3.1 OVERVIEW OF TDMA (TIME DIVISION MULTIPLE ACCESS)

- Multiple access technologies are used to support multiple users to share same radio spectrum.
- Sharing of the radio spectrum can be done in three ways, i.e. by sharing frequency, by sharing time or by allocating different codes to the users. Accordingly three different basic types of multiple access techniques are categorised.
- They are FDMA (Frequency Division Multiple Access), TDMA (Time Division Multiple Access), and CDMA (Code Division Multiple Access).
- The main requirement of the this sharing techniques is that it should not affect the quality of the signal.
- With the use of multiple access techniques efficient utilization of spectrum is possible, also capacity of the system is increased.
- These techniques are grouped into narrowband and wideband systems depending on the bandwidth allocation to users.

3.2 DUPLEXING

- **Definition :** Sending and receiving data to and from Base station is done using two separate channels. One for uplinking and one for down-linking data from BS. This process is known as **duplexing**.
- Two types of duplexing :

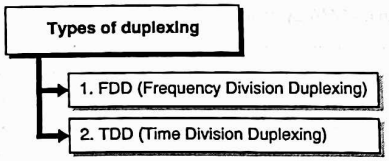


Fig. 3.2.1 : Types of duplexing

3.2.1 FDD (Frequency Division Duplexing)

Refer Fig. 3.2.2 of FDD scheme.

- Each user is allocated two different frequency carriers. One for forward (downlink : from BS to MS) and one for reverse (uplink : from MS to BS) communication links.

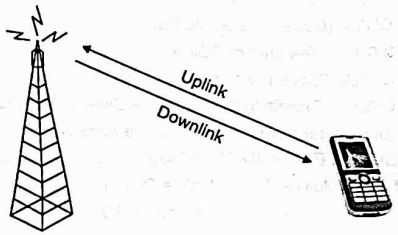


Fig. 3.2.2 : Frequency Division Duplexing

- Each duplex pair consists of two simplex channels.
- Duplexer is needed in MS and BS.
- Spacing between the uplink and downlink frequencies is kept constant throughout the system.

3.2.2 TDD (Time Division Duplexing)

Refer Fig. 3.2.3 of TDD scheme.

- Time is used instead of frequency for uplink and downlink of the data to and from BS and MS.
- Multiple users can share the same frequency channel by using different time slots.
- Each duplex channel is provided with different time slot for uplink and downlink.

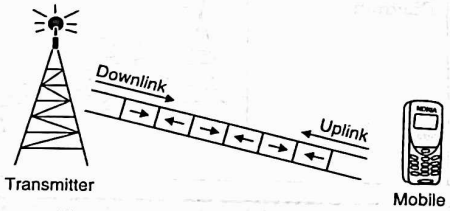


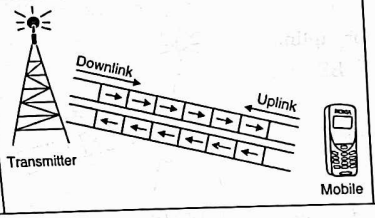
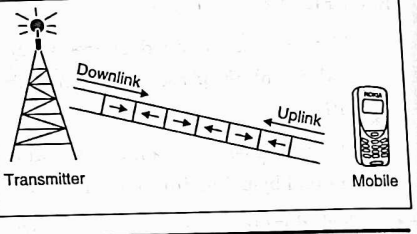
Fig. 3.2.3 : Time Division Duplexing

- Duplexer is not necessary but precise synchronisation is important in this scheme.
- Time latency is major issue hence it is more suitable for fixed wireless access systems when all the users are stationary as there is no change in the propagation delays among the users.

3.2.3 Comparison of FDD and TDD

Table 3.2.1 : Comparison of FDD and TDD

Sr. No.	Parameter	FDD	TDD
1	Working principle	Duplexing by allocation of two separate simplex channels for uplink and downlink between BS and MS.	Duplexing by sharing the frequency carrier and allocation of time slots for uplink and downlink between BS and MS.
2	Implementation	Easy	Complex
3	Need of duplexer in BS and MS	Required.	Not required.
4	Guard space between carriers	Required.	Not required as single carrier is shared.
5	Advantages	Easy to implement. Time latency is less. Simultaneous transmission and reception by transceivers. Synchronisation is not needed.	Efficient utilization of spectrum as single carrier is required. Duplexers are not needed.
6	Disadvantages	Wastage of bandwidth Use of duplexer makes the hardware complex.	Time latency is more. Synchronisation is needed. Simultaneous uplink and downlink is not possible.
7	Applications	Radio communication.	Cordless phones, short range portable access devices.

Sr. No.	Parameter	FDD	TDD
8	Diagram		

3.3 TYPES OF MULTIPLE ACCESS SCHEMES

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

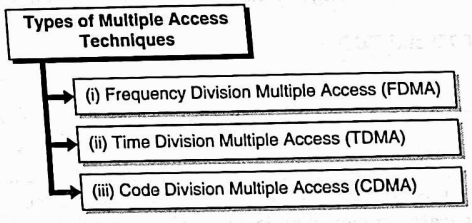


Fig. 3.3.1 : Types of multiple access techniques

(i) Frequency Division Multiple Access (FDMA)

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

(ii) Time Division Multiple Access (TDMA)

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

(iii) Code Division Multiple Access (CDMA)

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

3.3.1 Types of Multiple Access Depending on the Bandwidth Available

Depending on the bandwidth that is available to allocate to the users, the multiple access systems are grouped as:

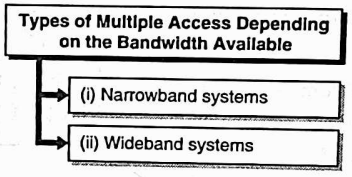


Fig. 3.3.2 : Types of Multiple Access Depending on the Bandwidth Available

(i) Narrowband systems

- In these systems, the available radio spectrum is divided into a large number of narrowband channels. These channels are working with the help of FDD.
- The frequency separation is increased to minimize the interference between the forward and reverse links on each channel. However, duplexers and a common transceiver antenna are to be installed in each subscriber unit.
- In **narrowband FDMA** a user is allocated a specific channel that is not shared by other users in observation. If FDD is used then the system is called as FDMA/FDD.
- In **narrowband TDMA**, a user shares the same radio channel but allocates a unique time slot to each user on the channel.
- A small number of users are separated in time on a single channel.
- The radio channels can be allocated using TDD or FDD while each channel is shared using TDMA. Such systems are called TDMA/FDD or TDMA/TDD access systems.

(ii) Wideband systems

- In these systems, the transmission bandwidth of a single channel is larger than the coherence bandwidth of the channel. So, multipath fading will not vary the received signal power. The frequency selective fades occur in a small part of the signal bandwidth at any instant of time.
- In these systems there are a large number of transmitters that transmit on the same channel.
- If TDMA is used then only one transmitter can access the channel at any instant of time. They can use FDD or TDD.
- If CDMA is used it allows all the transmitters to access the channel simultaneously. The systems can use FDD or TDD multiplexing techniques.

3.4 FREQUENCY DIVISION MULTIPLE ACCESS (FDMA)

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

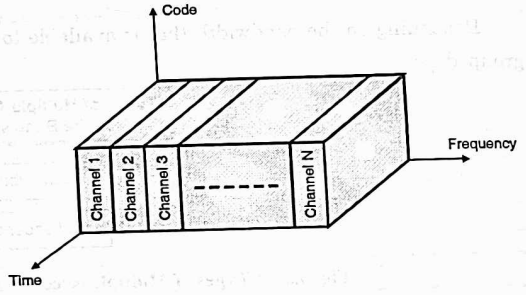


Fig. 3.4.1 : FDMA where different channels are assigned different frequency bands

- When a call is processed, no other user can share the same channel.
- In FDMA/FDD systems the users are assigned a pair of frequencies, one for the forward channel and other for the reverse channel.
- Fig. 3.4.1 shows the principle of FDMA scheme where different channels are assigned different frequency bands.

3.4.1 Features of FDMA

The features of FDMA are :

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

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

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

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

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

vi) The complexity of FDMA systems is less.

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

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

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

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

3.4.2 Nonlinear Effects in FDMA

- In this multiplexing method, the same antenna at the base station is shared by several radio channels.
- The power amplifiers are operated near saturation region for getting maximum possible power efficiency and it is **non-linear**.
- These non-linearities cause the spreading of signals over the entire frequency domain and result in Inter Modulation (IM) frequencies. IM is undesired RF radiation. It can interface with the other channels in the FDMA system.
- Adjacent channel interference can produced as a result of the spectrum spreading.
- Inter-modulation generates harmonics that cause interferences in the actual signal and inter-modulation must be minimized.

3.4.3 Number of Channels in a FDMA System

- In an FDMA/FDD system a single user occupies a single channel while call is in progress. The single channel is two simplex channels that are frequency duplexed with a separation.
- When a hand-off occurs or a call is completed, the channel is cleared so that another mobile subscriber can use it. The voice channels are sent on the forward channel from the base station to the mobile unit and on the reverse channel from the mobile unit to the base station.
- The **number of channels (N)** that can be simultaneously supported in a FDMA system is given by,

$$N = \frac{B_t - 2\,B_{guard}}{B_c}$$

Where, B_t : Total spectrum allocation

B_{guard} : Guard band allocated at edge of allocated spectrum

B_c : Channel bandwidth

3.4.4 Types of FDMA

There are two types of FDMA. They are :

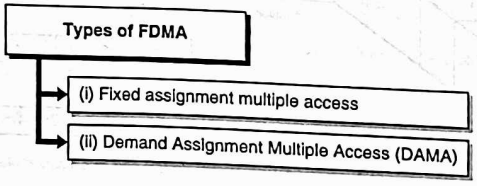


Fig. 3.4.2 : Types of FDMA

(i) Fixed Assignment Multiple Access (FDMA)

It is denoted as **"FAMA"**. In this method the channels are assigned in a predetermined manner and distributed so that random changes in the capacity are not allowed.

(ii) Demand Assignment Multiple Access (DAMA)

If there are multiple stations there is a change of capacity. Then channel can be allocated according to the demand.

3.4.5 Merits of FDMA

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

(ii) No synchronization is necessary.

(iii) The complexity of systems is low.

3.4.6 Demerits of FDMA

(i) Inter-modulation frequencies can cause adjacent channel interference.

(ii) As a result of non-linearities, inter-modulation products are generated.

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

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

(v) The bandwidth of FDMA channels is narrow.

3.5 TIME DIVISION MULTIPLE ACCESS

- It uses time instead of frequency. Different users share the same time slots of the complete time available.
- Each user to allocated a time slot in which the user can access the channel. In each slot only one user is allowed to transmit or receive.
- As shown in Fig. 3.5.1 each user is assigned a time slot so that channel may be thought as a time slot that reoccurs every frame where N slots comprise a frame.

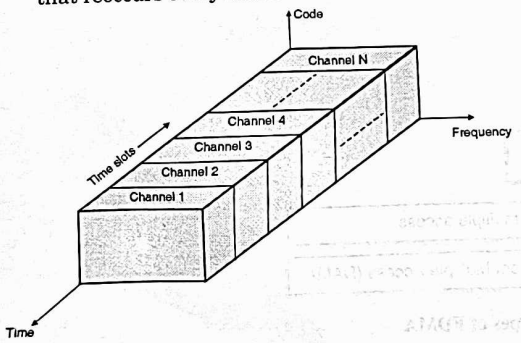


Fig. 3.5.1 : TDMA

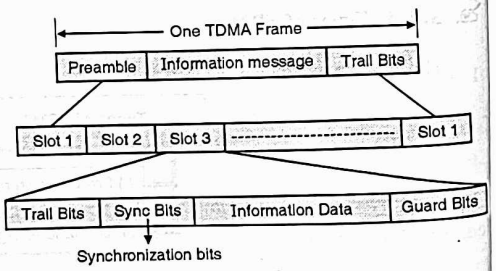


Fig. 3.5.2 : TDMA frame structure

- The TDMA systems transmit data in **burst and buffer** method. The transmission from different users in interfaced into a repeating frame structure as shown in Fig. 3.5.2.

- A frame consists of a number of slots. Each frame consists of preamble, an information message and trail bits. Half of the time slots will be used for the forward link channels and the remaining half for reverse link channels.
- The preamble field comprises the address and synchronization data that both the base stations and subscribers use to identify each other.
- The guard bits are used to provide synchronization of different receivers between, different time slots and frames. It is assumed that there are "N" number of slots for N users so that each user can access the channel in their allowed time slot.
- The TDMA/FDD systems have identical frame structure that can be used for forward or reverse transmission, but the carrier frequencies will be different for both the links.

3.5.1 TDMA Features

The features of TDMA are :

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

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

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

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

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

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

(vii) In TDMA, the handoff process is simple. An enhanced link control like that provided by Mobile Assisted Hand Off (MAHO) can be carried by the subscriber by listening on an idle slot in the TDMA frame.

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

3.5.2 Number of Channels in TDMA System

The **number of channel slots** that can be provided in a TDMA system is found by multiplying the number of TDMA slots per channel by number of channels available.

$$N = \frac{m\,(B_t - 2\,B_{guard})}{B_c}$$

Where, m : Maximum number of TDMA users supported on each radio channel

B_t : Total spectrum allocation

B_{guard} : Guard band allocated at the edge of allocated spectrum

B_c : Channel bandwidth

3.5.3 Efficiency of TDMA System

- The efficiency of a TDMA system is a measure of the percentage of the data that is transmitted. The transmitted data has information for providing overhead for the access scheme.
- The frame efficiency η_f is the percentage of bits per frame that contain transmitted data.
- The number of overhead bits per frame is expressed as,

$$b_{overhead} = N_r b_r + N_t b_p + N_t b_g + N_r b_g$$

where, N_r : Number of reference bursts per frame

N_t : Number of traffic bursts per frame

b_r : Number of overhead bits per reference burst

b_p : Number of overhead bits per preamble in each slot

b_g : Number of equivalent bits in each guard time interval

- The total number of bits per frame b_T is,

$$b_T = T_f R$$

where, T_f : Frame duration

R : Channel bit rate

Thus, the frame efficiency is,

$$\eta_f = \left(\frac{1 - b_{overhead}}{b_T}\right) \times 100\ \%$$

3.6 CDMA (CODE DIVISION MULTIPLE ACCESS)

- In this multiple access scheme many users share the same carrier frequency (f_c). The narrowband message signal is also multiplexed with a spreading signal of larger bandwidth. This spreading signal is a pseudo noise code sequence and it has higher chip rate than the data rate of the message signal.
- As the same channel is used by several users, there may be a problem of **near-far effect.**

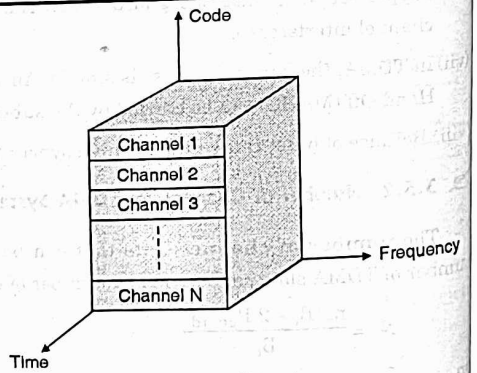


Fig. 3.6.1 : CDMA scheme

- The near-far problem occurs if the power of each user within the cell is not controlled such that they appear equal at the base station.
- The main advantage of CDMA when compared to other multiple access methods is reduced level of interference. As each user is allocated an individual pseudo random codeword that is orthogonal to the code words of the other users at the receiver end the receiver tunes to receive the intended signal of the user.
- To minimize the near-far problem power control is essential in CDMA systems. Power control is implemented at the base station by sampling the radio signal strength indicator (RSSI) levels of each mobile and then a power change command over the forward radio link.

3.6.1 Features of CDMA

The features of CDMA are :

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

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

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

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

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

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

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

Ex. 3.6.1 : In an omni-directional CDMA cellular system Eb/No required is 20 dB. If 100 users, each with a baseband data rate of 13 kbps are to be accommodated, determine the minimum channel bit rate of spread spectrum chip sequence assuming voice activity factor of 0.4.

Soln. :

Given : $\frac{E_b}{N_o} = 20$ dB, $N = 100$ users, $R = 13$ kbps, $\alpha = 0.4$

To find : $W = ?$

$$\frac{E_b}{N_o} = \frac{W/R}{(N-1)\,\alpha} = 10 \log\left(\frac{E_b}{N_o}\right)$$

$$20 = 10 \log\left(\frac{E_b}{N_o}\right)$$

$$\frac{E_b}{N_o} = \text{antilog } 2 = 100$$

$$\frac{E_b}{N_o} = \frac{W/R}{(N-1)\,\alpha}$$

$$100 = \frac{W}{\frac{13 \times 10^3}{(100-1) \times 0.4}}$$

$$W = 100 \times (100-1) \times 0.4 \times 13 \times 10^3 = \mathbf{51.48\ Mchips / sec}$$ ...Ans.

☞ **Comparison of FDMA, TDMA and CDMA**

Table 3.6.1 : Comparison of FDMA, TDMA and CDMA

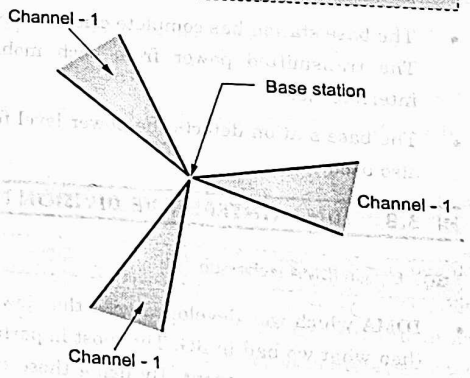
Sr. No.	Parameter	FDMA	TDMA	CDMA
1.	Method	Overall bandwidth is shared among many stations.	Time sharing of satellite transponder takes place.	Sharing of bandwidth and time both takes place.
2.	Interference effect	Due to nonlinearity of transponder amplifiers, inter modulation products are generated due to interference between adjacent channels.	Due to incorrect synchronization there can be interference between the adjacent time slots.	Both types of interferences will be present.
3.	Synchronization	Synchronization is not necessary.	Synchronization is essential.	Synchronization is not necessary.
4.	Code word	Code word is not required.	Code word is not required.	Code words are required.
5.	Guard times and bands	Guard bands between adjacent channels are necessary.	Guard times between adjacent time slots are necessary.	Guard bands and Guard times both are necessary.
6.	Hand-over	Hard handover	Soft handover	Soft handover
7.	Allocated bandwidth	12.5 MHz	12.5 MHz	12.5 MHz
8.	Frequency reuse	7	7	1
9.	Required channel bandwidth	0.03 MHz	0.03 MHz	1.25 MHz
10.	Number of RF channels	$\frac{12.5}{0.03} = 416$	$\frac{12.5}{0.03} = 416$	$\frac{12.5}{1.25} = 10$

Sr. No.	Parameter	FDMA	TDMA	CDMA
11.	Control channels / cell	2	2	2
12.	Usable channels / cell	57	57	8
13.	Voice channels / cell	$57 \times 1 = 57$	$57 \times 4 = 228$	$8 \times 4 = 320$
14.	Sectors per cell	3	3	3
15.	Voice calls/sector	$\frac{57}{3} = 19$	$\frac{228}{3} = 76$	$\frac{320}{3} = 106$
16.	Key resources	FDMA assigns individual channels to individual users.	TDMA systems divide the radio spectrum into time slots.	CDMA systems use the same carrier frequency and can simultaneously transmit.
17.	Sharing of resources	Each user is allocated a unique channel. No other user can share that channel when a call is in progress.	Each user makes use of non-overlapping time slots. The data transmission occurs in bursts.	Each user has its own pseudorandom codeword that is orthogonal to other keywords.
18.	System complexity	Lower	Higher	Higher
19.	System flexibility	Simple and Robust, inflexible	Flexible	Flexible

3.7 SDMA (SPACE DIVISION MULTIPLE ACCESS)

GQ. Explain in details Space Division Multiple Access technique.

The narrow beam of radio waves is aimed at particular part of space. The same channel is reused over the another narrow beam aimed at another part of the space. This division of space in different directions of base station through highly directional beams is called Space Division Multiple Access (SDMA). As shown Fig. 3.7.1 the space is divided and three channels are transmitted on same frequency.



Space Division Multiple Access (SDMA)

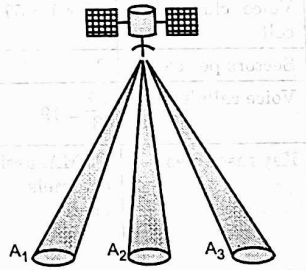
Fig. 3.7.1 : SDMA

☞ **Advantages**

1. It saves the channel bandwidth.
2. Improves the utility of bandwidth.

☞ **Role of SDMA In wire and Wireless Communications**

- SDMA can be used for mobile communication and satelite communication. The satelite dish antennas transmit signals to various zones on earth's surface. These antennas are highly directional. Hence same frequency can be used for multiple surface zones, as shown in Fig. 3.7.2.
- As shown in Fig. 3.7.2, area **A1** and area **A3** are physically apart. Hence same channel-1 is used to send signals to **A1** and **A3** with the help of highly directional atennas. There will be no signal interface between the signals of areas **A1** and **A3**.



Frequency Reuse by SDMA

Fig. 3.7.2 : Frequency Reuse by SDMA

- Satellite based SDMA required careful selection of zones (area) for each transmitter and precise antenna alignment to avoid co-channel and Fig. Frequency reuse by SDMA interchannel interference.
- In cellular (mobile) communiation, the power of the transmitting antennas is to be controlled to avoid the co-channel and interchannel interference.
- In cellular communication Space Division Multiple Access (SDMA), there are multidirectional horn antennas at the base station (BS). The base station identifies mobile users by means of their spatial signatures.
- The base station has complete control over the power of all the transmitted signals on the forward link. The transmitted power from each mobile user is dynamically controlled to avoid inter channel interference.
- The base station detects the power level from each mobile user and connects it. Adpative antennas are also used.

3.8 IDMA (INTERLEAVE DIVISION MULTIPLE ACCESS)

GQ. Expalin IDMA technique

- IDMA which was developed with the view of achieving something more in terms of speed and capacity then what we had in 3G. The most important in IDMA is turbo-code which has increased the efficiency of 4G to a larger extent. By using these turbo codes with interleave division multiple excess the data rates 4G technology has been increased significantly.

- The basic idea behind this article is to lead down how by using interleaver division multiple accesses we can achieve higher coding gain, capacity, high speed (both for uploading & downloading) by using turbo codes along with IDMA.
- Interleaver is the heart of IDMA system. IDMA is often called as the next generation multiple access techniques for CDMA and also for OFDM. In IDMA different users can use different types of Interleavers
- In IDMA system, the main challenge is to avoid ISI in the non-orthogonal signals, since here signal are not orthogonal as in OFDM . We also have a multiple access technique named CDMA (Code Division Multiple Access) where the symbols are not orthogonal and here the symbols are transmitted via asynchronous transmission and due to these problems like ICI and ISI are encountered in CDMA also the problem of MUD takes place in CDMA due to this type of transmission . Therefore to overcome all these issues in IDMA is used where all the signal are separated using interleavers and hence, IDMA can be called as a special form of CDMA .

