based on captured level of soil moisture and predicted precipitation to save water and energy.

iv. **Enabling of water pumps:** A water pump is connected to a relay switch that is controlled by a Wi-Fi enabled node. The node is controlled by the web service through a trigger generated by data processing and intelligence unit. Thus, water pumps are managed remotely using web based interface.

Advantages of IoT based Smart Irrigation System

i. Avoids excessive use of water in irrigation

ii. Avoids under irrigation

iii. Automated control of irrigation system increases crop yield

3.2 Case Study 2: Home Automation

Once a dream, smart homes are slowly and steadily becoming a part of daily uses around the world. These days, most smart IoT home automation devices allow you to control them via an app or even via voice commands.

Most of the home automation includes:

i. Smart lighting

ii. Smart appliances

iii. Intrusion detection

iv. Smoke / gas detectors

In all the above applications, the related real-time data is collected from things using sensors. The data is then used for monitoring, controlling and transferring information to other devices via the internet. This allows specific actions to be automatically activated whenever certain situation arises. In a simple *example*, consider a smart kettle. The kettle can be programmed to automatically turn off once it reaches a specific temperature. It might also send a notification to the user on the same.

The same concept can be applied to all the devices present in the home to make them smart IoT device.

i. **Smart lighting:** Smart lighting in home saves a lot of energy. It is because system is designed such that depending upon ambient light and occupancy in the room, lights are either switched off or dimmed. Smart lighting uses solid state lighting and IP enabled lights. Wireless enabled and internet connected lights can be controlled remotely using IoT architecture. Smart lights with sensors for occupancy, temperature, required lux level, ambient light etc. can be configured to change the light intensity/colour.

ii. **Smart appliances:** Modern homes have a number of appliances such as TVs, refrigerators, music systems, washing machines, dishwashers; oven etc. Managing and controlling these appliances can be tedious with each appliance having its own control or remote controls.

Smart appliances make the management easier and also provide status information to the users remotely. *For example*, smart washers/dryers that can be controlled remotely and notify when the washing/drying cycle is completed. Smart thermostats allow controlling the temperature remotely and can learn the user preference. Smart refrigerators can keep a track of the items stored using RFID tags and send updates to the users when an item is low on stock. The order may be placed automatically to the shopkeeper. Smart TVs allow users to search and stream videos and movies from the internet on a local storage drive, search TV channel schedules and fetch news, weather updates and other content from the internet.

iii. **Intrusion detection:** Home intrusion detection systems use security cameras and PIR/door sensors to detect instructions and raise alerts. Alerts can be in the form of SMS or email sent to the user. Advanced system can even grab the image or a short video of the intruder and sent as email attachment. A cloud controlled intrusion detection system uses location aware devices, where the geo-location of each node of a home automation system is independently detected and stored in the cloud.

iv. **Smoke / gas detectors:** Smoke detectors are installed in homes and buildings to detect smoke that is typically an early sign of fire. Smoke detectors use optical detection, ionization or air sampling techniques to detect smoke. Alerts raised by smoke detectors can be in the form of signals to a fire alarm system. Gas detectors can detect the presence of harmful gases such as Carbon Monoxide (CO), Liquid Petroleum Gas (LPG) etc.

A smart smoke/gas detector can raise alerts describing where the problem is, send an SMS or email to the user or the local fire safety department and provide visual feedback of its status (healthy, battery low etc.).

In all the above mentioned applications, the system architecture is as shown in *figure 4.5s*. The sensors will change according to "Thing" and application.