☞ **Types of Interleavers**

Random Interleavers

- This form the easiest way for the symbols to spread across the spectrum using interleavers. In random interleavers, the concept of pseudo-random computation is used.
- All the symbols that are to be transmitted are scrambled randomly in an arbitrary fashion Fig. 3.8.1 . Since the data is scrambled in an arbitrary way this help to reduce the burst error of the channels at the receiving side .

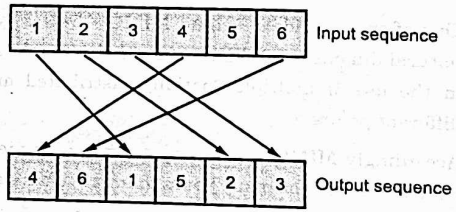


Fig. 3.8.1: Scrambling of data in Random Interleavers

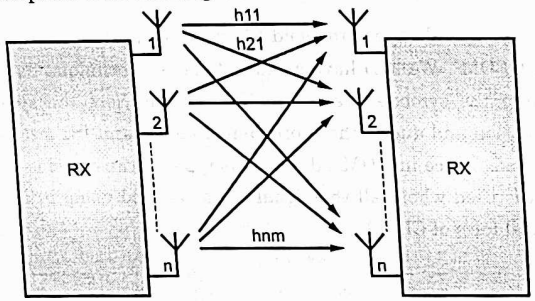
Master Random Interleavers

- Master Random Interleavers is similar to random interleavers in its functioning but it overcomes the drawbacks encountered in random interleavers.
- The major setback of random interleavers is that it is very difficult to separate the users. Here, in this case, the above-mentioned issue can be avoided.
- IDMA uses interleavers for transmission, therefore, it is essential for the BS (Base Station) to store all the interleavers with the respective patterns used, and therefore interleavers will definitely consume the memory making the spectrum less efficient to handle more number of users. Apart from this at an initial stage, it is also required for BS and MS (Mobile Station) to share the pattern of interleavers used for communication.

3.9 MIMO (MULTIPLE INPUT MULTIPLE OUTPUT)

GQ. Write a Short note on MIMO

- MIMO is effectively a radio antenna technology as it uses multiple antennas at the transmitter and receiver to enable a variety of signal paths to carry the data, choosing separate paths for each antenna to enable multiple signal paths to be used Fig. 3.9.1.



General Outline of MIMO system

Fig. 3.9.1 : General Outline of MIMO System

- One of the core ideas behind MIMO wireless systems space-time signal processing in which time (the natural dimension of digital communication data) is complemented with the spatial dimension inherent in the use of multiple spatially distributed antennas, i.e. the use of multiple antennas located at different points.
- Accordingly MIMO wireless systems can be viewed as a logical extension to the smart antennas that have been used for many years to improve wireless.
- It is found between a transmitter and a receiver, the signal can take many paths. Additionally by moving the antennas even a small distance the paths used will change. The variety of paths available occurs as a result of the number of objects that appear to the side or even in the direct path between the transmitter and receiver.
- Previously these multiple paths only served to introduce interference. By using MIMO, these additional paths can be used to advantage. They can be used to provide additional robustness to the radio link by improving the signal to noise ratio, or by increasing the link data capacity.
- The two main formats for MIMO are given below:
  - ***Spatial diversity :*** Spatial diversity used in this narrower sense often refers to transmit and receive diversity. These two methodologies are used to provide improvements in the signal to noise ratio and they are characterised by improving the reliability of the system with respect to the various forms of fading.
  - ***Spatial multiplexing :*** This form of MIMO is used to provide additional data capacity by utilising the different paths to carry additional traffic, i.e. increasing the data throughput capability.

- As a result of the use multiple antennas, MIMO wireless technology is able to considerably increase the capacity of a given channel while still obeying Shannon's law. By increasing the number of receive and transmit antennas it is possible to linearly increase the throughput of the channel with every pair of antennas added to the system. This makes MIMO wireless technology one of the most important wireless techniques to be employed in recent years.
- As spectral bandwidth is becoming an ever more valuable commodity for radio communications systems, techniques are needed to use the available bandwidth more effectively. MIMO wireless technology is one of these techniques

3.10 OFDM (ORTHOGONAL FREQUENCY DIVISION MULTIPLEXING)

3.10.1 Concept of OFDM

- OFDM is a technique in which bandwidth is divided into several orthogonal frequency subcarriers. There is no guard band in between adjacent subcarrier still the interference is avoided as there are orthogonal to each other.
- **Orthogonality :** Signals are orthogonal if they are mutually independent of each other. Orthogonality is a property that allows multiple information signals to be transmitted perfectly over a common channel and detected, without interference. OFDM achieves orthogonality in the frequency domain by allocating each of the separate information signals onto different subcarriers.
- It allows better spectral efficiency and simple equalization at the receiver.
- Even though there is overlapping in time and frequency domain still there is no mutual interference when the sampling is done at subcarrier positions.

Refer Fig. 3.10.1.

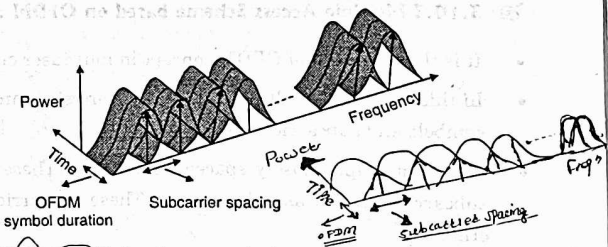


Fig. 3.10.1 : OFDM signal representation in time frequency domain

3.10.2 OFDM Transmitter and Receiver

Refer Fig. 3.10.2.

- **Serial To Parallel Conversion :** The input data is made compatible for transmission by converting it into suitable word size and then transmitting it parallelly using one carrier for each data word.
- **Modulator :** Each carrier which is to be used is allotted with the data whose amplitude and phase are chosen according to the modulation scheme being used (typically BPSK, QPSK, or QAM). It is used because of its simplicity and to reduce problems of fading due to amplitude variations.
- **IFFT :** IFFT on transmitter and FFT on receiver's side are used to reduce the use of I/Q modulators and demodulators. It is used to modulate and demodulate respectively. The data constellations on the subcarriers.

- **Cyclic prefix :** For OFDM the system bandwidth is broken up into N subcarriers, resulting in a symbol rate that is N times lower than the single carrier transmission. This low symbol rate makes OFDM naturally resistant to effects of Inter-Symbol Interference (ISI) caused by multipath propagation. Hence cyclic prefix ix added. Due to this the transmitted signal becomes periodic and the effect of time dispersive multipath channel becomes equivalent to cyclic convolution and it also discards the guard interval at the receiver. Due to this subcarriers remain orthogonal. Its length should not exceed the maximum excess delay of the multipath propagation channel.
- **Receiver :** The receiver basically does the reverse operation to the transmitter to retrieve the information transmitted.

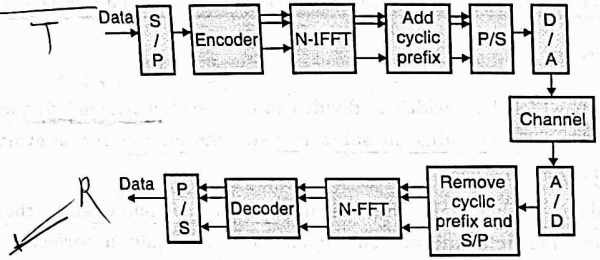


Fig. 3.10.2 : Block diagram of OFDM transmitter and receiver

3.10.3 Multiple Access Scheme based on OFDM : OFDMA

- It is the extension of OFDM concept in multiuser environment.
- In this technique multiple user signals are separated in both time and frequency domains using OFDM symbols and subcarriers respectively.
- It uses multiple closely spaced subcarriers. These subcarriers are then divided further into group of subcarriers called as subchannels. These subcarriers in subchannels need not to be adjacent to each other.
- Fig. 3.10.3 shows subcarriers of same colour represent subchannel group.

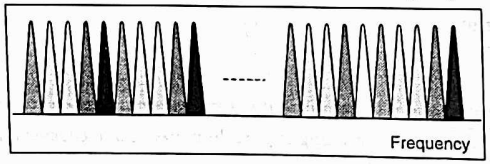


Fig. 3.10.3 : OFDMA spectrum showing subchannels

- Multiplexing is done by allocation of different subchannels or different OFDM symbols to different users to send and receive signals. The burst in OFDMA consists of several OFDM symbols.
- OFDMA can be well explained by the given example. Please refer Fig. 3.10.4.

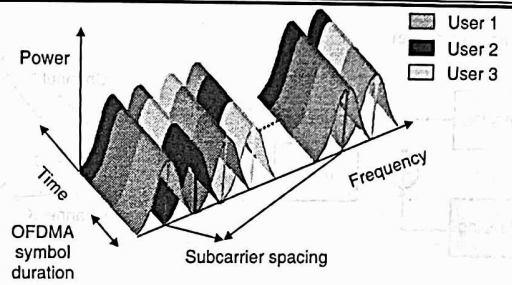


Fig. 3.10.4 : Example - Allocation of channels to the users in OFDMA

Subcarrier Allocation

- The working principle of OFDMA is based on allocation of subchannels based on subcarrier allocation strategies.
- There are three types : Refer Fig. 3.10.5
  1. SCAS (Sub Band Carrier Allocation Scheme)
  2. ICAS (Interleaved CAS)
  3. Generalized CAS

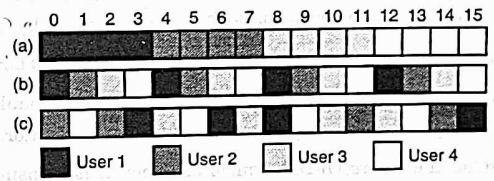


Fig. 3.10.5 : Subcarrier allocation schemes in OFDMA - (a) SCAS (b) Interleaved CAS(c) Generalised CAS

1. **SCAS (Sub Band Carrier Allocation Scheme) :** In this all the subcarriers of each user are grouped together. Hence it is easy to separate them using simple filter banks. However in this efficient use of frequency diversity is not done and it is affected by fading in the subcarriers of given users.
2. **ICAS (Interleaved CAS) :** The problems associated with SCAS are solved in this scheme. In this allocation of subcarriers is done with uniform spacing between them. Still it faces problem of restriction on resource allocation.
3. **Generalized CAS :** It is the most flexible and desirable method of subcarrier allocation. It gives choice to the users to select the best available subcarrier to transmit their information. Hence it provides complete use of channel frequency diversity. Also it provides flexibility in resource allocation.

☞ **OFDMA transmitter and receiver**

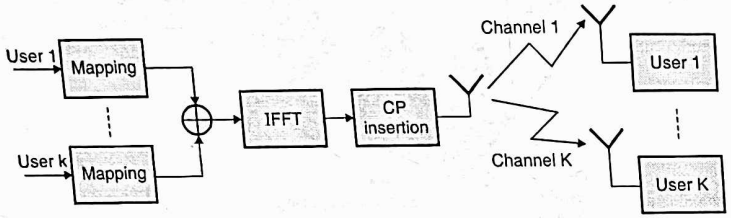


Fig. 3.10.6(a) : Block diagram of OFDMA transmitter for downlink path

Refer Fig. 3.10.6(a). It shows block diagram of OFDMA transmitter.

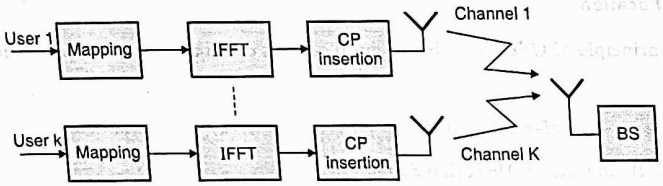


Fig. 3.10.6(b) : Block diagram of OFDMA transmitter for uplink path

- In the transmitter generally N subcarriers are allocated to K number of users using one of the above explained CAS scheme. Let M be length of the block of the data obtained by dividing the user data.
- Obviously these M data symbols makes use of their respective subcarriers for modulation.
- On a downlink path, other subcarriers of length N block of data are modulated with data from other users and the modulated output is sent using conventional OFDM modulator.
- Cyclic prefix is then added the before OFDM symbol and then it is transmitted over k channels to k different users.
- On the uplink path the uplink transmitter leaves the other subcarrier empty and resulting N block with M empty subcarriers are then sent to IFFT. After that different CP is added to different symbols and then they are sent on different channels to the base station.
- At the receiver first CP is removed and then N point samples are passed through N point FFT.

☞ **Why synchronization of uplink is a difficult problem in OFDMA?**

- OFDMA converts frequency selective channel into flat fading channel very efficiently. Hence for channel equalization one tap multipliers are used for each subcarrier. This output of equalizer is then used for detection.
- On downlink path each user picks up only M data symbols transmitted over its allocated subcarriers for channel equalization and detection purposes.
- But on uplink, the received signal is comprised of signals from all active users and hence it has different frequency offsets and different propagation delays. Hence offset correction needs to be applied in order to detect these signals. And all these parameters needs to be dealt with jointly and hence synchronization is a difficult issue in OFDMA on uplink path.

☞ **Advantages of OFDMA**

1. Scalability
2. Intrinsic protection against Multi Access Interference (MAI)
3. Flexibility in resource management
4. Robustness to multipath channels
5. Simple equalization

☞ **Disadvantage of OFDMA**

1. It is extremely sensitive to timing errors and carrier frequency offsets.
2. Subcarrier allocation algorithms used at transmitter introduces complexity.
3. When the OFDMA signal passes through RF amplifier with non linearities BER increases.
4. Cochannel interference is bit complex compared to CDMA.

☞ **Applications**

1. IEEE 802.20 (Mobile broadband wireless access)
2. WiMAX (Worldwide interoperability for microwave access)
3. ETSI (European Telecommunication's Standard Institute) broadband radio access network
4. Multiuser satellite communication
5. 4G LTE (Long term evolution) network

Chapter Ends...

❑❑❑

UNIT IV

CHAPTER 4

Wireless Communication Protocols

Syllabus

Wireless Application Protocol, The WAP Programming Model, WAP Architecture, Traditional WAP Networking Environment, Wi-Fi Direct, Li-Fi, NFC, SigFox, Z-Wave, LoRaWAN, Thread (based on IEEE 802.15.4), RT Wi-Fi, RTCP, RTSP, SPEED.

4.1 INTRODUCTION OF WIRELESS APPLICATION PROTOCOL (WAP)

GQ. Write short note on WAP.

☞ **Wireless Application Protocol (WAP)**

(1) WAP stands for wireless application protocol. WAP is worldwide standard for providing internet communications and advanced telephony service on digital mobile phones, and other wireless terminals.

Wireless terminals

(i) **Wireless :** lacking or not requiring a wire or wires pertaining to radio transmission.

(ii) **Application :** A computer program or piece of computer software that is designed to do a specific task.

(iii) **Protocol :** A set of technical rules about how information should be transmitted and received using computer.

(2) WAP is a technical standard for accessing information over a mobile wireless network. A WAP browser is a web browser for mobile devices such as mobile phones that uses the protocol.

(3) WAP is an important development in the wireless industry because of its attempt to develop an open standard for wireless protocols, independent of vendor and air - link.

(4) The WAP information is broken down under a number of headings.

(5) The Wireless Application Protocol takes a client server approach.

(6) The Wireless Application Protocol is aimed at turning a mass - market mobile phone into a "network - based smartphone".

(7) The WAP was conceived by four companies: Ericsson, Motorola, Nokia, and Unwired Planet (now Phone.com). The Wireless Markup Language (WML) is used to create pages that can be delivered using WAP.

4.1.1 WAP Applications

GQ. Write about the application of WAP.

(1) WAP is being used to develop enhanced forms of existing applications and new versions of today's applications.

(2) Existing mobile data software and hardware supplies are adding WAP support to their offering.

(3) New distribution channel for their existing products and services - for example, CNN and Nokia teamed up to offer CNN Mobile reply to incoming information on the phone by allowing new menus to access mobile services.

(4) Part of the business case for network operators - by making the value - added services more easily to reply to and request (using menus instead of keywords, for example),

(5) WAP can help generate additional traffic on the network and therefore revenue.

(6) The Wireless Application Protocol is envisaged as a comprehensive and scalable protocol designed for use with :

(a) Any mobile phone from those with a one line display to a smart phone.

(b) Any existing or planned wireless service such as the Short Message Service, Circuit Switched Data, Unstructured Supplementary Services Data (USSD) and General Packet Radio Service (GPRS). Indeed, the importance of WAP can be found in the fact that it provides an evolutionary path for application developers and network operators to offer their services on different network types, bearers and terminal capabilities. The design of the WAP standard separates the application elements from the bearer being used. This helps in the migration of some applications from SMS or Circuit Switched Data to GPRS for example.

(c) Any mobile network standard such as Code Division Multiple Access (CDMA), Global System for Mobiles (GSM), or Universal Mobile Telephone System (UMTS). (d) WAP has been designed to work with all cellular standards and is supported by major worldwide wireless leaders such as ATandT Wireless and NTT DoCoMo, multiple input terminals such as keypads, keyboards, touch - screens and styluses.

4.1.2 WAP Architecture/ Protocol Stack

GQ. Describe briefly WAP model architecture. OR Describe briefly WAP Protocol Stack in details.

AP is designed in a layered fashion, so that it can be extensible, flexible, and scalable. As a result, the WAP protocol stack is divided into five layers :

☞ **Layers of WAP Protocol**

(I)	Application Layer	(II)	Session Layer
(III)	Transaction Layer	(IV)	Security Layer
(V)	Transport Layer		

(I) Application Layer

Wireless Application Environment (WAE). This layer is of most interest to content developers because it contains among other things, device specifications, and the content development programming languages, WML, and WMLScript.

(II) Session Layer

Wireless Session Protocol (WSP). Unlike HTTP, WSP has been designed by the WAP Forum to provide fast connection suspension and reconnection.

(III) Transaction Layer

Wireless Transaction Protocol (WTP). The WTP runs on top of a datagram service, such as User Datagram Protocol (UDP) and is part of the standard suite of TCP/IP protocols used to provide a simplified protocol suitable for low bandwidth wireless stations.

(IV) Security Layer

Wireless Transport Layer Security (WTLS). WTLS incorporates security features that are based upon the established Transport Layer Security (TLS) protocol standard. It includes data integrity checks, privacy, service denial, and authentication services.

(V) Transport Layer

- Wireless Datagram Protocol (WDP). The WDP allows WAP to be bearer-independent by adapting the transport layer of the underlying bearer.
- The WDP presents a consistent data format to the higher layers of the WAP protocol stack, thereby offering the advantage of bearer independence to application developers.
- Each of these layers provides a well-defined interface to the layer above it. This means that the internal workings of any layer are transparent or invisible to the layers above it.
- The layered architecture allows other applications and services to utilise the features provided by the WAP-stack as well.
- This makes it possible to use the WAP-stack for services and applications that currently are not specified by WAP.
- The WAP protocol architecture is shown below alongside a typical Internet Protocol stack.
- Note that the mobile network bearers in the lower part of the Fig. above are not part of the WAP protocol stack.
- Routing protocols for ad hoc wireless networks: DSDV and AODV

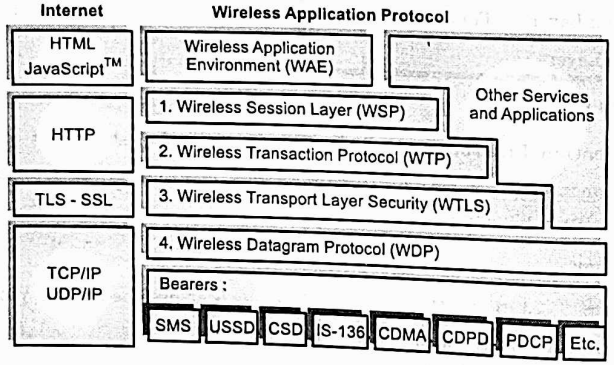


Fig. 4.1.1 : WAP Protocal Stack

4.2 WIRELESS APPLICATION PROTOCOL MODEL

GQ. Write a short note on Wirelss Application protocol Model.

- **WAP** stands for **Wireless Application Protocol**. It is a protocol designed for micro-browsers and it enables the access of internet in the mobile devices.
- It uses the mark-up language WML (Wireless Markup Language and not HTML), WML is defined as XML 1.0 application. It enables creating web applications for mobile devices. In 1998, *WAP Forum* was founded by Ericson, Motorola, Nokia and Unwired Planet whose aim was to standardize the various wireless technologies via protocols.
- WAP protocol was resulted by the joint efforts of the various members of WAP Forum.
- In 2002, WAP forum was merged with various other forums of the industry resulting in the formation of **Open Mobile Alliance (OMA)**.

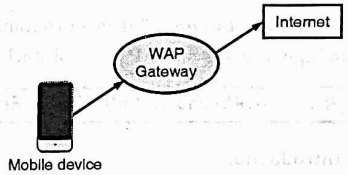


Fig. 4.2.1

WAP Model

- The user opens the mini-browser in a mobile device. He selects a website that he wants to view. The mobile device sends the URL encoded request via network to a WAP gateway using WAP protocol.

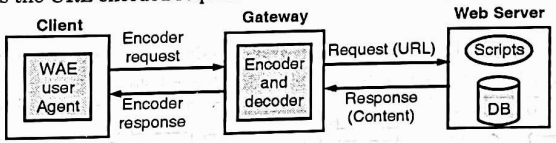


Fig. 4.2.2

- The WAP gateway translates this WAP request into a conventional HTTP URL request and sends it over the internet.
- The request reaches to a specified Web server and it processes the request just as it would have processed any other request and sends the response back to the mobile device through WAP gateway in WML file which can be seen in the micro-browser.

WAP Protocol stack

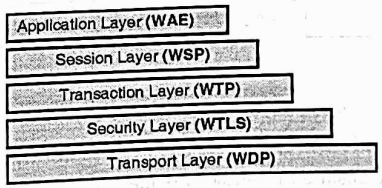


Fig.4.2.3

(1) **Application Layer :** This layer contains the *Wireless Application Environment (WAE)*. It contains mobile device specifications and content development programming languages like WML.

(2) **Session Layer :** This layer contains *Wireless Session Protocol (WSP)*. It provides fast connection suspension and reconnection.

(3) **Transaction Layer :** This layer contains *Wireless Transaction Protocol (WTP)*. It runs on top of UDP (User Datagram Protocol) and is a part of TCP/IP and offers transaction support.

(4) **Security Layer :** This layer contains *Wireless Transaction Layer Security (WTLS)*. It offers data integrity, privacy and authentication.

(5) **Transport Layer :** This layer contains *Wireless Datagram Protocol*. It presents consistent data format to higher layers of WAP protocol stack.