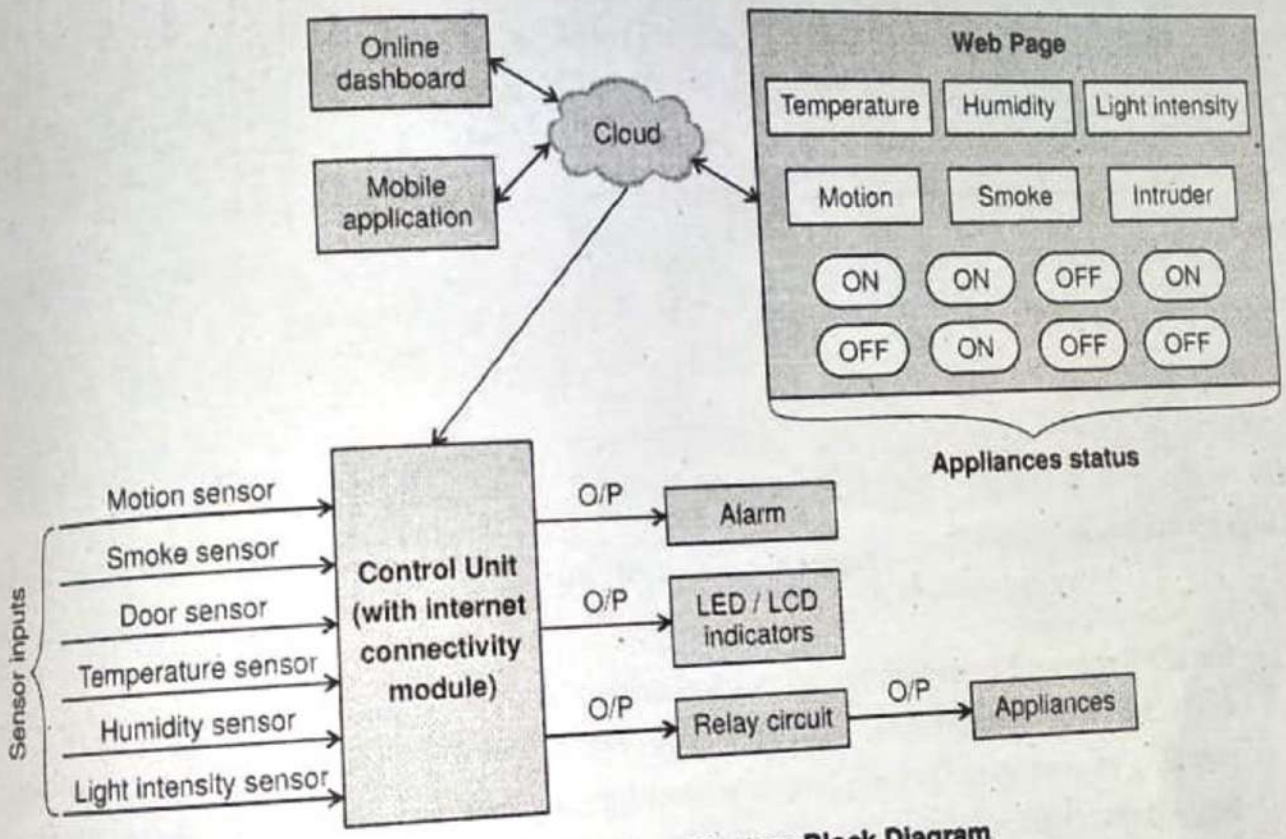


Figure 4.5: Smart Home System Block Diagram

3.3 Case Study 3: Smart Cities

IoT based smart cities help to develop, deploy and promote sustainable development practices to address growing urbanization challenges. Cloud-based IoT applications receive, analyze and manage data in real-time to help municipalities, enterprises and citizens to make better decisions so as to improve quality of life. Following are the remarkable advantages of IoT based smart city:

i. Improved energy distribution

ii. Streamlined trash collection

iii. Decreased traffic congestion

iv. Improved air quality

v. Conserved energy

The systems required to achieve the above advantages are described in subsequent paragraphs.