4.3 WIRELESS APPLICATION ENVIRONMENT (WAE)

Introduction

- Wireless Application Environment (WAE), the uppermost layer in the WAP stack, provides an environment that enables a wide range of applications to be used on the wireless devices.
- The main idea behind the Wireless Application Environment (WAE) is to create a general-purpose application environment based mainly on existing technologies and philosophies of the World Wide Web.
- One global goal of the WAE is to minimize over-the-air traffic and resource consumption on the handheld device, which is reflected in the logical model shown below:

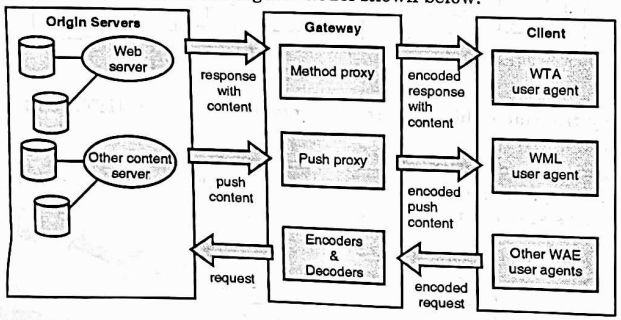


Fig. 4.3.1

- A client issues an encoded request for an operation on a remote server. Encoding is necessary to minimize data sent over the air and to save resources on the handheld device.
- Decoders in a gateway now translate this encoded request into a standard request as understood by the origin servers. This could be a request to get a web page to set up a call. The gateway transfers this request to the appropriate origin server as if it came from a standard client.

- Origin servers could be standard web servers running HTTP and generating content using scripts, providing pages using a database, or applying any other (proprietary) technology.
- The origin servers will respond to the request. The gateway now encodes the response and its content (if there is any) and transfers the encoded response with the content to the client.
- The WAE logical model not only includes this standard request/response scheme, but it also includes push services. Then an origin server pushes content to the gateway. The gateway encodes the pushed content and transmits the encoded push content to the client. Several user agents can reside within a client.
- User agents include such items as: browsers, phonebooks, message editors etc. WAE does not specify the number of user agents or their functionality, but assumes a basic WML user agent that supports WML, WMLscript, or both (i.e., a 'WML browser').
- However, one more user agent has been specified with its fundamental services, the WTA user agent. This user agent handles access to, and interaction with, mobile telephone features (such as call control).
- As over time many vendor dependent user agents may develop, the standard defines a user agent profile (UAProf), which describes the capabilities of a user agent.

4.4 COMPONENTS OF WAE

GQ. Expalin different component of WAE in details.

(1) Addressing Model

A syntax suitable for naming resources stored on servers. WAP use the same addressing model as the one used on the Internet that is Uniform Resource Locators (URL).

(2) Wireless Markup Language (WML)

A lightweight markup language designed to meet the constraints of a wireless environment with low bandwidth and small handheld devices. The Wireless Markup Language is WAP's analogy to HTML used on the WWW. WML is based on the Extensible Markup Language (XML).

(3) WMLScript

A lightweight scripting language. WMLScript is based on ECMAScript, the same scripting language that JavaScript is based on. It can be used for enhancing services written in WML in the way that it to some extent adds intelligence to the services; for example, procedural logic, loops, conditional expressions, and computational functions.

(4) Wireless Telephony Application (WTA, WTAI)

A framework and programming interface for telephony services. The Wireless Telephony Application (WTA) environment provides a means to create telephony services using WAP.

4.5 HARDWARE AND SOFTWARE REQUIREMENT

- At minimum developing WAP applications requires a web server and a WAP simulator. Using simulator software while developing a WAP application is convenient as all the required software can be installed on the development PC.
- Although, software simulators are good in their own right, no WAP application should go into production without testing it with actual hardware.
- The following list gives a quick overview of the necessary hardware and software to test and develop WAP applications –
  (1) A web server with connection to the Internet
  (2) A WML to develop WAP application
  (3) A WAP simulator to test WAP application
  (4) A WAP gateway
  (5) A WAP phone for final testing.
- Microsoft IIS or Apache on Windows or Linux can be used as the web server and Nokia WAP Toolkit version 2.0 as the WinWAP simulator.

4.6 CONFIG. WEB SERVER FOR WAP

- In the WAP architecture, the web server communicates with the WAP gateway, accepting HTTP requests and returning WML code to the gateway. The HTTP protocol mandates that each reply must include something called a Multi-Purpose Internet Mail Extensions (MIME) type.
- In normal web applications, this MIME type is set to text/html, designating normal HTML code. Images on the other hand could be specified as image/gif or image/jpeg for instance. With this content type specification, the web browser knows the data type that the web server returns.
- In WAP applications a new set of MIME types must be used, as shown in the following table –

File type	MIME type
WML (.wml)	text/vnd.wap.wml
WMLScript (.wmls)	text/vmd.wap.wmlscript
WBMP (.wbmp)	image/vnd.wap.wbmp

- In dynamic applications, the MIME type must be set on the fly, whereas in static WAP applications, the web server must be conFig.d appropriately.
- For more information about configuring MIME types for your web server, please consult your web server documentation.

4.7 WMLSCRIPT (WIRELESS MARKUP LANGUAGE SCRIPT)

GQ. What is WMLScript ? Expalin in details.

WMLScript (Wireless Markup Language Script) is the client-side scripting language of WML (Wireless Markup Language). A scripting language is similar to a programming language, but is of lighter weight. With WMLScript, the wireless device can do some of the processing and computation. This reduces the number of requests and responses to/from the server.

(1) WML Script Components

WML Script is very similar to Java Script. WML Script components have almost similar meaning as they have in Java Script. The WML Script program components are summarized here.

(2) WML Script Operators

WML Script supports following type of operators.

(i) Arithmetic Operators
(ii) Comparison Operators
(iii) Logical (or Relational) Operators
(iv) Assignment Operators
(v) Conditional (or ternary) Operators

(3) WML Script Control Statements

Control statements are used for controlling the sequence and iterations in a program.

Statement	Description
if-else	Conditional branching
For	Making self-incremented fixed iteration loop
while	Making variable iteration loop
break	Terminates a loop
continue	Quit the current iteration of a loop

(4) WML Script Functions

The user-defined functions are declared in a separate file having the extension .wmls. Functions are declared as follows –

```
function name (parameters) {
 control statements;
 return var;
}
```

The functions used are stored in a separate file with the extension .wmls. The functions are called as the filename followed by a hash, followed by the function name –

```
maths.wmls#squar()
```

(5) WML Scripts Standard Libraries

The are six standard libraries totally. Here is an overview of them –

- **Lang :** The Lang library provides functions related to the WMLScript language core.

  Example Function – abs(),abort(), characterSet(),float(), isFloat(), isInt(), max(), isMax(), min(), minInt(), maxInt(), parseFloat(), parseInt(), random(), seed()

- **Float :** The Float library contains functions that help us perform floating-point arithmetic operations.

  Example Function – sqrt(), round(), pow(), ceil(), floor(), int(), maxFloat(), minFloat()

- **String :** The String library provides a number of functions that help us manipulate strings.

  Example Function – length(), charAt(), find(), replace(), trim(), compare(), format(), isEmpty(), squeeze(), toString(), elementAt(), elements(), insertAt(), removeAt(), replaceAt()

- **URL :** The URL library contains functions that help us manipulate URLs.

  Example Function – getPath(), getReferer(), getHost(), getBase(), escapeString(), isValid(), loadString(), resolve(), unescapeString(), getFragment()

- **WMLBrowser :** The WMLBrowser library provides a group of functions to control the WML browser or to get information from it.

  Example Function – go(), prev(), next(), getCurrentCard(), refresh(), getVar(), setVar()

- **Dialogs :** The Dialogs library Contains the user interface functions.

  Example Function – prompt(), confirm(), alert()

(6) WML Scripts Comments

There are two types of comments in WMLScript –

- **Single-line comment :** To add a single-line comment, begin a line of text with the // characters.
- **Multi-line comment :** To add a multi-line comment, enclose the text within /* and */.

These rules are the same in WMLScript, JavaScript, Java, and C++. The WMLScript engine will ignore all comments. The following WMLScript example demonstrates the use of comments –

```
// This is a single-line comment.

/* This is a multi-line comment. */

/* A multi-line comment can be placed on a single line. */
```


(7) WML Script Case Sensitivity

The WMLScript language is case-sensitive. For example, a WMLScript function with the name WMLScript Function is different from wmlscript function. So, be careful of the capitalization when defining or referring to a function or a variable in WMLScript.

(8) Whitespaces in WMLScript

Except in string literals, WMLScript ignores extra whitespaces like spaces, tabs, and newlines.

(9) WML Script Statement Termination by Semicolons

A semicolon is required to end a statement in WMLScript. This is the same as C++ and Java. Note that JavaScript does not have such requirement but WML Script makes it mandatory.

4.8 WI-FI DIRECT

GQ. How Does Wi-Fi Direct Work?
GQ. What is different Wi-Fi Direct Applications

- Standard Wireless network connections allow devices to receive information through an access point. Through Wi-Fi Direct, devices have the ability to bypass this process and connect to each other directly. When most people think of device-to-device connections, Bluetooth comes to mind.
- Although Wi-Fi Direct offers a similar connection, it's also significantly more powerful than Bluetooth, able to handle a higher data volume at a faster rate.
- In the right setting, Wi-Fi Direct can transfer data at a rate 10 times faster than traditional Bluetooth on your android device. This makes Wi-Fi Direct the superior choice for business applications that require data sharing between devices.

4.8.1 How Does Wi-Fi Direct Work?

- Wi-Fi Direct doesn't require a centralized network or wireless router to share information between devices. Instead, when a connection is made, one device acts as the access point or hotspot. Other devices then connect to this original device using WPS and WPA/WPA2 protocols.
- Once this connection is established, data can be instantly shared between nearby devices, even when there's no network connection available.
- Connections through Wi-Fi Direct can vary depending on the application. Gamers can connect to share an experience on their personal devices or iPhones, or an individual can cast their device onto a television, allowing anyone in the room to see a real-time projection of what's visible on the device screen. Some devices can connect automatically, while others require pushing a button on the device before file-sharing or file transfer.
- For security purposes to this functionality, many connections require the input of a PIN or require you to scan a QR code for a wi-fi protected setup. Even with these extra steps, this kind of connectivity offers a variety of advantages in a business setting.

4.8.2 Benefits of Using Wi-Fi Direct

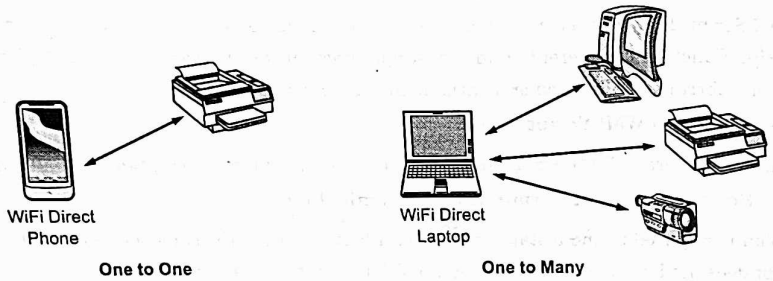


Fig. 4.8.1 : Wi-Fi Direct

- Without Wi-Fi Direct, devices would need to share information through an access point such as a router or over the internet. Sharing sensitive data over the internet comes with security risks, as anything stored or delivered online can be intercepted by cybercriminals. Accessing a local intranet can diminish some of this risk, but it also limits information sharing to areas where a connection can be established to the internal network. Wi-Fi Direct offers instant connectivity in any setting as long as the devices are within range of each other. This provides significant mobility in business applications.
- The power of Wi-Fi Direct also increases its usability. With higher data and speed capabilities, team members can easily share high-resolution video, photos, and large data files. This is an excellent collaborative tool when working with significant information because adjustments can be made in real-time, updating on any connected device instantly.

4.8.3 What Devices Are Wi-Fi Direct Enabled?

- Device compatibility is rarely an issue today thanks to Wi-Fi Direct technology being available over the last decade. Both Android 4.0 and Apple devices or IOS support direct connections, though Apple offers it under the names AirPlay and AirDrop. Smart televisions often allow casting from Wi-Fi Direct devices, and many streaming devices, such as Roku and Chromecast, are compatible as well.
- Businesses can also obtain compatible devices for the company floor, such as headsets, keyboards, printers, and even an Xbox for leisure. This can be especially helpful if there is a network connectivity issue, allowing some daily activities to continue through Wi-Fi Direct until the internet connection is restored.
- Most Wi-Fi Direct enabled devices can be connected, but some manufacturers will simplify the process and add perks for connections between devices from their brand. For example, Samsung devices that offer Wi-Fi Direct support that can be used to cast onto any enabled television and share information with any enabled device.
- However, connections between Samsung devices may require fewer steps and offer additional settings to enhance the experience for the user. Apple devices take this a step further and are designed to only allow connection with other Apple devices.
- There are ways to work around this, but they can be cumbersome and negate the convenience of Wi-Fi Direct. For this reason, businesses should take care when purchasing company devices to ensure they'll easily connect when needed.

4.8.4 Common Business Applications

Some Wi-Fi Direct applications that can help your business thrive:

- As mentioned earlier, setting up printer access through Wi-Fi Direct can ensure that off-line printing jobs can continue even when the network is down.
- Wi-Fi Direct can also be used during company meetings, allowing anyone taking the lead to cast their device onto the conference room television or send meeting files to everyone in attendance.
- Syncing company devices is also significantly faster through Wi-Fi Direct than using Bluetooth, allowing easy sharing of new company software or updating information stored within the device.
- Near-field communication can also work through Wi-Fi Direct connections.
- Offer entertainment options as perks to employees and customers.

4.8.5 Potential Drawbacks

- With all the advantages offered by Wi-Fi Direct, it's important to also consider some of the technology's limitations.
- Considering the usability of Wi-Fi Direct depends on connectivity without the use of a Wi-Fi network, the Internet of Things (IoT) expansion requires a connection complexity that Wi-Fi Direct can't keep up with. This means some interconnected devices will already require a standard Wi-Fi connection for daily operations, rendering Wi-Fi Direct all but obsolete.
- Security can also be an issue when choosing automatic connections or when a connected device is also connected to a network. Hackers can exploit weaknesses in Wi-Fi Direct devices that don't require security steps for connections or can use a network connection to gain access to other devices connected through Wi-Fi Direct. For this reason, it's important to avoid using this technology in a public space and to rely on temporary rather than automatic connections.
- Using newer Wi-Fi Direct technology can also help mitigate some of this risk by requiring more advanced steps to connect.

4.9 LI-FI

GQ. How Li-Fi work ? What is advantages and disadvantages of Li-Fi.
GQ. What is the difference between Wi-Fi and Li-Fi Technology.
GQ. Describe Li-Fi and explain Application of Li-Fi.

- **Light Fidelity (Li-Fi)** is VLC, visible light communication technology developed by research team at University of Edinburgh, including Professor Haas. Professor Harald Haas authored term. Light Fidelity is modern wireless communication technology that empowers remote transmission of data using LED light. Light Fidelity depends on novel ability of solid-state lighting systems to create 1s and 0s binary code with human-imperceptible LED illumination.

Information may be obtained within vicinity of visible light by means of electronic gadgets with photo-diode. This means that light bulbs can bring not only light but wireless connection at same time anywhere where LED's are used. Generally speaking, Wi-Fi plays an efficient role in wireless data coverage within buildings, while using Li-Fi we will provide excellent density data coverage in particular location without any radio interference issues. Li-Fi provides better latency, performance, accessibility and security than Wi-Fi, and under laboratory conditions has even reached extreme speeds greater than 1 Gbps.

4.9.1 History

- Professor Harald Haas, of University of Edinburgh, UK, is regarded as founding father of Li-Fi. The term Visible Radiation Communication (VLC) embodies any use of visible radiation portion of electromagnetic spectrum for data transmission.
- D-Light project was sponsored at Center for Digital Communications in Edinburgh from January 2010 until January 2012. Haas introduced this breakthrough in his 2011 TED Global talk, and helped advertise it. Li-Fi consortium, formed by Fraunhofer IPMS, Germany, IBSEN Telecom, Norway, Supreme Architecture, Israel / US, and TriLumina, USA, is planning to upgrade and advance different Optical Wireless Communication (OWC) technologies.
- Li-Fi technology was demonstrated at the 2012 Consumer Electronics Show in Las Vegas, employing pair of Casio smartphones to trade the data utilizing light of varying intensities emitted from their displays, noticeable up to 10 meters away.

4.9.2 Working of Li-Fi

- Light Fidelity technology is wireless communication device focused mainly on use of visible light between violet (800 THz) and red (four hundred THz). Li-Fi is based solely on propagation of information in defined and uniform fashion via amplitude modulation of light supply. There is LED transmitter (light emitting) on one end and photo detector (light sensor) on other.
- Li-Fi operates very simple and fast. The data input to LED transmitter is encoded into light by varying the flickering rate at which binary code (1s and 0s) is generated by LEDs flicker 'on' and 'off'. LED transmitter's on / off operation which seems to be invisible to human eye as speed of LEDs is less than microsecond.
- By switching ON LED is logical '1' it makes data transfer according to incoming binary codes, switching OFF is logical '0'. Data can be encoded in light by varying rate at which LEDs flicker on and off to different combinations of 1s and 0s Fig. 4.9.1.

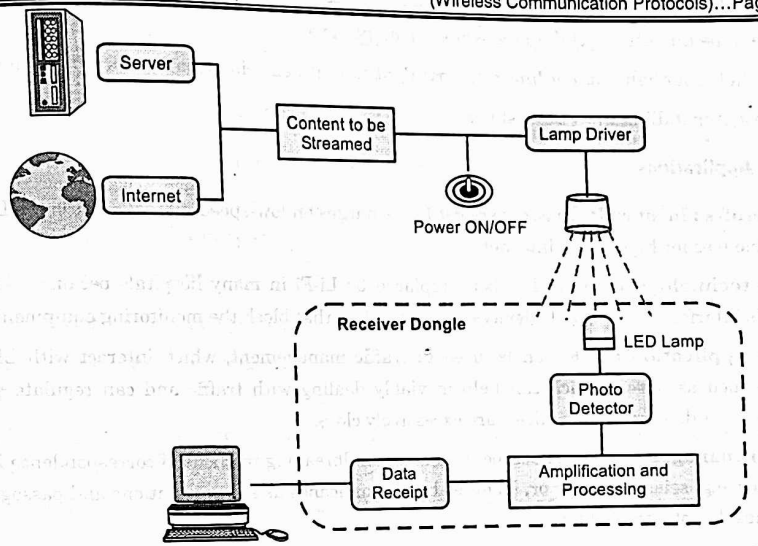


Fig. 4.9.1 : Li-Fi Working

4.9.3 Advantages

1. **Proficiency :** Energy utility can be minimised with use of LED illumination which are now accessible in home, workplaces and Mall and so on for lighting reasons. Consequently transmission of information requiring negligible additional power, which makes it efficient in terms of costs as well as energy.
2. **Cost :** Not only does Li-Fi need fewer components for its service, but it also requires only small additional capacity for data transmission.
3. **Availability :** Disponibility is not issue as light sources are available all over place. Along these lines, lights are can be utilized as model for information transmission.
4. **Security :** One principal advantage of Li-Fi is security. Since light can't go through opaque structures, Li-Fi web is accessible just to clients inside limited zone and can't be intercepted and misused, outside area under operation.
5. **High speed :** Combination of low interference, high bandwidths and high-intensity output, aids Li-Fi provides high data rates i.e., 1 Gbps or even beyond.

4.9.4 Disadvantages

1. The availability of light source is necessary for internet access. This could restrict areas and situations where Li-Fi might be used.
2. To trade data it requires close or immaculate line of sight.
3. Light waves can not penetrate walls and therefore Li-Fi has much shorter range than Wi-Fi.

4. Opaque impediments affect data transmission on pathways.
5 Normal light, sunlight, and ordinary electric light can influence information transmission speed.
6. High cost of installing the VLC systems.

4.9.5 Applications

- **In Aircrafts :** In air crafts, passengers get high-charges on low-speed internet, but using Li-Fi provides affordable fees for high-speed internet.
- **Health technologies :** WI-Fi has been replaced by Li-Fi in many hospitals because use of Wi-Fi in hospitals interferes with mobile devices and computers that block the monitoring equipment signals.
- **Traffic Application :** Li-Fi can be used in traffic management, which interact with LED lights of vehicles such as buses, which can help in viably dealing with traffic and can regulate accidents by warning other drivers when vehicles are excessively close.
- **Disaster management :** Li-Fi can be used as groundbreaking methods of correspondence in the midst of disaster, e.g. seismic tremor or, on other hand, hurricanes as subway stations and passages; common dead zones do not impede Li-Fi.
- **Power Plant application :** Li-Fi is progressively safe, bottomless availability in all regions of power plant as utilization of Wi-Fi and other radiation source isn't acceptable.

4.9.6 What is the difference between Wi-Fi and Li-Fi Technology

Wi-Fi offers highest speed access to internet among the current technology. However, if we compare Li-Fi with Wi-Fi, we find the following key differences:

	Li-Fi	Wi-Fi
Spectrum Used	Visual Light	Radio Frequency
Range	Depends on light intensity, can be lower than Wi-Fi	Less than 200 meters
Cost	High installation cost, low regular usage cost	Low cost
Security	High	Less (compared to Li-Fi)
Data transfer speed	Higher (compared to Wi-Fi, can be up to 100 times faster)	High
Availability	Yet to be available for commercial use	Widely available

4.10 SIGFOX

GQ. Explain Sigfox protocol in details.
GQ. Explain Network Architecture of Sigfox.

Sigfox is an inexpensive, reliable, low-power solution to connect sensors and devices.

With our dedicated radio-based network, we are committed to giving a voice to the physical world, and make the Internet of Things truly happen.

The Sigfox protocol focuses on:

- **Autonomy**. Extremely low energy consumption, allowing years of battery life.
- **Simplicity**. No configuration, connection request or signaling. Your device is up and running within minutes!
- **Cost efficiency**. From the hardware used in the devices to our network, we optimize every step to be as cost-effective as possible.
- **Small messages**. No large assets or media allowed on the network, only small notifications: up to 12 bytes.
- **Complementarity**. Thanks to its low cost and ease of configuration, you can also use Sigfox as a secondary solution to any other type of network, e.g.: Wi-Fi, Bluetooth, GPRS, etc.

4.10.1 Accessing the Sigfox Service

Putting your device on the Sigfox network

- Getting your device to communicate with Sigfox is very easy: everything you need is included! Our subscription service is based on the number of devices you want to connect to the network.
- If you have a device that communicates using other networks, it may already be compatible with Sigfox. If not, then Sigfox Build will take you through the steps to prototype, certify and connect it.

Subscribing to the Sigfox network

- The Sigfox network is global it is managed by local Sigfox Operators (SO).
- Contracting with an SO grants you access to the following:
  - The Sigfox public network,
  - The Sigfox Cloud, where you can see and manage all your devices on the network,
  - The Sigfox support platform, available 24/7, for easy troubleshooting while you develop your product

4.10.2 Network overview

Sigfox's network works with lightweight messages (12 bytes, excluding payload headers).The life cycle of a Sigfox message is always the same:

- A device wakes up and emits a message using its radio antenna,
- Multiple Sigfox base stations in the area receive the message,
- Base stations send the message to the Sigfox Cloud,
- The Sigfox Cloud sends the message to a customer's backend platform.

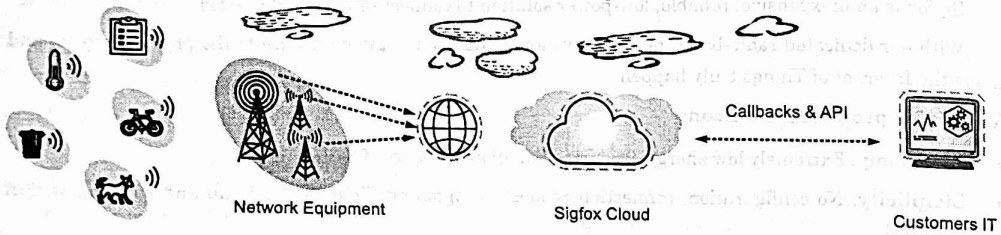


Fig. 4.10.1 : Sigfox network

What is a Sigfox "base station"?

Base stations are local Sigfox antennas, which receive messages from emitting devices and forward them to the Sigfox Cloud. They are deployed in the field by our local Sigfox Operators.

They are composed of three major elements:

- **An antenna**, to receive messages over the air, usually deployed on high points or towers,
- **A LNA or LNAC** (low-noise amplifier), to amplify the signal and filter noise,
- **An access point,** which understands the Sigfox messages and sends them to the Sigfox Cloud.

Once connected, they become part of our public network. They then start listening for all Sigfox messages sent by devices in the vicinity.

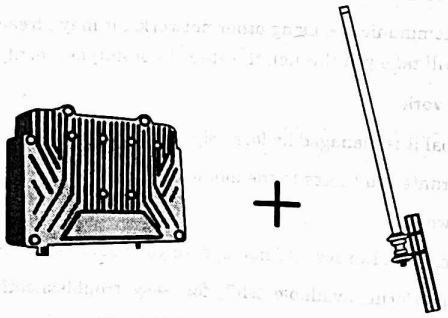


Fig. 4.10.2 : device Connection

Coverage

Sigfox is a public network, which means that devices rely on the infrastructure deployed through cities and countries by the local Sigfox Operator to communicate.

4.11 Z-WAVE

GQ. What is Z-Wave Technology ? how it works ?

- The concept of Z-Wave technology is that it uses a low-power RF radio circuitry which is embedded into home electronics devices and systems.
- Z-Wave technology is aimed at a number of wireless home automation areas including lighting, residential access control, entertainment systems and all forms of household appliances. Z-Wave can be used within a network (Home Area Network, HAN), and can therefore be used to set up all areas of home automation, possibly controlled by a single controller.
- With many more home devices becoming remotely controlled, Z-Wave technology is seen as having a large market opportunity, especially with the talk about the Internet of Things, IoT becoming more widespread.
- Z-Wave modules are available from a variety of sources relatively cheaply and therefore they provide an excellent format for home automation.
- The International Telecommunications Union, ITU has included the Z-Wave PHY and MAC layers as an option in its G.9959 standard. This defines a set of guidelines for sub-1-GHz narrowband wireless devices.

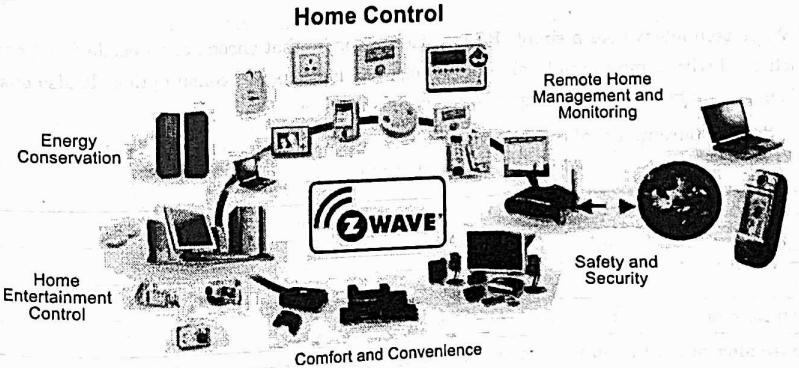


Fig. 4.11.1 : different Application of Z-Wave

4.11.1 Z-Wave Alliance

- To support and promote Z-Wave technology, and organisation known as the Z-Wave Alliance was founded. This is a consortium of manufacturers who have products int his sector. By having a common standard, the market share is increased as users are able to select products from different manufacturers to more exactly suit their needs.
- The Alliance also provides certification of products, thereby enabling standards to be maintained and user to select products they know will operate alongside each other.

4.11.2 Z-Wave technology basics

Z-Wave uses a mesh network topology and accordingly any non battery powered device acts as a signal repeater, enabling reliable connections from one node to the next. Battery powered devices do not act as repeaters as this would result in high levels of battery drain. The mesh network approach means that, the more devices in the network, the more resilient it becomes.

- the frequencies used for Z-Wave are below that of the normal 2.4 GHz Wi-Fi band and this enables better penetration of walls and other items found in all homes, but in addition to this, the mesh network means that data to be transferred can intelligently routed by the network to get around obstacles and thereby obtaining robust whole-home coverage.
- Z-Wave typically has a range of about 100 metres or 328 feet in open air. However walls and other items in the home will considerably reduce this and therefore it is recommended that the maximum device spacing Z-Wave network is around 10 metres of 30 feet. Anything closer will provide better communications.
- The Z-Wave signal can hop roughly 600 feet, and Z-Wave networks can be linked together for even larger deployments. Each Z-Wave network can support up to 232 Z-Wave devices allowing the flexibility to provide sufficient devices for a complete automated home.

4.11.3 Z-Wave RF interface

- The Z-Wave technology uses a simple RF interface to ensure that encode and decode functions are able to be achieved with a minimum level of processing, and hence power consumption. It also ensures that the RF signal can be transmitted with the maximum efficiency.
- Some of the key parameters of the Z-Wave RF interface are summarised in the Table 4.11.1.

Table 4.11.1

Z-Wave Technology Summary	
Parameter	Details
Data rate	9.6 or 40 kbit/s; speeds are fully interoperable.
Modulation scheme	GFSK Manchester channel encoding
Approximate max range	Around 30 m in almost line of site situations. Reduce range is expected within buildings.
Frequency bands	868.42 MHz SRD Band (Europe) 900 MHz ISM band: 908.42 MHz (United States) 916 MHz (Israel) 919.82 MHz (Hong Kong) 921.42 MHz (Australian/New Zealand)
Duty cycle	In Europe, the 868 MHz band has a 1% duty cycle limitation
Power save	Z-Wave units are only be active 0.1% of the time to reduce power consumption

4.11.4 Z-Wave Network layer

The Z-Wave network layer is the area of the protocol stack that controls the data exchange between the different devices, sending data over the RF or radio layer.

The network layer consists of three layers:

- ***Media Access Layer :*** Referred to as the MAC, this layer controls the basic usage of the wireless hardware. It does this in a manner that is not visible to the end user.
- ***Transport Layer :*** The transport layer within the Z-Wave technology protocol stack controls message transfer between two wireless nodes and ensures error free transmission.
- ***Routing Layer :*** The routing layer manages the Z-Wave wireless mesh capabilities. It enables the various nodes to link together and route messages from one node to another if one node is out of range of another..

4.11.5 Z-Wave devices

In order to have a hierarchy within a wireless network, various types of Z-Wave device are specified:

- ***Controller :*** As the name implies, these devices are those that control other Z-Wave devices. Controller devices are factory programmed with what is termed a Home ID. This cannot be changed by the user.
- ***Slave :*** Slave devices are those that are controlled by controllers. Slave devices do not have a pre-programmed Home ID, but instead they take the Home ID assigned to them by the Z-Wave network controller.
- ***Routing slave :*** This form of Z-Wave slave is one that knows its neighbours and has partial knowledge of routing table. It can reply to the node from which it has received the message. It can also send unsolicited messages to a number of predefined nodes to which it has routes.

4.12 LORAWAN

GQ. What is LoRa ?
GQ. What is LoRaWAN ? Elaborate LoRaWAN Network elements.
GQ. Elaborate LoRa Based Device Classes with example .

4.12.1 LoRa Introduction

- LoRa is a radio modulation technique that is essentially a way of manipulating radio waves to encode information using a chirped (chirp spread spectrum technology), multi-symbol format. LoRa as a term can also refer to the systems that support this modulation technique or the communication network that IoT applications use.
- The main advantages of LoRa are its long-range capability and its affordability. A typical use case for LoRa is in smart cities, where low-powered and inexpensive internet of things devices (typically sensors or monitors) spread across a large area send small packets of data sporadically to a central administrator.

Spreading Factor (SF)

- The chirp spread spectrum technology uses so-called "chirps," which are signals with a frequency that moves up or down (up-chirp or down-chirp respectively) at different speeds. The spreading factor (SF) determines the speed of a chirp.
- A high SF means a broadcast has higher range and penetration, at the cost of increased power consumption. A lower SF is faster and transmits more data at the same bandwidth and time.

Low Power Wide Area Networks (LPWAN)

- A low-power wide-area network (LPWAN) is a type of wireless telecommunication network that allows connected devices to have long-range communications capabilities at a low bit rate. LPWANs are typically used in asset monitoring and management in smart cities and industrial internet of things deployments. This is in contrast to wireless wide-area networks (typically used by large corporate organizations) that carry more data and use more power. Examples of LPWAN technology are Lora/LoraWAN, Sigfox, MIoTy, Wi-SUN, LTE-M, and NB-IOT.
- LPWAN technology has an operating range of up to ten kilometers, and because it is a relatively simple and lightweight protocol, the devices and hardware are relatively inexpensive. The transceivers (small battery-powered devices) also use little power, allowing them to run for up to twenty years.

4.12.2 LoRaWAN

LoRaWAN is a low-power, wide area networking protocol built on top of the LoRa radio modulation technique. It wirelessly connects devices to the internet and manages communication between end-node devices and network gateways. Usage of LoRaWAN in industrial spaces and smart cities is growing because it is an affordable long-range, bi-directional communication protocol with very low power consumption — devices can run for ten years on a small battery. It uses the unlicensed ISM (Industrial, Scientific, Medical) radio bands for network deployments.

An end device can connect to a network with LoRaWAN in two ways:

- Over-the-air Activation (OTAA): A device has to establish a network key and an application session key to connect with the network.
- Activation by Personalization (ABP): A device is hardcoded with keys needed to communicate with the network, making for a less secure but easier connection.

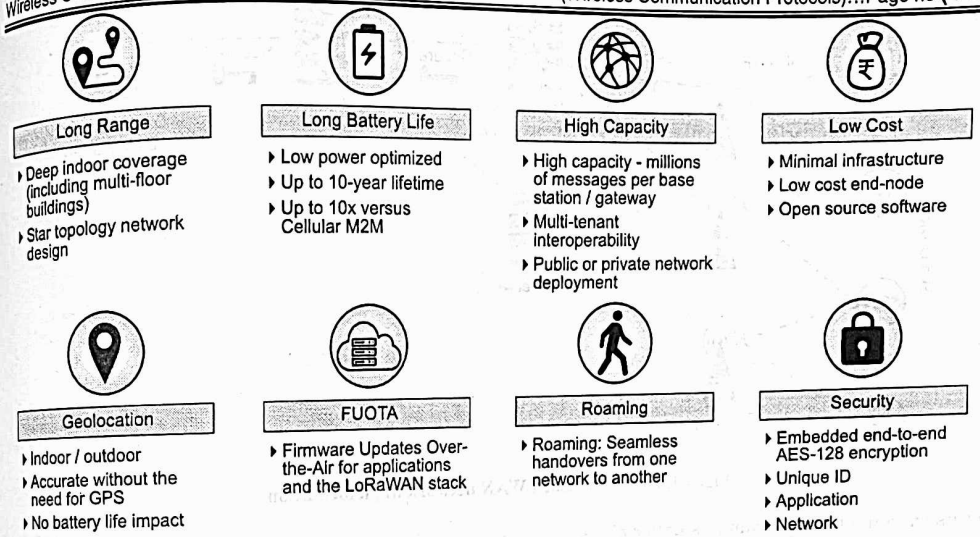


Fig. 4.12.1 : Highlights important advantages of deploying a LoRaWAN network:

4.12.3 LoRaWAN Network Fundamentals

- To fully understand LoRaWAN networks, we will start with a look at the technology stack. As shown in Fig. 4.12.2 , LoRa is the physical (PHY) layer, i.e., the wireless modulation used to create the long-range communication link.
- LoRaWAN is an open networking protocol that delivers secure bi-directional communication, mobility, and localization services standardized and maintained by the LoRa Alliance.

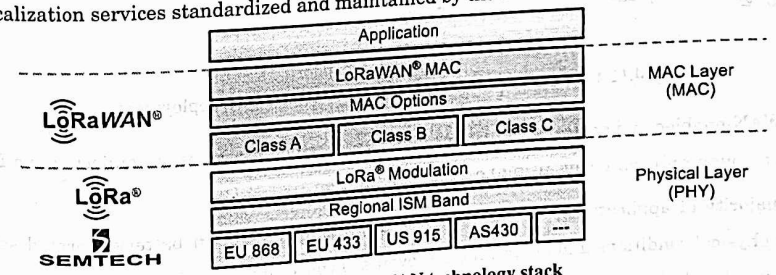


Fig. 4.12.2 : LoRaWAN technology stack

4.12.3(A) LoRaWAN Network Elements: An Introduction

Now that we have a basic understanding of LoRa, we will examine the architecture of a LoRaWAN network. Fig. 4.12.3 shows a typical LoRaWAN network implementation from end to end.

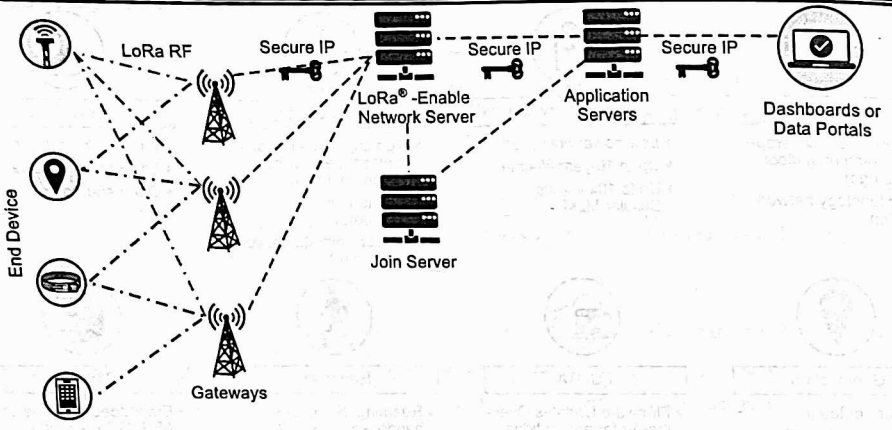


Fig. 4.12.3 : Typial LoRaWAN network implementation

Let us examine this diagram in smaller pieces.

4.12.3(B) LoRa-based End Devices

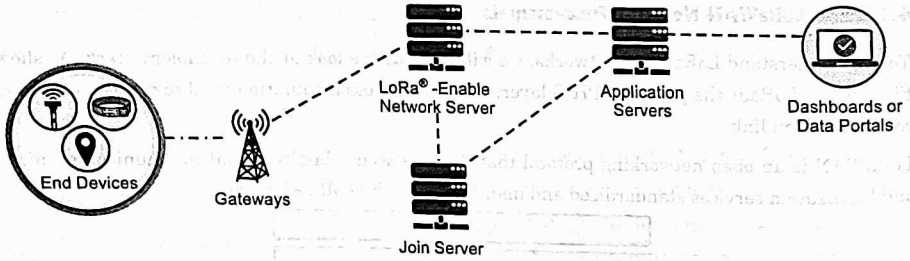


Fig. 4.12.4: End devices in a typical LoRaWAN network deployment

- A LoRaWAN-enabled end device is a sensor or an actuator which is wirelessly connected to a LoRaWAN network through radio gateways using LoRa RF Modulation.
- In the majority of applications, an end device is an autonomous, often battery-operated sensor that digitizes physical conditions and environmental events. Typical use cases for an actuator include: street lighting, wireless locks, water valve shut off, leak prevention, among others.
- When they are being manufactured, LoRa-based devices are assigned several unique identifiers. These identifiers are used to securely activate and administer the device, to ensure the safe transport of packets over a private or public network and to deliver encrypted data to the Cloud.

4.12.3(C) LoRaWAN Gateways

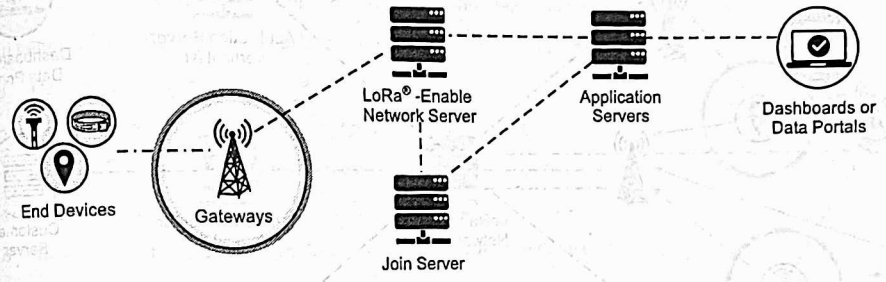


Fig. 4.12.5: Gateways in a typical LoRaWAN network deployment

- A LoRaWAN gateway receives LoRa modulated RF messages from any end device in hearing distance and forwards these data messages to the LoRaWAN network server (LNS), which is connected through an IP backbone.
- There is no fixed association between an end device and a specific gateway. Instead, the same sensor can be served by multiple gateways in the area. With LoRaWAN, each uplink packet sent by the end-device will be received by all gateways within reach, as illustrated in Fig. 4.12.5. This arrangement significantly reduces packet error rate (since the chances that at least one gateway will receive the message are very high), significantly reduces battery overhead for mobile/nomadic sensors, and allows for low-cost geolocation (assuming the gateways in question are geolocation-capable).
- The IP traffic from a gateway to the network server can be backhauled via Wi-Fi, hardwired Ethernet or via a Cellular connection. LoRaWAN gateways operate entirely at the physical layer and, in essence, are nothing but LoRa radio message forwarders. They only check the data integrity of each incoming LoRa RF message. If the integrity is not intact, that is, if the CRC is incorrect, the message will be dropped. If correct the gateway will forward it to the LNS, together with some metadata that includes the receive RSSI level of the message as well as an optional timestamp.
- For LoRaWAN downlinks, a gateway executes transmission requests coming from the LNS without any interpretation of the payload. Since multiple gateways can receive the same LoRa RF message from a single end device, the LNS performs data de-duplication and deletes all copies. Based on the RSSI levels of the identical messages, the network server typically selects the gateway that received the message with the best RSSI when transmitting a downlink message because that gateway is the one closest to the end device in question.

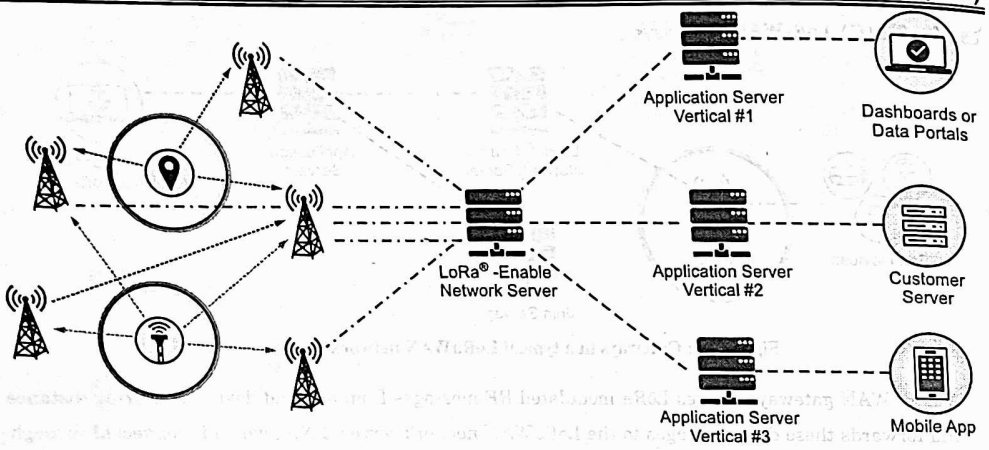


Fig. 4.12.6 : Gateways receiving and transmitting messages from end devices

- Furthermore, LoRa allows for scalable, cost-optimized gateway implementation, depending on deployment objectives. For example, in North America, 8-, 16-, and 64-channel gateways are available.
- The 8-channel gateways are the least expensive. The type of gateway needed will depend on the use case. Eight- and 16-channel gateways are available for both indoor and outdoor use. Sixty-four channel gateways are only available in a carrier-grade variant. This type of gateway is intended for deployment in such places as cell towers, the rooftops of very tall buildings, etc.

4.12.3(D) Network Server

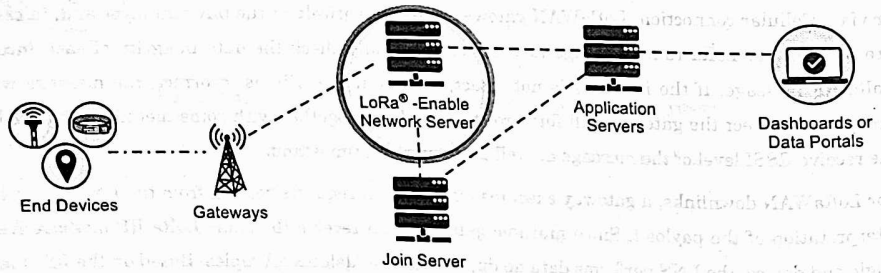


Fig. 4.12.7 : LoRaWAN Network Server in a typical LoRaWAN network deployment

- The LoRaWAN network server (LNS) manages the entire network, dynamically controls the network parameters to adapt the system to ever-changing conditions, and establishes secure 128-bit AES connections for the transport of both the end to end data (from LoRaWAN end device to the end users Application in the Cloud) as well as for the control of traffic that flows from the LoRaWAN end device to the LNS (and back).

- The network server ensures the authenticity of every sensor on the network and the integrity of every message. At the same time, the network server cannot see or access the application data.
- In general, all LoRaWAN network servers share the following features:
  - Device address checking
  - Frame authentication and frame counter management
  - Acknowledgements of received messages
  - Adapting data rates using the ADR protocol
  - Responding to all MAC layer requests coming from the device,
  - Forwarding uplink application payloads to the appropriate application servers
  - Queuing of downlink payloads coming from any Application Server to any device connected to the network
  - Forwarding Join-request and Join-accept messages between the devices and the join server

4.12.3(E) Application Servers

Application servers are responsible for securely handling, managing and interpreting sensor application data. They also generate all the application-layer downlink payloads to the connected end devices.