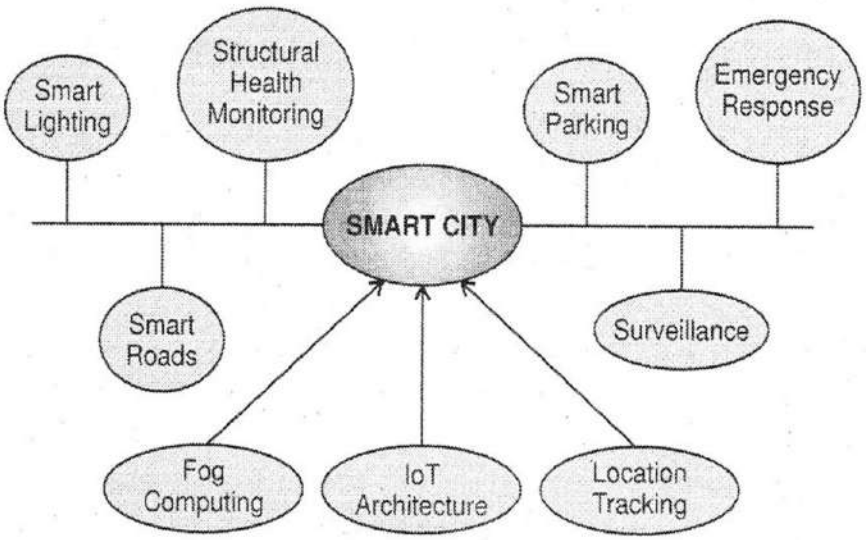


Figure 4.6: Smart city domains

i. **Smart lighting:** Smart lighting allows lighting to be dynamically controlled and adaptive to the ambient conditions. Smart lights are connected to the internet. They are controlled remotely to configure lighting schedules and lighting intensity. These are set considering foggy days, cloudy days, festival days etc. Such type of smart lighting systems for roads, parks and buildings saves lot of electricity.

ii. **Smart roads:** Smart roads equipped with sensors can provide information on driving conditions, travel time estimates and alerts drivers in case of worst driving conditions, traffic congestions and accidents. Such systems helps in making the driving safe and help in reducing traffic jams. Information sensed from the roads is communicated via internet to cloud-based applications and social media. The system provides the drivers and passengers with a consistent view of the road situation a few hundred meters ahead of them, so that they can react to potential dangers early enough.

iii. **Structural health monitoring:** Structural health monitoring systems use a network of sensors to monitor the vibration levels in the structures such as bridges, dams, buildings, towers etc. The data collected from these sensors is analyzed to assess the health of the

structures. It can detect cracks, mechanical breakdowns, damages to a structure and estimated life span of structure. In case of intimation of structure failure, advance warnings can be given and corrective action in this regard can save structure from damaging as well as can avoid disaster situation.

iv. **Smart parking:** Finding a parking space during rush hours in crowded cities is critical and time consuming. Smart parking makes the search for parking spaces easier and convenient for drivers. IoT based smart parking system detects the number and location of empty parking slots and sends the information over the internet. The smart parking applications can be accessed by the drivers from smart phones, tablets and in-car navigation systems.

v. **Surveillance:** Surveillance of infrastructure, public transport and events in cities is required to ensure safety and security. IoT based surveillance infrastructure system capture videos using camera for further analysis.

vi. **Emergency response:** IoT systems can be used for monitoring the critical infrastructure in cities such as buildings, gas and water pipelines, public transport and power sub-stations. IoT systems for fire detection, gas and water leakage detection helps in generating alerts and minimizing their effects on the critical infrastructure.

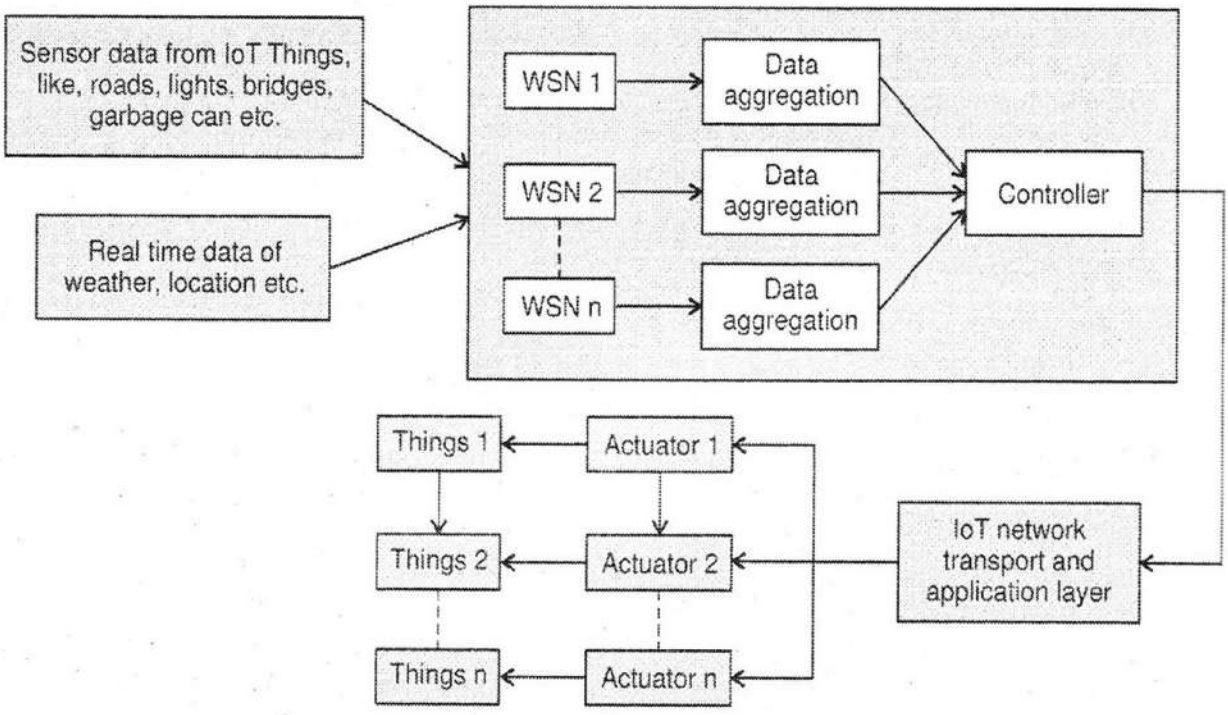


Figure 4.7: Smart city architectural model

Exercises

A. Multiple choice questions

1. Which challenges should be considered in IoT?
   a. Privacy and security
   b. Power consumption
   c. Network congestion
   d. all of the above

2. _____ empowers IoT by bringing together everyday objects.
   a. Intelligence
   b. Connectivity
   c. Dynamic nature
   d. Enormous scale

3. _____ Provide the means to create capability that reflects true awareness of the physical world and people.
   a. Sensors
   b. Heterogeneity
   c. Security
   d. Connectivity

4. IoT devices are naturally vulnerable to _____ threats.
   a. Sensors
   b. Heterogeneity
   c. Security
   d. Connectivity

5. Which challenge comes under securing the information?
   a. Signaling
   b. Security
   c. Presence detection
   d. Power consumption

6. Which is most important challenge when we use many devices on the same network?
   a. Signaling
   b. Security
   c. Presence detection
   d. Power consumption

7. Which of the following issues are considered in IoT?
   a. Security issue
   b. Reliability issue
   c. Scalability issue
   d. All issues

8. Process of identifying any individual
   a. Auditing
   b. Authorisation
   c. Authentication
   d. Accounting

9. Scalability of IoT means
   a. Expandable/reducible in terms of scale or size.
   b. Measurable
   c. Increasing/decreasing monetary costs
   d. All of these

10. Which one of these is the most important factor to be considered in an IoT implementation
    a. Scalability
    b. Power efficiency
    c. Efficient and scalable addressing schemes
    d. All of these

11. IoT devices must have
    a. A USB port
    b. A unique identification
    c. Wired connectivity
    d. All of the above

12. Why data volume is a problem in IoT-based cloud computing?
    a. because data are encrypted and hard to analyze.
    b. because data coming from IoT devices are always in raw format and difficult to store.
    c. because the density of IoT devices is increasing each day and in turn the volume of generated data is growing very fast.
    d. because IoT device density is decreasing each day and in turn the volume of generated data are decreasing very fast.

13. Which of these can be considered as the skeleton for smart cities?
    a. Buildings
    b. Rivers
    c. Banks
    d. Sensors

14. Which of these can be considered as the sensors of smart cities?
    a. Light intensity sensors
    b. Motion sensors
    c. Optocoupler
    d. None of the above

15. Smart Agriculture incorporates:
    a. Alert generation in case of above-threshold pollutants in the air or water
    b. Scheduling harvesting and controlling water pumps
    c. Controlling On/OFF of field lighting
    d. None of these

16. Heterogeneity for IoT in smart cities stands for
    a. Integration of varying hardware platforms and specifications
    b. Integration of different radio specifications
    c. Integration of various software platforms
    d. All of these

17. Which of these sensors can be most appropriately used for activity monitoring in wearables?
    a. Accelerometer
    b. Cameras
    c. LIDARs
    d. LED