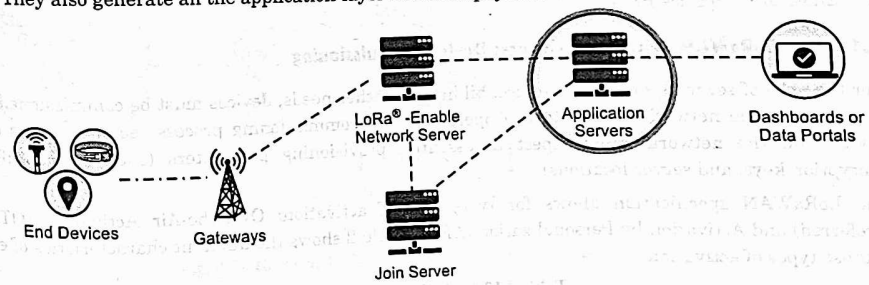


Fig. 4.12.8 : LoRaWAN Application Server in a typical LoRaWAN network deployment

4.12.3(F) Join Server

- The join server manages the over-the-air activation process for end devices to be added to the network.
- The join server contains the information required to process uplink *join-request* frames and generate the downlink *join-accept* frames. It signals to the network server which application server should be connected to the end-device, and performs the network and application session encryption key derivations.
- It communicates the Network Session Key of the device to the network server, and the Application Session Key to the corresponding application server

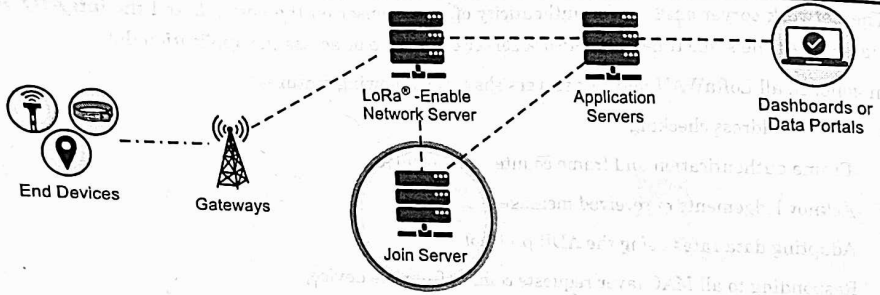


Fig. 4.12.9 : LoRaWAN Join Server in a typical LoRaWAN network deployment

- For that purpose, the join server must contain the following information for each end-device under its control:
  - DevEUI (end-device serial unique identifier)
  - AppKey (application encryption key)
  - NwkKey (network encryption key)
  - Application Server identifier
  - End-Device Service Profile

4.12.4 LoRaWAN Network Elements: Device Commissioning

- For the sake of security, quality of service, billing, and other needs, devices must be commissioned and activated on the network at the start of operation. The commissioning process securely aligns each device and the network with respect to essential provisioning parameters (such as identifiers, encryption keys, and server locations)
- The LoRaWAN specification allows for two types of activation: Over-the-Air Activation (OTAA) (preferred) and Activation by Personalization (ABP). Table 2 shows the different characteristics of each of these types of activation.

Table 4.12.1 : Activation Types

Over-the-Air Activation (OTAA)	Activation by Personalization (ABP)
• Device manufacturers autonomously generate essential provisioning parameters	• A simplified (less secure) commissioning process
• Secure keys (session-long and derived) can be renewed regularly	• IDs and Keys are personalized at fabrication
• Devices can store multiple "identities" to dynamically and securely switch networks and operators during its lifetime	• Devices become immediately functional upon powering up; the Join procedure is skipped
• High-grade, tamper-proof security options are available	• Devices are tied to a specific network/service; the NetID is a portion of the device network address

4.12.5 LoRaWAN Network Elements: Security

There are two key elements to the security of a LoRaWAN network: the *join procedure* and *message authentication*. The join procedure establishes mutual authentication between an end device and the LoRaWAN network to which it is connected. Only authorized devices are allowed to join the network. LoRaWAN MAC and application messages are origin-authenticated, integrity-protected and encrypted end-to-end (i.e., from end device to the application server and vice versa).

These security features ensure that:

- Network traffic has not been altered
- Only legitimate devices are connected to the LoRaWAN network
- Network traffic cannot be listened to (no eavesdropping)
- Network traffic cannot be captured and replayed

With that foundation, we will take a look at the LoRaWAN security measures in more detail.

4.12.5(A) The Join Procedure

- We will begin with the security keys, as illustrated in Fig. 4.12.10. Individual root keys are securely stored on the end devices, and matching keys are securely stored on the join server.

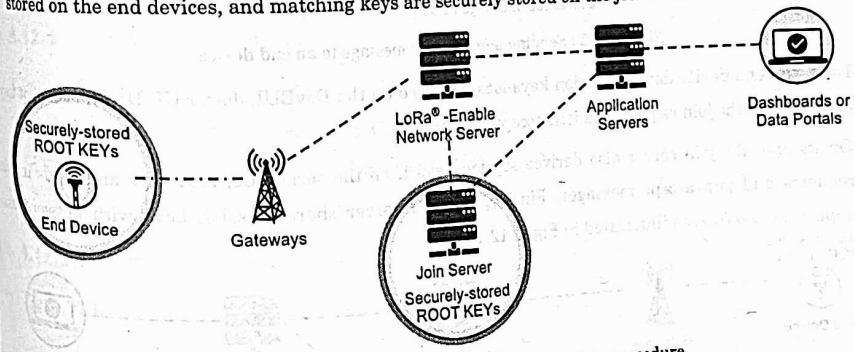


Fig. 4.12.10: Security keys generated during the Join procedure

- The end device sends a *join request* message to the join server, as illustrated in Fig. 4.12.11.

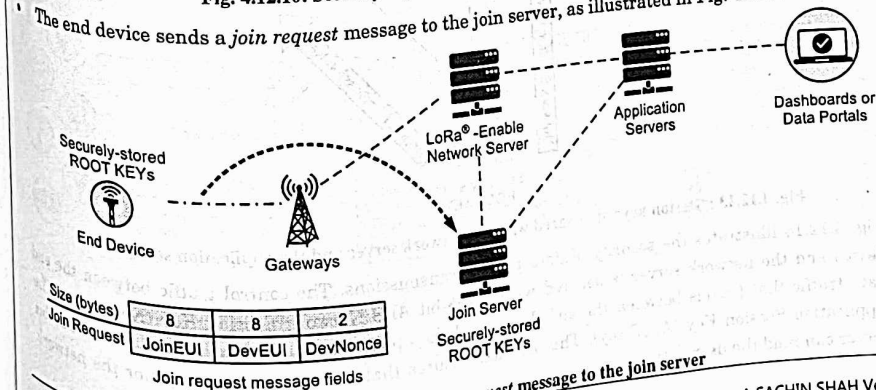


Fig. 4.12.11 : Sending a *join request* message to the join server

- After the join server authenticates the device requesting to join the network, it returns a *join accept* message to the device, as illustrated in Fig. 4.12.12.

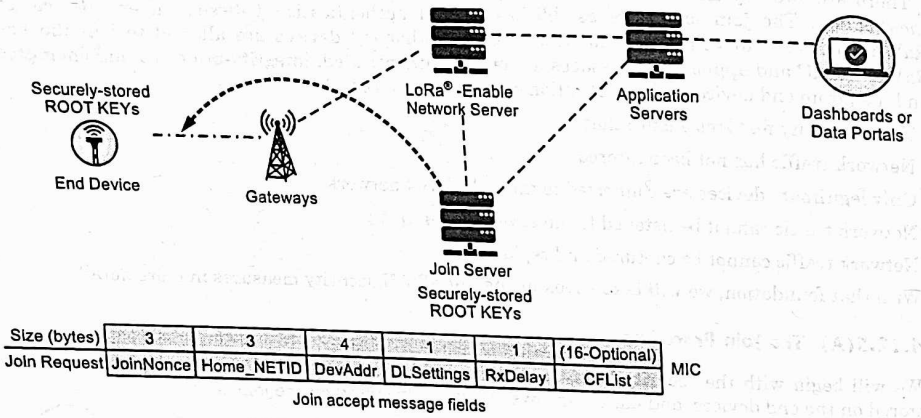


Fig. 4.12.12 : Sending a *join accept* message to an end device

- Next, the end device derives session keys locally, based on the DevEUI, Join EUI, DevNonce, root keys and fields in the join request and join accept messages.
- On its end, the join server also derives session keys from the serial IDs, root keys and fields in join requests and join accept messages. Finally, the join server shares session keys with network and application servers, as illustrated in Fig. 4.12.13.

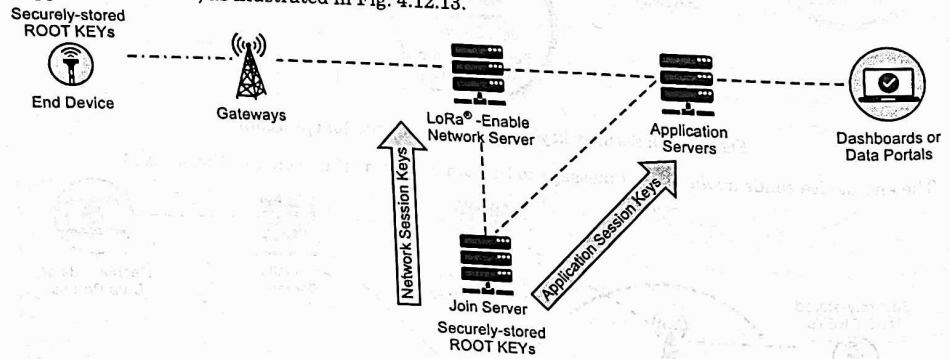


Fig. 4.12.13 : Session keys are shared with the network server and the application server

- Fig. 4.12.14 illustrates the security of data packet transmissions. The control traffic between the end device and the network server is secured with a 128-bit AES Network Session Key (NwkSKey). The data traffic that travels between the end device and the application server, is secured with a 128-bit Application Session Key (AppSKey). This method ensures that neither the gateway nor the network server can read the user data.

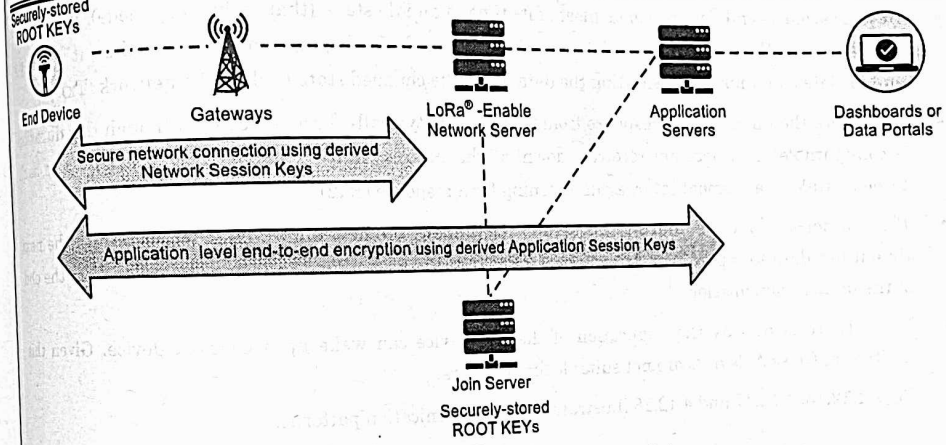


Fig. 4.12.14 : Secure transmission of data packets

4.12.6 Device Classes: A, B and C

- LoRa-based end devices may operate in one of three modes, depending on their device class. All such devices must support Class A operation. Class B devices must support both Class A and Class B modes, and Class C devices must support all three modes of operation.
- These modes of operation have to do with how the devices communicate with the network.

4.12.6(A) Class A Devices

- Fig. 4.12.15 shows how the Class A mode of operation works.

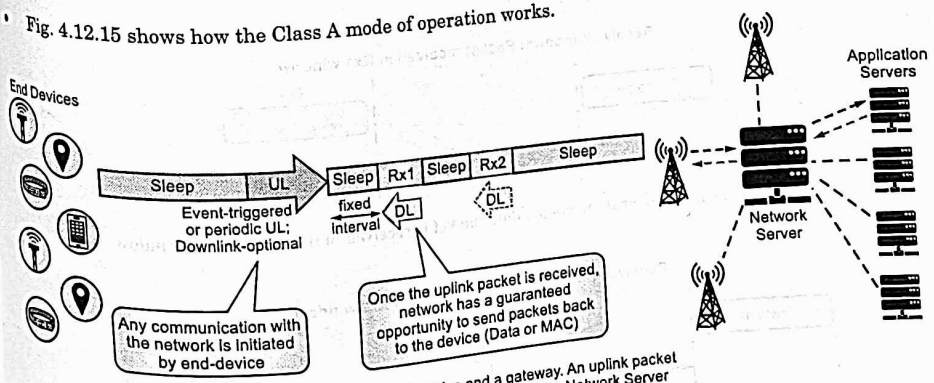


Fig. 4.12.15 : Class A operation

- In this case, the end device spends most of its time in an idle state, (that is, in sleep mode). When there is a change in the environment related to whatever the device is programmed to monitor, it wakes up and initiates an uplink, transmitting the data about the changed state back to the network (Tx).
- The device then listens for a response from the network, typically for one second (although this duration is configurable). If it does not receive a downlink during this *receive window* (Rx1), it briefly goes back to sleep, waking a moment later, again listening for a response (Rx2).
- If no response is received during this second Rx window, the device goes back to sleep until the next time it has data to report. The delay between Rx1 and Rx2 is conFig.d in terms of a delay from the end of the uplink transmission.
- Note: There is no way the application of the end device can wake up a Class A device. Given this limitation, Class A devices are not suitable for actuators.
- Fig.s 4.12.16, 4.12.17 and 4.12.18 illustrate these communication patterns.

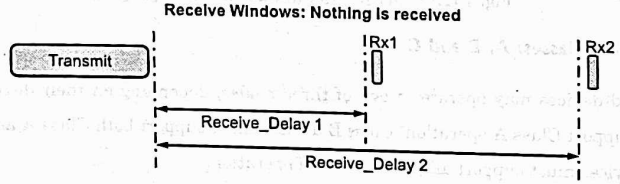


Fig. 4.12.16 : Class A operation when nothing is received

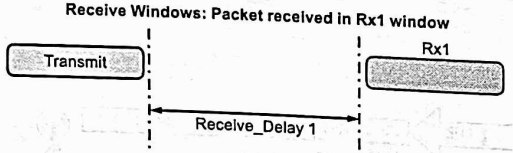


Fig. 4.12.17 : Class A operation when a data packet is received in the first receive window

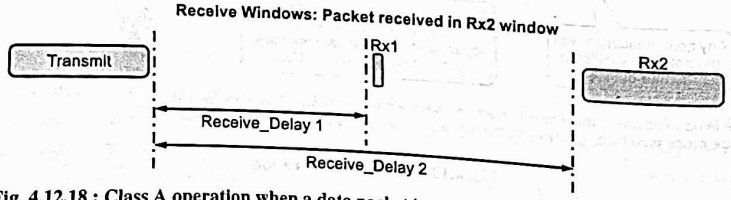


Fig. 4.12.18 : Class A operation when a data packet is received in the second receive window

Note : A device will not try to send another uplink message until either:

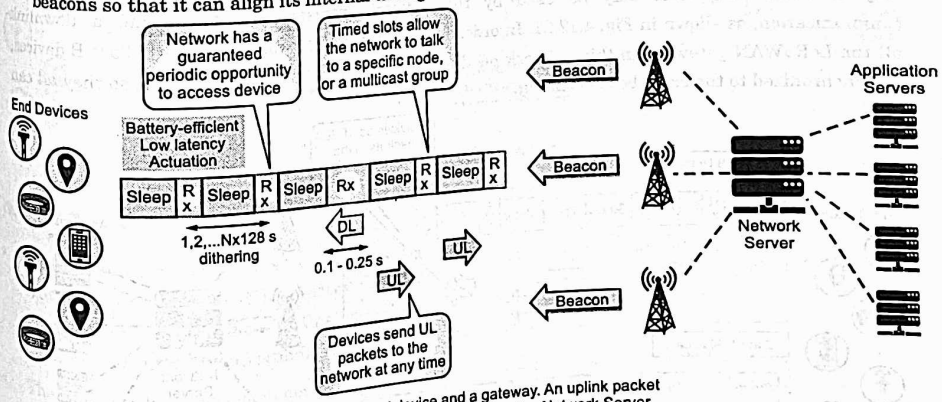
1. It has received a downlink message during Rx1, or
2. The second receive window following the last transmission is complete

4.12.6(B) Class B Devices

- An enhancement of Class A, LoRaWAN Class B mode offers regularly-scheduled, fixed-time opportunities for an end device to receive downlinks from the network, making Class B end devices suitable for both monitoring sensors as well as actuators. All LoRa-based end devices start in Class A mode; however, devices programmed with a Class B stack during manufacturing may be switched to Class B mode by the application layer.
- End devices in Class B mode provide for regularly-scheduled receive windows, in addition to those that open whenever a Class A-style uplink is sent to the server.

Class B Beacons

- For the Class B mode of communication to work, a process called *beaconing* is required. During the beaconing process, a time-synchronized beacon must be broadcast periodically by the network via the beaconing process, a time-synchronized beacon must be broadcast periodically by the network via the gateways, as illustrated in Fig. 4.12.19. The end device must periodically receive one of these network beacons so that it can align its internal timing reference with the network.



There is no fixed association between an end device and a gateway. An uplink packet will be processed by all gateway within range and forwarded to the Network Server

Fig. 4.12.19 : Class B beaconing operations

- Devices use beacons to derive and align their internal clocks with the network. Devices do not need to process every beacon if the device is already aligned.
- In most cases, realigning several times a day is sufficient, with a minimal impact on battery life, as illustrated in Fig. 4.12.20.

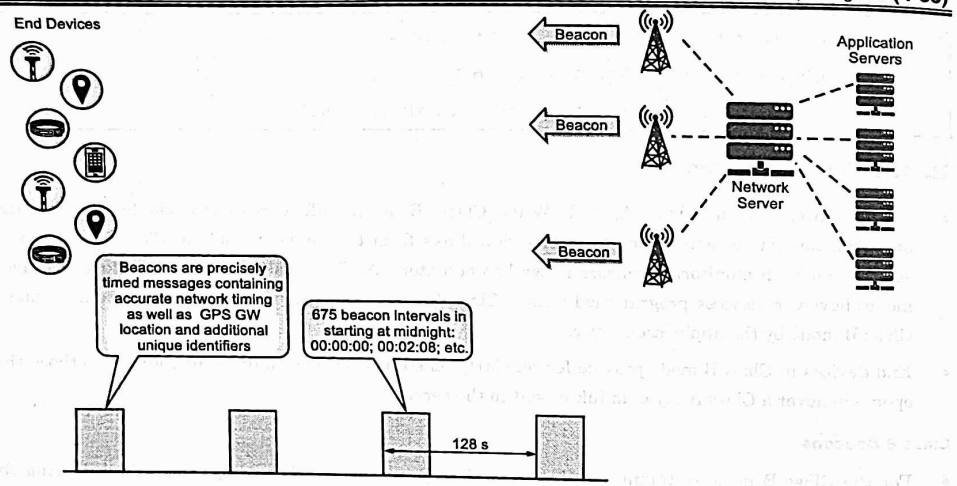


Fig. 4.12.20 : Periodic Class B beaconing for device synchronization

- Based on the beacon's timing reference, end devices can open receive windows (*ping slots*) periodically. Any of these ping slots may be used by the network infrastructure to initiate a downlink communication, as shown in Fig. 4.12.21. In order for a LoRaWAN network to support Class B devices, all the LoRaWAN gateways in this network need to have a built-in GPS timing source, so they all can be synchronized to the exact beacon timing.

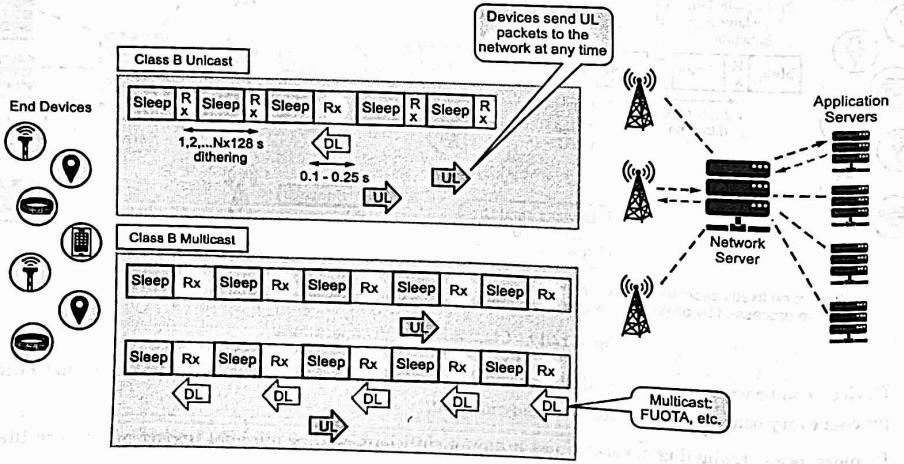


Fig. 4.12.21 : Class B ping slots

Note : Class B devices can also operate in Class A mode.

4.12.6(C) Class C Devices

- Class C are always "on"; that is, they do not depend on battery power. Class C devices include such things as street lights, electrical meters etc. These devices are always listening for downlink messages, unless they are transmitting an uplink. As a result, they offer the lowest latency for communication from the server to an end device.
- Class C end devices implement the same two receive windows as Class A devices, but they do not close the Rx2 window until they send the next transmission back to the server. Therefore, they can receive a downlink in the Rx2 window at almost any time.
- A short window at the Rx2 frequency and data rate is also opened between the end of the transmission and the beginning of the Rx1 receive window, as illustrated in Fig. 4.12.22.

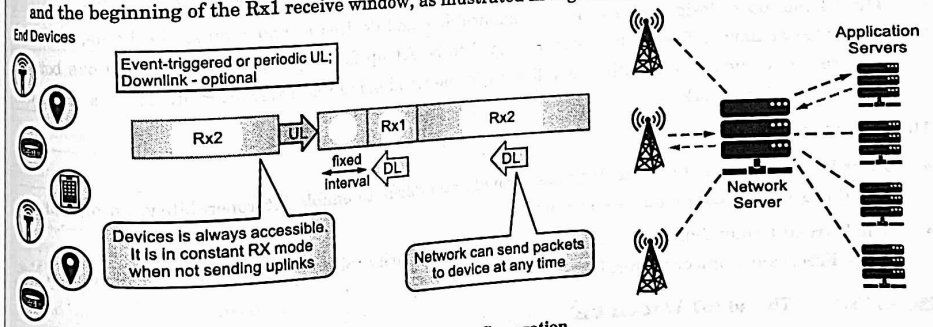


Fig. 4.12.22: Class C operation

4.12.7 The LoRa Alliance

- With more than 500 member companies, the LoRa Alliance is one of the fastest-growing technology alliances. A community of innovators, the LoRa Alliance is committed to standardizing low power wide area networks (LPWANs). To this end, the group provides the LoRaWAN Specification (https://lora-alliance.org/search/specification) free of charge.
- The specification is based on open standards and provides for certified interoperability.

4.13 THREAD (BASED ON IEEE 802.15.4)

What is Thread : IEEE 802.15.4 ? Explain in details.

- **IEEE 802.15.4** is an IPv6-based networking protocol designed for low-power Internet of Things devices in an IEEE 802.15.4-2006 wireless mesh network, commonly called a Wireless Personal Area Network (WPAN). Thread is independent of other 802.15 mesh networking protocols, such a ZigBee, Z-Wave, and Bluetooth LE.

- Thread's primary features include:
  - **Simplicity :** Simple installation, start up, and operation
  - **Security :** All devices in a Thread network are authenticated and all communications are encrypted
  - **Reliability :** Self-healing mesh networking, with no single point of failure, and spread-spectrum techniques to provide immunity to interference
  - **Efficiency :** Low-power Thread devices can sleep and operate on battery power for years
  - **Scalability :** Thread networks can scale up to hundreds of devices
- Thread is a wireless networking protocol using IP data transfer.
- Thread wireless connectivity has been developed specifically to support the Internet of Things, IoT, and as a result, it incorporates many features that have not been available in previous standards.
- Thread has been designed for consumer applications and devices in and around the home, To enable this to be achieved, Thread has been designed to be set up for easy and secure connections between hundreds of devices to each other and directly to the cloud using real Internet Protocols in a low-power, wireless mesh network.

Thread Group

- In order to promote the technology and provide standards to enable interoperability, an organisation called the Thread Group has been set up.
- The Thread Group founding members include: Yale Security, Silicon Labs, Samsung Electronics, Nest Labs, Freescale Semiconductor, Big Ass Fans and ARM.

4.13.1 Thread IoT Wireless Basics

- Thread has been designed to enable IPv6 data to be carried, a facility that other similar networking technologies cannot currently accommodate.Thread is builds upon proven wireless standards including IEEE 802.15.4 and 6LoWPAN. It has been tailored to suit low power operation - a capability that is becoming increasingly important for IoT applications.
- Thread IoT technology can also securely connect up to 250 devices in a wireless mesh network that includes direct Internet and cloud access for every device. In this way, Thread builds on existing standards, while also extending the capability.

4.13.2 Thread IoT Advantages

Thread wireless connectivity offers a number of key advantages:

1. **Security :** Security is a key issue for the Internet of Things. With hacking becoming more sophisticated devices on the Internet of Things need to be very securely protected. Thread uses banking class encryption to close the security loop-holes found in many previous standards.

2. **Simplicity :** Ease of use and simplicity for the end user were key requirements in the development of the Thread IoT standard. The systems allows for easy connection of devices using from tablets, smartphones and the like.
3. **Low power :** With users not wanting to maintain the charge of batteries within their devices, The Thread IoT concept has been designed so that devices are able to operate at extremely low power levels.
4. **Reliability :** Thread wireless connectivity has been designed to provide reliable communications to many devices. Reliability was a key concept in its design.

4.13.3 Thread IoT Summary

The Thread IoT standard features a number of specification Table 4.13.1 :

Table : 4.13.1

Thread IoT Standard Key Points	
Parameter	Details
Addressability	Direct addressability to all devices - device to device or device to cloud
Scalability	Scalable to 250-300 devices in a home
Latency	< 100 milliseconds for typical interactions
Interface	Allow the use of multiple border routers
Battery operation	Battery operated devices have years of expected life, e.g. door locks, security sensors etc
Thread physical layer standard	IEEE 802.15.4 (2006)
IEEE 802.15.4 MAC (including MAC security)	IEEE 802.15.4 (2006)

4.13.4 IEEE 802.15.4 Basics

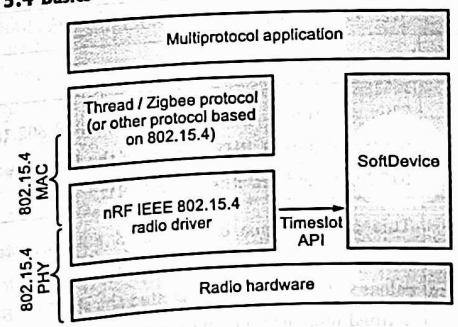


Fig. 4.13.1 : IEEE 802.15.4 radio driver architecture

- IEEE 802.15.4 is a standard that was developed to provide a framework and the lower layers in the OSI model for low cost, low power wireless connectivity networks.
- IEEE 802.15.4 provides provides the MAC and PHY layers, leaving the upper layers to be developed for specific higher later standards like Thread, Zigbee, 6LoWPAN and many others.
- As a result, IEEE 802.15.4 does not take the limelight in the way that other standards might, but nevertheless it forms the basis for a large number of standards and accordingly it ifs far more widely deployed than may be apparent at first sight.
- Low power is one of the key elements of 802.15.4 as it is used in many areas where remote sensors need to operate on battery power, possibly for years without attention.
- The IEEE 802.15.4 standard is aimed at providing the essential lower network layers for a wireless personal area network, WPAN. The chief requirements are low-cost, low-speed ubiquitous communication between devices.
- IEEE 802.15.4 does not aim to compete with the more commonly used end user-oriented systems such as IEEE 802.11 where costs are not as critical and higher speeds are demanded and power may not be quite as critical. Instead, IEEE 802.15.4 provides for very low cost communication of nearby devices with little to no underlying infrastructure.
- The concept of IEEE 802.15.4 is to provide communications over distances up to about 10 metres and with maximum transfer data rates of 250 kbps. Anticipating that cost reduction will require highly embedded device solutions, the overall concept of IEEE 802.15.4 has been devised to accommodate this.

4.13.5 IEEE 802.15.4 standard

The IEEE 802.15.4 standard has undergone a number of releases. In addition to this there are a number of variants of the IEEE 802.15.4 standard to cater for different forms of physical layer, etc. These are summarised below in the table 4.13.2.

Table 4.13.2

IEEE 802.15.4 Standard Summary	
IEEE 802.15.4 Version	Details and comments
IEEE 802.15.4 - 2003	This was the initial release of the IEEE 802.15.4 standard. It provided for two different PHYs - one for the lower frequency bands of 868 and 915 MHz, and the other for 2.4 GHz.
IEEE 802.15.4 - 2006	This 2006 release of the IEEE 802.15.4 standard provided for an increase in the data rate achievable on the lower frequency bands. This release of the standard updated the PHY for 868 and 915 MHz. It also defined four new modulation schemes that could be used - three for the lower frequency bands, and one for 2.4 GHz.

IEEE 802.15.4 Standard Summary	
IEEE 802.15.4a	This version of the IEEE 802.15.4 standard defined two new PHYs. One used UWB technology and the other provided for using chirp spread spectrum at 2.4 GHz.
IEEE 802.15.4c	Updates for 2.4 GHz, 868 MHz and 915 MHz, UWB and the China 779-787 MHz band.
IEEE 802.15.4d	2.4 GHz, 868 MHz, 915 MHz and Japanese 950 - 956 MHz band.
IEEE 802.15.4e	This release defines MAC enhancements to IEEE 802.15.4 in support of the ISA SP100.11a application.
IEEE 802.15.4f	This will define new PHYs for UWB, 2.4 GHz band and also 433 MHz
IEEE 802.15.4g	This will define new PHYs for smart neighbourhood networks. These may include applications such as smart grid applications for the energy industry. It may include the 902 - 928 MHz band.

Although new versions of the standard are available for use by any of the higher layer standards, Zigbee still uses the initial 2003 release of the IEEE 802.15.4 standard.

4.13.6 IEEE 802.15.4 applications

The IEEE 802.15.4 technology is used for a variety of different higher layer standards. In this way the basic physical and MAC layers are already defined, allowing the higher layers to be provided by individual system in use.

IEEE 802.15.4 Derived Standards	
Application or system	Description of the IEEE 802.15.4 application or system
Zigbee	Zigbee is supported by the Zigbee Alliance and provides the higher levels required for low powered radio system for control applications including lighting, heating and many other applications.
Wireless HART	WirelessHART is an open-standard wireless networking technology that has been developed by HART Communication Foundation for use in the 2.4 GHz ISM band. The system uses IEEE802.15.4 for the lower layers and provides a time synchronized, self-organizing, and self-healing mesh architecture.
RF4CE	RF4CE, Radio Frequency for Consumer Electronics has amalgamated with the Zigbee alliance and aims to provide low power radio controls for audio visual applications, mainly for domestic applications such as set to boxes, televisions and the like. It promises enhanced communication and facilities when compared to existing controls.
MiWi	MiWi and the accompanying MiWi P2P systems are designed by Microchip

IEEE 802.15.4 Derived Standards	
	Technology. They are designed for low data transmission rates and short distance, low cost networks and they are aimed at applications including industrial monitoring and control, home and building automation, remote control and automated meter reading.
ISA100.11a	This standard has been developed by ISA as an open-standard wireless networking technology and is it described as a wireless system for industrial automation including process control and other related applications.
6LoWPAN	This rather unusual name is an acronym for "IPv6 over Low power Wireless Personal Area Networks" It is a system that uses the basic IEEE 802.15.4, but using packet data in the form of Ipv6.

While the IEEE 802.15.4 standard may not be as well known as some of the higher level standards and systems such as Zigbee that use IEEE 802.15.4 technology as the underpinning lower levels system, it is nevertheless very important. It spans a variety of different systems, and as such provides a new approach - providing only the lower layers, and allowing other systems to provide the higher layers which are tailored for the relevant application.

4.13.7 IEEE 802.15.4 Frequencies and Frequency Bands

The IEEE 802.15.4 frequency bands align with the licence free radio bands that are available around the globe. Of the bands available, the 2.4 GHz (2 400 MHz) band is the most widely used in view of the fact that it is available globally and this brings many economies of scale.

IEEE 802.15.4 RF Channel Details			
Frequency band (MHz)	**Channels available**	**Throughput available (kbps)**	**Region use allowable**
868 - 868.6	1	20	Europe
902 - 928	10 (2003 rel)30 (2006 rel)	30	USA
2 400	16	250	Global

With new allocations arising as a result of issues such as the digital dividend and other countries adopting and using IEEE 802.15.4, other frequencies and bands are being considered. These include: 314-316 MHz, 430-434 MHz, and 779-787 MHz frequency bands in China and the 950 MHz-956 MHz band in Japan. Other frequencies are also being considered for UWB variants of IEEE 802.15.4.

4.13.8 IEEE 802.15.4 Modulation Formats

- There were two different modulation schemes defined for IEEE 802.15.4 in the original standard released in 2003. Both these air interface or radio interface configurations are based on direct sequence spread spectrum, DSSS techniques. The one for the lower frequency bands provides a lower data rate in view if the smaller channel width, whereas the format used at 2.4 GHz enables data to be transferred at rates up to 250 kbps.
- The 2006 release of the 802.15.4 standard upgraded an number of areas of the air interface and the modulation schemes. There were four different physical layers that were defined. Three used the DSS approach using either binary or offset quadrature phase shift keying, BPSK and OQPSK. An optional physical layer approach was defined using amplitude sift keying, ASK.

IEEE 802.15.4 MAC overview

The purpose of the IEEE 802.15.4 MAC layer is to provide an interface between the PHY or physical layer and the application layer. The as IEEE 802.15.4 does not specify an application layer, this is generally an application system such as Zigbee, RF4CE, MiWi, etc.

The IEEE 802.15.4 MAC provides the interface to the application layer using two elements:

- ***MAC Management Service :*** This is called the MAC Layer Management Entity, MLME. It provides the service interfaces through which layer management functions may be called or accessed. The IEEE 802.15.4 MAC MLME is also responsible for controlling a database of objects for the MAC layer. This database is referred to as the MAC layer PAN information base or PIB. The MLME also has access to MCPS services for data transport activities.
- ***MAC Data Service :*** This si called the MAC Common Port Layer, MCPS. This entity within the IEEE 802.15.4 MAC provides data transport services between the peer MACs.

4.13.9 IEEE 802.15.4 Network Topologies

- There are two main forms of network topology that can be used within IEEE 802.15.4. These network topologies may be used for different applications and offer different advantages.
- The two IEEE 802.15.4 network topologies are:
  - ***Star topology :*** As the name implies the start format for an IEEE 802.15.4 network topology has one central node called the PAN coordinator with which all other nodes communicate.
  - ***Peer to Peer network topology :*** In this form of network topology, there is still what is termed a PAN coordinator, but communications may also take place between different nodes and not necessarily via the coordinator.
- It is worth defining the different types of devices that can exist in a network. There are three types:
  - ***FFD :*** Full Function Device - a node that has full levels of functionality. It can be used for sending and receiving data, but it can also route data from other nodes.
  - ***RFD :*** Reduced Function Device - a device that has a reduced level of functionality. Typically it is

an end node which may be typically a sensor or switch. RFDs can only talk to FFDs as they contain no routing functionality. Thee devices can be very low power devices because they do not need to route other traffic and they can be put into a sleep mode when they are not in use. These RFDs are often known as child devices as they need other parent devices with which to communicate.

- ***Coordinator :*** This is the node that controls the IEEE 802.15.4 network. This is a special form of FFD. In addition to the normal FFD functions it also sets the IEEE 802.15.4 network up and acts as the coordinator or manager of the network.

- These definitions were originally generated for use in Zigbee, but their use has now been introduced with IEEE 802.15.4 network terminology.

IEEE 802.15.4 star topology

- In the star topology, all the different nodes are required to talk only to the central PAN coordinator. Even if the nodes are FFDs and are within range of each other, in a star network topology, they are only allowed to communicate with the coordinator node.
- Having a star network topology does limit the overall distances that can be covered. It is limited to one hop.

IEEE 802.15.4 peer to peer topology

- A peer to peer, or p2p network topology provides a number of advantages over a star network topology. In addition to communication with the network coordinator, devices are also able to communicate with each other. FFDs are able to route data, while the RFDs are only able to provide simple communication.
- The fact that data can be routed via FFD nodes means that the network coverage can be increased. Not only can overall distances be increased, but nodes masked from the main network coordinator can route their data via another FFD node that it may be able to communicate with.

4.14 RTWI-FI

- Real-Time WiFi (RT-WiFi) which is a real-time high speed wireless communication protocol. At the very bottom, RT-WiFi adopts physical layer of Wi-Fi in order to support high data rate. On top of that, we are hacking MAC (medium ac- cess control) layer of Wi-Fi to adopt TDMA (Time Division explore the channel diversity.

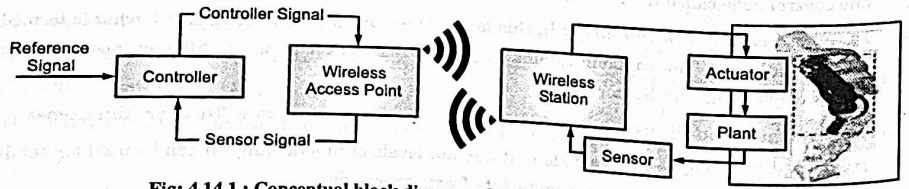


Fig: 4.14.1 : Conceptual block diagram of the human rehabilitation system

- Fig. 4.14.1 shows the architecture of a wire-free human rehabilitation system at local site. The wireless station and the access point here are Linux boxes, each equipped with Atheros AR9285 Wi-Fi card. The dura- tion of each time slot is set as 500μs, so that we can achieve a data rate of 2kHz which is sufficient for a wide range of wireless control applications.
- In order to provide reli- able communication, RT-WiFi utilizes channel hopping and channel blacklists mechanisms to avoid interference, and it supports acknowledgment and retransmission to further improve reliability.
- Moreover, since the sensors and actuators in WCSs are usually attached at battery-powered mobile devices, RT-WiFi takes an energy-efficient design by turning on its wireless radio only in time slots when transmitting or receiving is scheduled, and it aggressively puts devices in power saving mode to minimize energy consumption.
- With the design goal to support reliable, real-time, and high speed communication, we envision RT-WiFi can serve as an ideal platform to high speed WCSs. By adjusting the data rate of RT-WiFi, our wireless platform can support a wide range of WCSs and achieve good balance among sampling rate, reliability, and energy efficiency.

4.15 RTCP

Real-time Transport Protocol (RTP)

GQ. Explain Real-Time Transport Protocol (RTP)

Real-time Transport Protocol (RTP) allows only that type of message, which carries data from the source to the destination. But in some cases, we need some other type of messages in a session. The messages that can control the transmission and quality of data as well as also allow the recipients so that they can send feedback to the source or sources. A protocol designed for this purpose, which is known as Real-time Transport Control Protocol (RTCP).

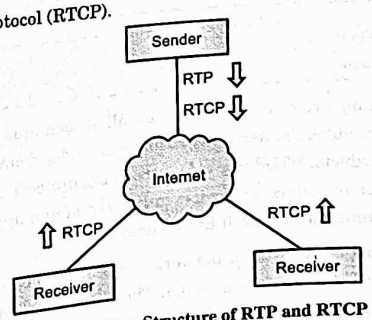


Fig. 4.15. 1: Flow Structure of RTP and RTCP

The above diagram shows the flow structure of RTP and RTCP protocol.

RTCP has five types of messages that are given below:

1. **Sender Report :** The sender report is sent after a fixed interval by the active sender in a conference to report transmission as well as statistics of reception for all RTP packets transmitted during the time period. The report sent by the sender contains the detail of absolute time-stamp, that is the number of seconds elapsed since midnight on January 1, 1970. After receiving the RTP messages by the receiver, these details of absolute timestamps helps the receiver for synchronization process. And this is very much important in audio video transmission for fing the relative timestamp.
2. **Receiver Report :** Passive participants are those participants that do not send RTP packets, and for them the Receiver report is used. This report is used to informs the sender and other receivers about the quality of service.
3. **Source Description Message :** The source sends a source description message within a fixed interval to give some extra information about itself. It contains the details about the name of the source, its mail ID, contact number or source controller.
4. **Bye Message :** To shut down a stream, a source sends a type of message which is known as Bye message. It is used by the source to announcing for leaving the conference. This message is a direct announcement for other sources about the absence of a source. It can be used for combining different media file.
5. **Application-Specific Message :** If we want to make our application extensible then RTCP allows application-specific RTCP packets which is introduced by RTC 3611. It can be used to extend the type of application.
6. **UDP Port of RTCP :**RTP use a well known UDP Port, but RTCP does not. RTCP uses a temporary port. It must be an odd-numbered port. It uses UDP port number which is the next higher odd number and that follows the port number which selected for RTP.

4.16 RTSP

GQ. Real Time Streaming Protocol in details .
GQ. When and why use an RTSP stream ?

- RTSP or Real Time Streaming Protocol is included on all IP cameras, NVRs, and DVRs that CCTV Camera World sells. RTSP provides the flexibility to integrate video from products manufactured by one company in to third party products. RTSP is a video streaming protocol that provides a video stream for use in third party software or recorders, or for use in live streaming applications. Continue reading to learn more about RTSP streaming and what it can be used for.
- Real Time Streaming Protocol or RTSP is a network protocol designed for use in entertainment and communications systems to control streaming media. The protocol was designed to create an easy way to access or manipulate a media stream. In CCTV and security camera systems the media is a video stream that can be with or without audio. The protocol packs complex transcoding and programming

together behind the scenes to transfer video over a network or to the internet with an easy to use link.

- RTSP has many uses outside of CCTV so there is a lot of information out on the web and it can get really technical. Since we're only concerned about security cameras we'll focus on how RTSP relates to the security cameras we sell. As we mentioned in the introduction RTSP is an included feature on all of our IP cameras, NVRs, and DVRs when connected to a network.
- The RTSP stream from a surveillance system or IP security camera directly relates to the encoding settings that are set on the device itself. This means that anyone looking to stream to a 4K TV or monitor should purchase a 4K security camera or 4K NVR system.
- Note: RTSP is a network protocol that requires a network connection. This means that Coaxial cameras, such as CVI or analog, cannot be used for projects with RTSP unless they are paired with a compatible DVR.

4.16.1 When and Why Use an RTSP Stream?

Alternate stream for increased ONVIF compatibility

- The main purpose of RTSP when it comes to security cameras is to assist with ONVIF compatibility. While RTSP can only send video and audio it helps by providing another type of stream to try if ONVIF compatibility does not work in the devices you are trying to use. This relates to when someone attempts to use an IP camera with a third-party recorder.
- Most professional NVR or XVR systems provide alternate ways to add 3rd party manufactured cameras and one of those ways is to access the RTSP stream from a camera.

Recording or live back up to a secondary location

- RTSP streaming also provides the ability to re-record and store the stream on another server or recorder. Since RTSP has been around a long time there are many media and NAS servers that have support for RTSP.
- Most XVR and NVR systems not only provide RTSP streams to send video out, they can also accept RTSP streams to record! This is useful for customers who prefer to have a secondary or redundant backup of their footage, or if it is required by regulations in industries like the marijuana industry.

4.16.2 Smart home system integration

- Companies like Control4, Savant, and other smart home installers offer RTSP stream compatibility to display security cameras or recorders on their home automation equipment.
- RTSP technology provides an easy way for these companies to transmit a video stream to multiple devices in a home at the same time.
- For example if a person has multiple tablets or home control stations they can pull a stream from a camera or NVR no matter where they are in their home or business.

4.16.3 VLC Media Player

- A great program to use RTSP streams with is VLC Media Player. VLC can be used to directly access the RTSP stream that a camera or system provides. The most common use of VLC is to watch a camera without logging into the web interface. Someone who is curious about how encoding settings affect their cameras can use VLC to view the RTSP stream to preview their changes and confirm there are no video artifacts. To finely tune encoding settings we recommend using a trial and error approach.
- Lower bitrates allow for more retention on recorder storage and less data usage when remote viewing. For more information on bitrates and how they effect remote viewing check out our article on watching security cameras with a slow internet connection

4.16.4 ebroadcasting the stream to live streaming services

- Last but not least is streaming a security camera to a live stream website. Some common live streaming CCTV projects include: animal sanctuaries, national parks, zoos, beaches, and construction sites. Most live streaming websites require a RTMP (Real Time Messaging Protocol) stream so the stream can be rebroadcast over the internet. Pairing a RTSP stream with streaming software like the free Open Broadcasting Software(OBS) offers a way to convert a RTSP stream to RTMP. Other paid or freemium software options include: Xsplit, VMIX, and Wirecast.
- Once the software is setup and conFig.d there will be live video streaming to Youtube, Facebook Live, or Twitch depending on what the user chooses to stream to. To learn more about streaming to the web using OBS as a streaming software watch and read our How to stream a security camera to YouTube Live article.

4.16.5 How do you use the RTSP stream from an IP camera, NVR, or DVR?

- We will discuss using the RTSP stream from the security cameras and recorders we carry here at CCTV Camera World.
- The RTSP stream URL varies from brand to brand but this article is meant for customers who have already purchased or are thinking about purchasing from CCTV Camera World.

RTSP performance

- Fetching the RTSP stream from a security camera or recorder involves transcoding the native stream. This transcoding not only has a CPU overhead on the device you are fetching the stream from, it introduces a delay or lag in the video stream.
- While IP cameras are not lag-free when compared to real-time live action, RTSP increases that lag. To demonstrate what to expect from RTSP streaming, we made the below video comparing the RTSP stream fetched from one of our 4K security cameras in 12MP mode to real live action, and to direct streaming from the camera's web service.

4.17 SPEED

Design Goals

The goal of the SPEED algorithm is to provide three types of real-time communication services, namely, real-time unicast, real-time area-multicast and real-time area-anycast, for ad hoc sensor networks. In doing so, we satisfy the following additional design objectives.