18. Which of the following sensors are used in smart home for detection of intruder
    i. Light sensor ii. Motion sensor iii. Camera
    iv. Temperature sensor v. Gas sensor
    a. i, ii, iv
    b. ii, iii
    c. i,ii,v
    d. all of the above

19. Which sensors are used in Smart Irrigation system
    a. Humidity sensor
    b. Temperature sensor
    c. Both can be used
    d. None of above

20. Smart city can monitor
    a. Public transport
    b. Water leakages
    c. Gas levels in atmosphere
    d. all of the above

B. Answer in one or two lines

1. List any four major application areas of IoT.
2. What is use of IoT in environmental monitoring?
3. What is role of IoT in manufacturing and logistic?
4. List any two IoT based gadgets used for health monitoring.
5. List down any four challenges of IoT.
6. Which factors affected durability of IoT system?
7. Define scalability of IoT system.
8. Which parameter of irrigation system can be controlled in smart irrigation system.
9. List the sensors used in smart irrigation system.
10. What are advantages of smart irrigation system?
11. What is meaning of 'Smart Lighting' in smart home?

12. Name few smart appliances at home with their smart function.
13. What is intrusion detection system?
14. Which gas can be detected by smoke/ gas detector system of smart home.
15. Name the sensor are used for smart home system.
16. What are advantages of IoT based smart city?
17. Define smart roads.
18. How smart lighting in smart cities can save electricity.
19. 'Smart parking' system helps drivers and saves their time- comment.
20. Name IoT 'Things' of smart city.

C. Answer in detail

1. Explain application domains of IoT.
2. How IoT can be used in medical field?
3. How power consumption becomes important in IoT?
4. Why data volume generated in IoT applications becomes a challenge for designers and how it is taken care of?
5. Write note on secure connectivity and secure data storage in IoT.
6. Draw and explain smart irrigation system for agricultural field.
7. Which parameter are controlled in smart home system?
8. Draw and explain architecture of smart home system.
9. Which smart applications are normally considered in smart city?
10. Draw and explain architecture of smart city.
11. What are advantages of smart city using IoT?
12. What is meaning of structural health monitoring in smart city and how it is useful?

Answers

1.	d	2.	b	3.	a	4.	c	5.	b
6.	d	7.	d	8.	c	9.	d	10.	d
11.	b	12.	c	13.	a	14.	a	15.	b
16.	d	17.	a	18.	b	19.	c	20.	d

VISION

About Author

Dr. Mrs. Deepa Ramane has an excellent combination of academic expertise, teaching and research experience and practical skills. She completed her Doctorate in Electronic Science from University of Pune. She is gold medalist at M.Sc. and third rank holder at B.Sc. of same University. After working in an Electronics Industry for initial three years as R&D engineer, due to passion for teaching, she switched to teaching career in 1995 by joining Dr. D.Y. Patil Institute, Pimpri, Pune. At Dr. D.Y Patil Arts, Commerce and Science College, she worked as HoD, Electronics department and shouldered many other academic, administrative and research related responsibilities. In 2014, she switched over to Sinhgad College of Science, Pune and is working as IQAC Coordinator and Head of Physics and Electronics department. She is BOS member of Electronics Science of Savitribai Phule Pune University and also of S.P.College, Pune. She is actively participating in design, implementation and evaluation of curriculum of Electronics.

She has more than 30 research papers in International journals and conferences at her credit. She is author of 20 academic books on Electronics subject. (1 international, 4 national and 15 district level). She has organised more than 40 conferences/workshops/seminars. She has delivered many guest lectures at various conferences, competitions and seminars.

She is recognized Ph.D. and M.Phil. guide for SPPU. Her expertise is in Instrumentation System, Embedded System, Communication, Wireless Sensor Networks and Internet of things (IoT).

S.Y. B.Sc. (Computer Science) Sem-IV

- Data Structures and Algorithms-II
- Computer Networks-I
- Embedded System Design
- Wireless Communication and Internet of Things
- Computational Geometry
- Operations Research

www.visionpune.com

Innovation Throughout
VISION PUBLICATIONS
www.visionpune.com
visionpublications@gmail.com

Review us on
/visionpune
YouTube

ISBN: 978-93-90646-11-1
9 789390 646111

₹160/-