1. **Stateless architecture :** The physical limitations of ad hoc sensor networks, such as large scale, high failure rate, and constrained memory capacity necessitate a stateless approach in which routers do not maintain much information about network topology and flow state. Routing-table based protocols, such as DSDV, are suitable for wireless networks with a relatively small number of nodes and large memories. It is hard to imagine, however, that each sensor node in a sensor network would be able to have thousands of routing entries that would be needed in state-based approaches. In contrast, SPEED maintains neither a routing table nor per-flow state. Thus, its memory requirements are minimal.
2. **Real-time guarantees :** Sensor networks are commonly used to monitor and control the physical world. To provide a meaningful service such as disaster and emergency surveillance, meeting real- time constraints is one of the basic requirements of such protocols. Algorithms using on-demand routing are not designed to provide delay uarantees and may therefore fail to be suitable candidates for real-time applications. SPEED provides per-hop delay guarantees through a novel distributed feedback control scheme. Combining this feature with a simple scheme that bounds the number of hops from source to destination, SPEED achieves an end-to-end delay guarantee with small overhead.
3. **QoS routing and congestion management :** Most reactive routing protocols can find routes that avoid network hot spots during the route acquisition phase. Such protocols work very well when traffic patterns don't fluctuate very quickly during a session. They are less successful when congestion patterns change rapidly compared to session lifetime. When a route becomes congested, such protocols either suffer a delay or initiate another round of route discovery. SPEED uses a novel backpressure re-routing scheme to re-route packets around large-delay links with minimum control overhead.
4. **Traffic load balancing :** In sensor networks, the bandwidth is an extremely scarce resource compared to a wired network. Because of this, it is valuable to utilize several simultaneous paths to carry packets from the source to the destination. Most current solutions don't utilize multiple paths, which leads to high queuing delays and unbalanced power consumption. Instead, SPEED uses non-deterministic forwarding to balance each single flow among multiple concurrent routes.
5. **Localized behavior :** Pure localized algorithms are those in which any action invoked by a node should not affect the whole system. In this sense, for algorithms such as AODV, DSR, and TORA this is not the case. In these protocols a node uses flooding to discover the new path. In sensor networks where thousands of nodes communicate with each other, broadcast storms may result in significant power consumption and possibly a network meltdown.

   Instead, all distributed operations in SPEED are localized to achieve high scalability.

6. **Loop-free routing :** Since SPEED is based on greedy geographic forwarding, it is inherently loop-free [15]. While SPEED does not use routing tables, SPEED does utilize location information to carry out routing.

☞ **SPEED protocol**

The SPEED protocol consists of the following components:

- The API
- Neighbor beacon exchange.
- Receive delay estimation
- The stateless geographic non-deterministic forwarding algorithm (SNGF).
- Neighborhood Feedback Loop.
- Backpressure Rerouting.
- Last mile local flooding.

These components are described in the subsequent sections, respectively.

4.17.1 Application API and Packet Format

The SPEED protocol provides four application- level API calls:

- **AreaMulticastSend (position, radius, deadline, packet) :** This service identifies a destination area by its center position and radius. It guarantees that every node inside that area will receive a copy of the sent packet within the specified end-to-end deadline.
- **AreaAnyCastSend (position, radius, deadline, packet) :** This service guarantees that at least one node inside the destination area receives the packet before the deadline.
- **UincastSend(Global_ID,deadline,packet) :** In this service the node identified by Global_ID will receive the packet before the deadline.
- **SpeedReceive() :** this primitive permits nodes to accept packets targeted to them. There is a single data packet format for the SPEED protocol. It contains the following major fields:
- **PacketType :** this field denotes the type of communication: AreaMulticast , AreaAnyCast or unicast.
- **Global_ID :** this field is only used in the unicast case to identify destination node.
- **Destination area :** Describes a 3D space with a center point and radius where the packets are targeted.
- **TTL :** Time To Live field is the hop limit used for last mile processing.
- Payload.

Chapter Ends...

□□□

UNIT V

CHAPTER 5

Security in Wireless Communication

Syllabus

Security Issue and challenges in GSM, 1G, 2G, 3G, 4G. Multimedia security in 5G and 6G, post-quantum cryptography, Molecular communication, visible light communication (VLC), and distributed ledger (DL). UMTS Security, Bluetooth Security, WEP, WPA2.

Wireless Security Tools: Kismet, URH (Universal Radio Hacker).

5.1 SECURITY ISSUES AND CHALLENGES IN IN GSM, 2G, 3G, 4G

GQ. Which are main security issues for 2G

5.1.1 Main security Concerns Regarding with GSM

- Communications and signaling traffic in the fixed network are not protected.
- Does not address active attacks, whereby some network elements (e.g. BTS: Base Station) Only as secure as the fixed networks to which they connect
- Lawful interception only considered as an after-thought
- Terminal identity cannot be trustedwhile some of the **major attacks are:**
- *Man-in-the-middle attack*. This attacker positions itself between the target user and a network eavesdropping and modifying the traffic.
- *Eavesdropping*. The attacker eavesdrops signaling and data connections.
- *Network Impersonation*, the attacker sends signaling and data to the target user pretending to be a genuine network. A fake BST must be in place.
- *User Impersonation*, the intruder sends signaling data to the network pretending to be originated by the target user. It is possible to avoid **eavesdropping and cloning** due to the use of encryption and authentication.
- **Weaknesses in crypto algorithms** (A3 algorithm for authentication, A5 algorithm for encryption, A8 algorithm for key generation) that were not submitted to peer review due to nondisclosure.
- GSM only authenticates the user to the network and not vice versa. The security model, therefore, offers confidentiality and authentication, but limited authorization capabilities, and no non-repudiation.
- **GSM uses several cryptographic algorithms for security**. The A5/1 and A5/2 stream ciphers are used for ensuring over-the-air voice privacy. Both algorithms have been exploited:
  - A5/2 is exploitable with a real-time a ciphertext-only attack
  - A5/1 with a rainbow table attack.

5.1.2 3G

GQ. Which are main security issues for 3G.

- 3G offer greater security allowing mutual authentication between terminals and networks.
- With 3G network growth the mobile will play a similar ordinary role of a computer.
- Hackers are able to penetrate mobile devices exactly in the same way they accessed to our confidential data on our computer.

- Hackers can easily spy our movements, listen to our phone call, reads our messages, access to all our private data. This third-generation technology brings along with it a vast number of vulnerabilities, making it a haven for hackers and crackers.
- All this while, very few consumers were actually aware of the threats to 3G and each operator will need to spend 5-10 percent of its gain in securing. 3G services suffer more security threats and it is necessary to define new security solutions at different levels, both at the service provider's end and the handset manufacturer's.
- The 3G networks will make mobile communication network and bandwidth equivalent to a computer network, which will in turn, open the chances for cyber criminals to carry out attacks at will through the mobile networks.
- From a purely technological perspective 3G networks use the KASUMI block crypto instead of the older A5/1 stream cipher, but also KASUMI cipher has been identified several serious weaknesses. Consider also that the increasing of connectivity means a sensible grow of the security exposure harder to manage.

5.1.2(A) Main Security Problems related to 3G Networks

GQ. What is the main security problems related to 3G Network ?

- IMSI is sent in cleartext when allocating TMSI to the user
- The transmission of IMEI is not protected; IMEI is not a security feature
- A user can be enticed to camp on a false BS. Once the user camps on the radio channels of a false BS, the user is out of reach of the paging signals of SN
- Hijacking outgoing/incoming calls in networks with disabled encryption is possible. The intruder poses as a man-in-the-middle and drops the user once the call is set-up

According to ETSI TS 121 133 specification 3G threats could be classified as

Unauthorized access to sensitive data (violation of confidentiality)

- **Eavesdropping:** An intruder intercepts messages without detection.
- **Masquerading:** An intruder hoaxes an authorized user into believing that they are the legitimate system to obtain confidential information from the user; or an intruder hoaxes a legitimate system into believing that they are an authorized user to obtain system service or confidential information.
- **Traffic analysis:** An intruder observes the time, rate, length, source, and destination of messages to determine a user's location or to learn whether an important business transaction is taking place.
- **Browsing:** An intruder searches data storage for sensitive information.
- **Leakage:** An intruder obtains sensitive information by exploiting processes with legitimate access to the data.
- **Inference:** An intruder observes a reaction from a system by sending a query or signal to the system. For example, an intruder may actively initiate communications sessions and then obtain access to

information through observation of the time, rate, length, sources or destinations of associated messages on the radio interface.

Unauthorized manipulation of sensitive data (Violation of integrity)

- **Manipulation of messages:** Messages may be deliberately modified, inserted, replayed, or deleted by an intruder

Disturbing or misusing network services (leading to denial of service or reduced availability)

- **Intervention:** An intruder may prevent an authorized user from using a service by jamming the user's traffic, signaling, or control data.
- **Resource exhaustion:** An intruder may prevent an authorized user from using a service by overloading the service.
- **Misuse of privileges:** A user or a serving network may exploit their privileges to obtain unauthorized services or information.
- **Abuse of services:** An intruder may abuse some special service or facility to gain an advantage or to cause disruption to the network.
- **Repudiation:** A user or a network denies actions that have taken place.

Unauthorized access to services

- Intruders can access services by masquerading as users or network entities.
- Users or network entities can get unauthorized access to services by misusing their access rights

5.1.3 4G

GQ. Wrtie a short note on 4G security requirements and challenges.
GQ. Elaborate 4G security threats and attacks.

- The fourth generation (4G) networks is integration of many existing access networks such as 3G, LTE, WLAN (Wi-Fi), Wi-Max, and satellite communications where users are always connected. It is providing voice and data transfer with high quality-of-service (QoS), and is intended to provide high speed internet access to support voice/video multimedia applications.4G networks provides an open environment where different service providers with different wireless technologies share an IP-based core network to provide uninterrupted services to their subscribers with the same quality of service (QoS).
- In 4G systems, mobile equipments are switching from one network to another of different operators and wireless technologies; this is known as vertical handover. All these elements providing loop holes in security and vulnerabilities. Due to the open nature and IP-based infrastructure for 4G wireless, attention needs to be given to understand and study the security threats and issues. The task of securing 4G wireless networks and systems is a challenging one.
- The main security concerns of a 4G network includes, first, Securing hardware, software, data and operating System known as Application Security, second, Confidentiality Integrity Authentication and Authorization (CIAA) of data known as Network access security, and User's Identity, Confidentiality and authorization known as User security.

5.1.3(A) 4G Security Requirements And Challenges

- The main concern of any wireless mobile device is security with respect to data, hardware, user's identity and privacy. Security flaws are initiated either by the attacker or because of incorrect network or user's mobile parameter settings.
- For e.g., if user's mobile settings are kept open, any attacker can access the data, and in another scenario even after having good security features of the device, signaling at12tack can lead to resource exploitation. In thesecases, the affected mobile user will be denied access even the resources such as channel, bandwidth, energy are available. Thus in 4G systems it is required to add security features that can balance the resource availability while achieving high QoS.
- The security requirements of 4G heterogeneous networks have been defined on two levels:
- firstly, these are on mobile equipment; and, secondly, on operator networks. Mobile equipment requirements include protecting the device's integrity, privacy and confidentiality, controlling access to data, and preventing the mobile equipment being stolen.
- Existing research on security of 4G heterogeneous networks focused on the security such as authentication and authorization that is on the interface between the network and the operator.
- **Security** issues in mobile computing are now presenting many challenges. The ability to move from one network to another, and from one provider to another creating thus vertical and horizontal handoffs, has increased the complexity of mobile security. Therefore, it is necessary to design security solutions which are independent from the network, provider, and end user devices. The protection should involve not only data but, also an entity that is
- 4G should protect both the entities and infrastructure. The network and service providers must ensure their infrastructures and services are protected against all kinds of threats, as well as provide end users with secured accesses/services.

5.1.3(B) 4G Security Threats And Attacks

- 4G networks represent an open environment where different wireless technologies and service providers share an IP-based core network to provide uninterrupted services to their subscribers with almost the same quality of service (QoS).
- **Due to the open architecture and IP based environment, 4G heterogeneous networks receive new security threats and derive threats from the internet.**
- There are many possible threats within a 4G network system. These threats are: IP address spoofing, User ID theft, Theft of Service (ToS), Denial of Service (DoS), and intrusion attacks. New threat in 4G not seen in 3G the network infrastructure was owned by the service providers and access was denied to other network equipment. In mobile communications, another security problem is when the end user device is disconnected from the network because of no power in the battery.
- When device is switched on it will go from level of disconnection to connection presents an opportunity for the attacker to show himself as a mobile device or a mobile support station.

- In addition, new end user devices are sources of denial of service attacks, viruses, worms, and so on.
- The security threats according to X.805 are destruction, corruption modification of information, theft, removal or loss of information, disclosure of information, and interruption of services.
- Protocol specific attacks include malformed message attacks, buffer overflow attacks, Denial-of-Service (DoS) attacks, RTP session hijacking, and insertion of unauthentic RTP. 4G Networks can be viewed as convergence of networks such as Wi-Fi, WIMAX, and LTE.
- 4G will inherit all the security problems of 4G's access networks (such as 3G cellular networks, LTE, Wi-Fi, Wi-Max networks, sensor networks and so on). Therefore we need to do security analysis of these standards.

5.1.3(C) Possible Threats on 4G

- The Spam over Internet Telephony (SPIT), the new spam for VoIP, will become a serious problem just like the e-mail spam today. For example, SPITs targeting VoIP gateways can consume available bandwidth, thereby affecting the QoS and voice quality. Clearly, the open nature of VoIP makes it easy for the attackers to broadcast SPITs similarly to the case of spam emails.
- Other possible VoIP threats include, spoofing that misdirects communications, modifies data, or even transfers cash from a stolen credit card number, SIP registration hijacking that substitutes the IP address of packet header with attacker's own, eavesdropping of private conversation that intercepts and crypt-analyzes IP packets, and phishing attacks that steal user names, passwords, bank accounts, credit cards, and even social security numbers.

DOS attack On 4G Networks

- A DoS attack on a network is reducing the capacity of the network and disrupting communication. It reduces both the functionality and the overall performance causing inconvenience to both user and service provider. 4G is a heterogeneous network that consists of many wireless technologies from 2G to 3G to WLAN and WiMax.
- Each modulation technique suffers from jamming attack that can be the one way of DoS attack in the physical layer. Jamming attacks block the communication between the users's mobile device to the Base Station (BS). Jammer is a device, which can partially or completely disrupt a node's signal, by adding a noise to the signal. Jammer parameters such as signal strength, location and type influence the performance of the network and each jammer having a different effect on the user and the network.
- Jammer and interference caused by the cell allocation takes places in the physical layer; whereas in the routing layer, collision attack and signaling attack causes the system to either go to shutdown. In the transport layer, the possibility of flooding and authorization attack is high. In the application layer, authentication attacks are possible.

5.2 POST-QUANTUM CRYPTOGRAPHY

GQ. Explain Different Post Quantum Cryptography (PQC) algorithms.
GQ. Explain Post Quantum Cryptography in details.

- Due to recent developments in the field of quantum computers, the search to build and apply quantum-resistant cryptographic algorithms brings classical cryptography to the next level. Using those machines, many of today's most popular cryptosystems can be cracked by the Shor Algorithm. This is an algorithm that uses quantum computation to equate the prime number phases expressed as sine waves to factor large integers, effectively solving the discreet logarithm problem that many current cryptographic algorithms are focused on.
- Predominantly, state-of-the-art public key algorithms are based on related problems, three of which are at the top of the list. These three types of problems are known as the discrete algorithm problem, the entire factoring problem, and the new pre-eminent elliptical curve discrete algorithm problem. These three groups will be broken by Shor's quantum PC approximation. This is undoubtedly concerning, considering that these equations are commonly used to ensure the protected sharing of confidential information across the Internet, the development of digital signatures and the securing of other links over unsafe networks.
- In view of the inherited shortcomings and major disadvantages involved in the implementation of an effective and smooth Quantum Key Distribution (QKD) , the quest for a classic, non-quantum cryptography algorithm that will operate in current real-time infrastructures is an increasingly growing field of study. These quantum robust algorithms are called Post-Quantum Cryptography (PQC) algorithms and are assumed to remain stable after the availability of functional large-scale quantum computing machines , as depicted in **Fig. 5.2.1.**
- Every modern cryptography must be combined with existing protocols, such as transport layer security. The latest cryptosystem has to weigh:

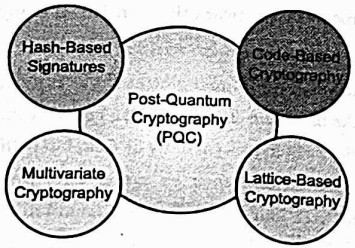


Fig. 5.2.1 : Basic types of Post-Quantum Cryptography (PQC)

- The size of the encryption keys and the signature.
- Time taken to encrypt and decrypt at either end of a contact line, or to sign messages and validate signature.

- For each proposed alternative, the amount of traffic sent over the wire needed to complete encryption or decryption or to transmit a signature.
- Latency induced by encryption and decryption at both ends of the communication line, assuming a number of devices to slow and memory limited IoT devices from large and fast servers.
- For ultra low latency, limit the size of public keys and signatures.
- Clear network architecture that facilitates crypt-analysis and the detection of vulnerabilities that could be exploited in a dense IoT network.
- Seamless integration with the existing infrastructure.
- Post-Quantum protocols include a rich collection of primitives that can be used to solve the problems presented by implementation across different computing platforms (e.g., cloud versus IoT ecosystems) and for various use cases. This involves the ability to compute encrypted data by having resilient (somewhat widely described than ever before) protocols against powerful attackers based on asymmetric key cryptography (using quantum machines and algorithms) and to provide security beyond the context of classical cryptography.
- Indeed, PQ cryptosystems are committed to strengthening the protection of mission-critical infrastructures, especially in energy, medical, surveillance, space exploration, etc. Due to the flexibility and scalability of PQ cryptosystems, these algorithms are also implemented in next generation 5G/NB-IoT networks, as well as for secure communications, for electric vehicle charging infrastructure.

5.2.1 Introduction to Post-Quantum Cryptography (PQC)

The PQC algorithms, as summarized in , are mainly implemented by either Hash-Based Signature Algorithms, Code-Based Cryptography, Multivariate Cryptography Protocols, or by Lattice-Based Cryptography. In the following section, we shall discuss the PQC algorithms briefly.

Hash based signatures	Multivariate cryptography	Code-based cryptography	Lattice based cryptography
Hash-based signature schemes use one-time signature schemes as their building block a given one-time signing key can only be used to sign a single message securely. Indeed, signatures reveal part of the signing key	This algorithm relies on the complexity of solving systems of multivariate polynomial equations	The private key is associated with an error-correcting code and the public key with a scrambled and erroneous version of the code Security is based on the complexity of decoding a generic linear code	Security is related to the difficulty of finding the nearest point in a lattice with hundreds of spatial dimensions (where each lattice point is associated with a private key) giving an arbitrary location in space (associated with the public key)
#	F (x)	100 1010 01	

Fig. 5.2.2 : Implementation methods of four basic quantum secure algorithms

5.2.1(A) Hash-Based Signatures

- A hash-based signature scheme initializes from a one-time signature (OTS), i.e., a signature scheme where each key pair only needs to be used to sign a message with. If an OTS key pair signs two different notes, this cab threatens the network, and a hacker will easily fake signatures that expose the customer's personal details. Merkle used the scheme of Lamport and its variations.
- Merkle recommended that a binary hash tree later named Merkle tree be used to create a many-time signature scheme. The leaves are the hash values of OTS public keys in a Merkle tree. Each inner node is measured as the hash of its two child nodes concatenating. If a collision tolerant hash function is used, this ensures that all leaf nodes, i.e., all OTS public keys, can be authenticated using the root node.
- The root node of the Merkle tree turns into a public key in a Merkle signature scheme (MSS) and the set of all OTS hidden keys becomes the secret key. Random bit strings are the hidden keys for hash-based OTS. Therefore, one can store a short seed and (re)generate the OTS secret keys using a cryptographically protected pseudo-random generator instead of storing all OTS secret keys.
- To prevent reuse of OTS key pairs, they are used according to the order of the leaves, starting with the leftmost leaf. To do this, the scheme keeps as an internal state the index of the last used OTS key pair. They are used according to the order of the leaves, starting with the leftmost node, to stop reuse of OTS key pairs. In order to do this, the scheme holds the index of the last used OTS key pair as an internal condition.

5.2.1(B) Code-Based Signatures

- Code-based cryptography is an upcoming contender for the diversification of today's public-key cryptosystems, most of which rely on the complexities of either the factorization or the discrete logarithm problem. Code-based cryptography, unlike public-key algorithms, is based on the problem of decoding unknown error-correcting codes, considered to be NP-hard. There are two simple Code-based cryptography systems named after Robert McEliece and Harald Niederreiter , their inventors. Compared to traditional cryptosystems, such as RSA , both share the issue of having massive key lengths, which renders their implementation impossible on embedded devices with very limited resources.
- The input message is converted into a code-word for plain text encryption by either adding random errors to the message or encoding a message in the error sequence. By deleting the errors or retrieving the original input message from the errors, decryption restores plain-text. It is, therefore, important to conceal the algebraic structure of the text, essentially cloaking it as an anonymous generic code. An adversary understanding the particular code used will be able to decipher the message.

5.2.1(C) Multivariate Cryptography

- The challenge of solving non-linear equation structures over finite fields is the foundation of Multivariate Cryptography schemes. Generally speaking, seeking a solution for such structures is called a NP-complete/-hard problem. Patarin's Secret Fields is one of the fascinating cases, generalizing a suggestion by Matsumoto and Imai.

- The same basic architecture is used for all Multivariate Public-Key Cryptosystems (MPKC), as they all depend on the use of multivariate polynomials over a finite field. The polynomial equations are of degree two in most cases, resulting in multivariate quadratic polynomials, which are still credited with being solved as NP-hard.
- The MQPKC can not be solved more easily with Shor's algorithm than using a classical computer, since it does not depend on any of the hard problems that Shor's algorithms can solve, as compared to many other forms of PKC (public-key cryptography). It is also a potential candidate group for, a quantum resistant encryption scheme.

5.2.1(D) Lattice-Based Cryptography

- Miklos Ajtai first demonstrated Lattice-based algorithms, with the suggestion of designing stable cryptographic algorithms based on the hard lattice problem (NP). A lattice-based public-key encryption scheme was adopted , but a scheme that was sufficiently robust and proven stable was not presented until 2005, when Oded Regev proposed his scheme. This method uses both lattices and a generalization of the problem of parity learning.
- A lattice, given in n-dimensional vector space, is a particular arrangement of points with an periodic structure and is used in a variety of fields. Lattice-based cryptographic algorithms are mostly based on either the problem with the nearest vector (CVP) or the problem with the shortest vector (SVP). In most lattice-based cryptographic algorithms, the cryptographic builders used are very time-efficient and simple, while still providing security proofs based on the worst-case hardness.
- A number of the simple problems used in this type of cryptographic algorithms often tend to be quantum resistant, since they are not based on any of the complicated problems solved by the algorithm of Shor. This results in one of a few types of algorithms that are believed to carry promise as potential candidates for post-quantum cryptography is lattice-based cryptography.
- For everyday Internet communications, generic cryptographic protocols, such as TLS and HTTPs , ensure that the communication between the two parties (sender and receiver) are authentic and private. Certain encryption algorithms that underpin these protocols, such as RSA , Diffie-Hellman, and elliptic curve , all are based on hard-to-solve mathematical problems and are categorized as asymmetric cryptographic primitives. The time and resources needed to address these issues are prohibitive, which ensures that data encrypted using current encryption algorithms is considered secure. Due to the fact that the quantum computers using Shor's factorization quantum algorithm can quickly solve current asymmetric cryptographic primitives.
- Several security specialists and scholars agree that the lattice-based cryptography algorithm is the path forward to deliver quantum-resistant encryption and, opposed to the other post-quantum cryptography strategies,. Lattice-based cryptography uses two-dimensional algebraic constructs known as lattices , which are not easily defeated with quantum computing schemes.

- A lattice is an infinite arrangement of dots, and the most vital lattice-based computational problem is the Shortest-Vector Problem (SVP) , which requires finding the point in the grid that is closet to a fixed central point in the space, called the origin. This is easy to solve in a two-dimensional grid, but, as the number of dimensions increases, even a quantum machine cannot solve the problem effectively. The fact that lattice-based cryptography provides fast, quantum-safe, fundamental primitives, and enables the construction of primitives previously thought impossible, makes it the front runner candidate for IoT applications.

5.2.2 Foundations of Lattice-Based Cryptography

High dimensional geometric structures are implemented by lattice cryptography, as seen in **Fig. 5.2.3**, to conceal or mask the original details, generating a complexity that is deemed difficult to overcome even with available fault-tolerant quantum computers without the existence of the original key. A lattice is an infinite grid of dots, often arranged in a 2-dimensional setting.

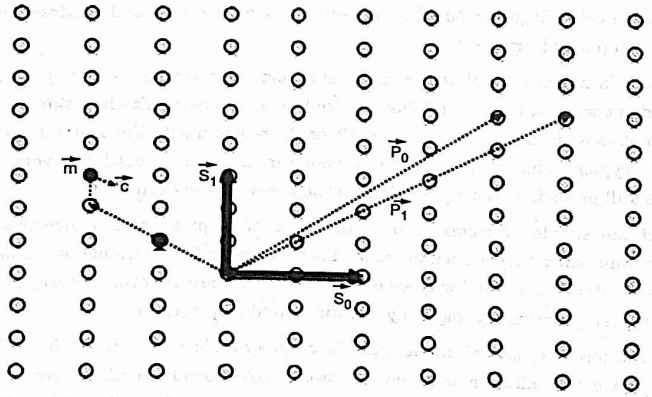


Fig 5.2.3 : High dimensional geometric structures

5.3 MOLECULAR COMMUNICATION

5.3.1 Introduction to Molecular Communication

- There are various environments, such as inside the hu- man body, where conventional wireless communication using electromagnetic (EM) waves is not feasible or detrimental. In this case, information transmission using chemical signals has been proposed as a promising solution, referred to as Molecular Communications (MC).
- Because of its unique, the interest in MC has been steadily growing over the past decade and IEEE has even launched initial standardization efforts. In MC, the information is encoded using the concentration, release time, and type of molecules.

- The propagation from transmitter to receiver can be passive (only diffusion of molecules) or active (diffusion-advection, molecular motors). Moreover, the receivers can also be clas- sified as passive or active, where the former only observe the received molecules and the latter detect the molecules by a chemical reaction. In order to fully exploit the potential of MC systems, their integration with the Internet is crucial.

5.3.2 Macro-Scale Molecular Communication

- In many industrial applications, it is preferable to transmit information wirelessly, instead of using wired solutions. In this case, embedded wireless sensors potentially have to convey information across complex and harsh environments.
- Unfortu- nately, in subterranean (e.g., tunnels or mines) and confined industrial environments (e.g., pipe networks including oil, water, and gas pipelines) conventional wireless communication using EM waves may not be feasible, because they suffer from high propagation path loss.
- For example, in tunnels or underground mines the path loss exponent can be greater than for a wide range of radio frequencies. Moreover,when a tunnel or pipe network cannot act as wave-guide for EM waves the path loss is even greater.

5.3.3 Internet of Bio-Nanothings (Micro-Scale Molecular Communication)

- The Internet of Things (IoT) refers to the integration of intelligent/smart machines and objects on the Internet. Thus, these smart devices can be accessed and controlled via the Internet.
- The advances made in the field of nanotechnology, i.e., new materials, such as graphene and metamaterials, enable the development of devices in the nano-meter range, which are referred to as nanothings.
- The interconnection of nanothings with the Internet is known as Internet of NanoThings (IoNT) and is the basis for various future healthcare and military applications.
- Nowadays, nanothings are based on synthe-sized materials (e.g., graphene), use electronic circuits, and EM-based communication. Unfortunately, these characteristics could be harmful for some application environments, such as inside the human body. Thus, recently the concept of Internet of Bio-NanoThings (IoBNT) has been introduced in , where nanothings are biological cells that are created using tools from synthetic biology and nanotechnology. Such biological nanothings are referred to as bio-nanothings.
- Similar to artificial nanothings, bio-nanothings have control (cell nucleus), power (mitochondrion), communication (signal pathways), and sensing/actuation (flagella, pili or cilia) units.For the communication between cells, MC is especially well suited, since the natural exchange of information between cells is already based on this paradigm.
- MC in cells is based on signal pathways (chains of chemical reactions) that process information that is modulated into chemical characteristics, such as the molecule concentration. The IoBNT concept enables many future applications.

- For example, intra-body sensing and actuation, where bio nanothings that are scattered inside the human body collaboratively collect health-related information. This information is then sent to an external healthcare provider through the Internet. Moreover, it is also possible to receive control signals (e.g., to release drugs) from the healthcare provider. Some applications scenarios for IoBNT, such as cooperative abnormality/cancer detection in blood vessels, using mobile bio-nanothings have been recently studied in.
- Since the communication in IoBNT is not restricted to the communication between bio-nanothings, an interface between the MC and the cyber (Internet) domain is needed, in order to allow information exchange between the nanonetwork and the Internet. This interface needs to accurately read the molecular information and translate it to EM parameters and vice versa. Developing such interfaces is one of the main challenges for the practical realization of IoBNT.
- Moreover, the interfaces may be application dependent. Another important issue in IoBNT is the security of information transmission. If this cannot be guaranteed, the opportunities offered by IoBNT can be used maliciously. For example, it can be used to steal personal health information or create new diseases and viruses. To address this issue, methods known from computer networks should be combined with security solutions from nature (e.g.,human immune system)

5.4 VISIBLE LIGHT COMMUNICATION (VLC)

GQ. Write a Short note on Visible Light Communication

GQ. What is different Applications of VLCs ?

5.4.1 Introduction to Visible Light Communication (VLC)

- VLC is a wireless method that enables high-speed transmission of data with visible light. This data is transmitted by modulating the intensity of light given off by a light source. The signal is received by a photodiode device that transforms the data into forms that are readable and readily-consumed by end users.
- Visible light communication (VLC) is the use of visible light as a method of wirelessly transmitting data. VLC is an affordable method of transmitting data at light speed. The light used in VLC is between 780-375 nanometers.
- Although radio frequency is more commonly used for communications, VLC has a number of advantages over the invisible frequencies of radio. VLC offers very low latency and high bandwidth, while radio has both a more limited spectrum and more potential for cross talk and interference than VLC. The limitation of line of sight can also be a security feature, unless a hacker has line of sight to a network device on a private network. If so, it can still be susceptible to an air gap attack from the outside world. Li-Fi is an implementation of wireless networking that uses VLC.

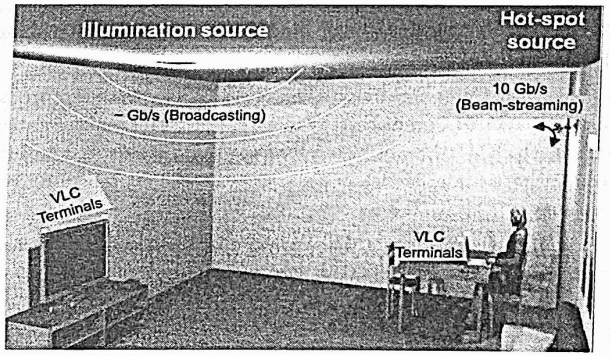


Fig. 5.4.1 : VLC terminal Communication

- Although VLC technologies have been historically uncommon, the draw of light based communication is strengthening as the proliferation of wireless devices increases and radio's limited spectrum becomes more crowded. The increased draw toward VLC technologies grows because networks, which affect each other in different radio frequencies, cause no interference to VLC. In IoT, VLC tech is being used as a communication method to connect millions of consumer electronics and machine-to-machine (M2M) devices cost-effectively.
- Visible Light Communication (VLC) is emerging to overcome the crowded radio spectrum as a solution for wireless communication networks. In VLC, data is transmitted by modulating the amplitude of an optical source that operates at a much faster rate within the visible range of the EM spectrum, making light-emitting diodes (LEDs) the most suitable light source for VLC due to their high switching rate. The EM spectrum ranging from 380 nm to 750 nm corresponding to the 430 THz to 790 THz frequency range is occupied by the VLC systems, and the availability of this broad bandwidth in the VLC has solved the problem of low bandwidth in RF communication.
- In VLC, security problems in RF communication can be solved, as optical source lights can not pass through opaque bodies and are confined in an intended area, nor does VLC cause any interference with RF signals resulting in improving VLC security. It is a well-known fact that exposure to high-intensity RF signals can lead to burns and damage to body tissues, reducing the transmission capacity of the system itself thereby affecting the system performance.
- VLC uses LEDs as a non-harmful optical source for the human body and can be used to reduce extra energy for illumination and communications. VLC devices, however, cost substantially less than current RF modules and can also provide higher data rates. In view of the above advantages, because of its high bandwidth, low power consumption, no health risks, and the fact that it is a more effective data transmission process, VLC is considered one of the promising candidates for wireless communication systems.

5.4.2 Applications of VLCs

- Some of the applications of VLCs include Light Fidelity (Li-Fi) , underwater communication , smart transport network , etc.
- Li-Fi is a new technology that uses the illumination principle as a method of transmitting data using visible light and is identical to Wi-Fi, which uses radio frequencies for communication. Li-Fi can reach a speed of up to 10 Gbps, which is 250 times higher than the speed of superfast broadband, and if there is concern about electromagnetic interference in airlines, hospitals, etc. where RF contact is prohibited, Li-Fi can also be a solution.
- Nevertheless, since Li-Fi is a complementary technology that seeks to solve the challenges faced by the existing technology, one does not simply use a light bulb to transmit data to fast-moving objects or objects behind walls.

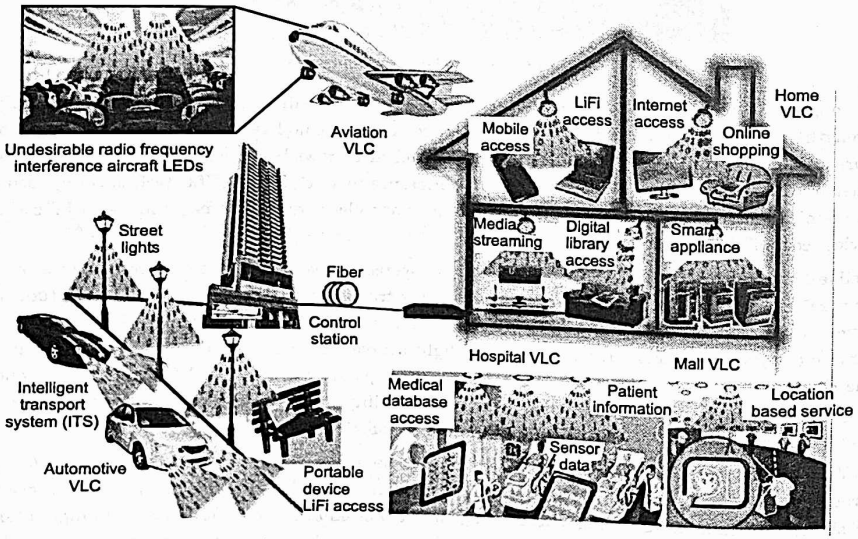


Fig. 5.4.2 : Different Application of VLC

- VLC can also be used in underwater communication as an effective substitute for RF waves since RF signals can not spread well in seawater because of the salty, high conductivity, and high attenuation of seawater conditions.
- Yet, when moving deep into the ocean, sound waves have a low propagation rate, restricted bandwidth, and high power demand, as well as being likely to communicate with marine animals, such as dolphins. VLC can effectively overcome these radio waves and sound waves limitations in underwater communication by allowing the use of visible light for data communication. The use of VLC for

underwater communication, however, poses some concerns as the data transmission rate and the distance can be seriously impaired when the water loses its transparency due to the presence of suspended particles, i.e. turbidity.

- VLC may be used to prevent accidents by communicating between vehicles with regard to pre-crash sensing, collision warning, lane shift warning, traffic signal violation warning, etc., as the risk of accidents in developing countries is growing. Since these kinds of applications require reliable reachability and low latency, a high-speed visible light communication system like Li-Fi is needed. However, some problems will be met with VLC implementation, including interference with ambient light sources, interference with other VLC devices, and VLC integration with existing technologies such as Wi-Fi.

5.4.3 LEDs Implementation in VLC

- Due to its outstanding features, such as low cost, low power consumption, providing multiplexing options for wavelengths, and compatibility with existing solid-state lighting systems, LEDs have gained considerable interest in high-speed VLC applications.
- However, conventional polar LEDs grown on the c-plane have limited bandwidth, especially in the green spectral region due to their inbuilt piezoelectric polarization. This polarization in c-plane-oriented InGaN quantum wells separates electrons and holes, thus increasing the time of radiative recombination resulting in a strong Quantum Confined Stark Effect (QCSE).
- Not only can the QCSE cause a significant peak shift, but also a significant drop in luminous efficiency under high injection current, resulting in a significant deterioration of device performance along with Auger effects. This polarization field can be reduced or removed by increasing the quantum wells in semipolar or nonpolar orientations. This allows better electron and hole overlapping and faster radiative recombination, especially in thicker quantum wells Thus, higher electro-optic bandwidths can be predicted for such crystal orientations along with potentially reduced Auger effects.
- Because of the luminous efficiency benefits offered by semipolar LEDs and stable light wavelengths, its functionality has been extended in applications such as high-resolution display, high-speed visible light communication, and researchers have therefore begun to devote their efforts to the production of semipolar GaN-based LEDs.
- Nevertheless, enhancing the modulation characteristics of the LED light source and the emission efficiency under high-speed modulation is part of a better VLC implementation. Several researchers have shown that the modulation characteristics of LEDs rely on the lifetime of carrier recombination, so semipolar LEDs with less QCSE can have faster radiative recombination and help to boost modulation characteristics for VLC applications.
- However, compared with LEDs, micro-LEDs (μ-LEDs) have a better frequency response owing to their higher efficiency, low-power consumption, high brightness, and especially longer life. Higher brightness for μ-LEDs corresponds to a faster transmission rate with a lower bit error rate (BER) for VLC applications.

- LEDs of micro-size can have a high modulation bandwidth by achieving a small carrier lifetime, as they can sustain higher injection current densities. In addition, having a small active region will lead to a decrease in geometric capacitance, thus reducing the RC time constant, which is a limiting factor of modulation bandwidth.

5.5 DISTRIBUTED LEDGER

GQ. What Is A Distributed Ledger? Explain in details.
GQ. How Are Blockchain And Distributed Ledger Different?
GQ. Explain in details : public or private / permissioned / permissionless distributed ledger.
GQ. Why are distributed ledger technologies useful?
GQ. The Benefits Of Blockchain And Distributed Ledger Technology.

5.5.1 Introduction Distributed Ledger

- Distributed ledger technologies, like blockchain, are peer-to-peer networks that enable multiple members to maintain their own identical copy of a shared ledger. Rather than requiring a central authority to update and communicate records to all participants, DLTs allow their members to securely verify, execute, and record their own transactions without relying on a middleman.
- While there are a wide variety of DLTs on the market, they are all comprised of the same building blocks: a public or private / permissioned / permissionless distributed ledger, a consensus algorithm (to ensure all copies of the ledger are identical), and a framework for incentivizing and rewarding network participation.

Public vs. private and permissioned vs. permissionless

Distributed ledgers are categorized as "private" or "public" and "permissioned" or "permissionless" — they can be any combination of any of the two. To achieve full decentralization, Hedera believes distributed ledgers must be public permissionless networks.

- **Private / Permissioned** : This type of network offers no decentralization. The applications and the network nodes running those application must both be invited to join the network and meet certain criteria or provide a form of identification. Any party can also be removed without warning at any time.
- **Private / Permissionless** : Requires that applications deployed in production be invited to join the network and can be removed without warning at any time. The nodes which constitute the network and run said applications can freely and anonymously join and contribute, typically in exchange for a network's native cryptocurrency.
- **Public / Permissioned** : Allows applications to be deployed in production or removed, without having to notify anyone, reveal their identity, or meet any application criteria requirements. The nodes which constitute the network and run said applications must be invited to join the network.
- **Public / Permissionless** : This type of network is the most decentralized. Applications can be deployed in production or removed, without having to notify anyone, reveal their identity, or meet any application criteria requirements. Additionally, the nodes which constitute the network can freely and anonymously join and contribute, typically in exchange for a network's native cryptocurrency.

Reaching consensus

- Although every node on a permissioned or permissionless distributed ledger maintains and updates their own copy of the ledger, it is imperative that each of these ledgers remains identical. Imagine, for instance, that your copy of the ledger reveals that you have $100 in your account, while the cashier's ledger holds that you have $1. This discrepancy would make it very difficult, if not impossible, to buy a candy bar. Without identical ledgers, participants in the network could not make transactions.
- In order to keep the distributed ledger consistent, DLTs must have a consensus algorithm, or a method of ensuring that all copies of the ledger agree. **A consensus algorithm is a method of synchronizing the data across a distributed system. In the case of a DLT, the consensus algorithm ensures that all copies of the ledger are identical.**
- There are many different consensus algorithms on the market, each with different advantages. Perhaps the most intuitive algorithm is a simple vote. According to this algorithm, each node independently calculates how they think they should update their ledger based on the information available to them. Then, each node sends this information to every other node. At this point, every node in the network has access to their decision and every other node's decision. The nodes then calculate the majority or plurality vote, and they all update their ledgers according to this democratic consensus.
- Although the simple vote is effective and intuitive, it is not efficient at scale. Because every node must send their vote to every other node, the bandwidth and processing power required to come to consensus grows exponentially with the size of the network. In other words, every additional node dramatically decreases the efficiency of the network. Because DLTs become more secure and transparent when more nodes are added to the network, many other consensus algorithms have been developed to better suit the need for large, efficient, and reliable peer-to-peer networks.
- If you are curious about other consensus algorithms, you can learn about them by visiting the following pages within the learning center: voting-based consensus, economy-based consensus, and more coming soon.

5.5.2 Why are Distributed Ledger Technologies Useful?

- Distributed ledger technologies allow businesses and individuals alike to quickly carry out secure transactions without needing to rely on a middleman.
- By avoiding intermediaries, distributing control of the ledger, and providing a tamper-apparent network, DLTs present a more cost-efficient, accessible, and reliable transaction platform than centralized ledger systems.

Remove the middleman

- Because central ledgers rely on intermediaries, they are burdened by the costs and inefficiencies of the middleman. DLTs do away with these limitations by avoiding middlemen and intermediaries altogether. Without a central agent, there is no need to pay a central agent. And, without the need for clunky bureaucracy, you can exchange assets directly and immediately. You no longer have to limit the speed of your transaction to the efficiency of expensive bankers, lawyers, or politicians.

- Moreover, you no longer have to trust bankers, lawyers, or politicians with the ledger and your assets. DLTs are trustless systems, meaning that no participant needs to trust any other participant to guarantee a valid ledger.

Accessibility

- While centralized systems monopolize control and limit access to their ledger, DLTs provide a much more accessible service. DLTs allow businesses and individuals to carry out transactions freely, without relying or trusting any other individual.
- Public DLTs take this further by issuing no restrictions on transactions or participation; no one can be denied from the platform, and no transaction will be treated with priority over another.

Tamper-apparent

- Traditional ledgers may provide fast and simple record-keeping, but they are vulnerable to corruption and hacking. Because only one central entity controls the ledger, a corrupt central agent can tamper with the records without the consent or knowledge of the affected members. Moreover, because there is only one copy of the ledger, hackers have a clear, single target for their attacks. Without visibility into whether tampering has occurred, we must simply trust that the central third-party is neither corrupt nor compromised when we use a centralized ledger.
- Distributed ledgers, however, are inherently resistant to tampering. While a malicious agent could compromise a central system by altering the single ledger, they would need to alter at least a plurality of ledgers to have an impact on a distributed system.
- Though DLTs are not tamper-proof, they are tamper-apparent. That is, if tampering does occur, the network's transparency ensures that all members of the network will be aware of the change. Though a participant of a DLT cannot be completely certain that the ledger will remain unaltered, they can rest assured that they will know if tampering does occur.
- Hedera Hashgraph has achieved the gold standard of security in distributed ledger consensus mechanisms, which is asynchronous Byzantine fault tolerance (aBFT) and is the only distributed ledger to-date which has formally proven this quality. Hedera guarantees consensus, in real time, and is resistant to Distributed Denial of Service (DDoS) attacks, an area of vulnerability for some public ledger platforms.

Immutability and controlled mutability

- Some distributed ledgers take security beyond tamper-apparent by establishing immutability, preventing any and all participants from changing established records for any reason. Members of these immutable DLTs can only view the ledger and carry out new transactions.
- Even if all participants in the network wished to change the ledger, there would be no pathway within the system's architecture for that change to occur. Therefore, participants of an immutable distributed ledger can be certain that their ledger is not only tamper-apparent, but tamper-proof. A distributed ledger technology is immutable if it does not provide any participant or group of participants the ability to alter or delete established records. Of course, immutability does come with downsides. In some cases,

changing past records could be beneficial. For instance, if a bug in the DLT's code causes a transaction to be misrepresented in the ledger, immutability would prevent anyone from fixing that problem. The invalid transaction would forever be part of the official ledger. Additionally, as laws change to catch up with technology, new government regulations may necessitate a change in record-keeping practices. Immutable systems would not be able to adapt to these changing legal conditions, and would therefore risk violating government standards.

- Recognizing the downsides of both mutability and immutability, some DLTs opt for controlled mutability. DLTs with controlled mutability allow records to be changed, but place heavy restrictions upon that pathway.
- Controlled mutability is the best of both worlds: no malicious participant or group of participants can alter the records without everyone knowing (tamper-apparent), but the DLT can adapt to bugs and changing regulations. Hedera Hashgraph is one example of a DLT with controlled mutability.

5.5.3 What Is A Distributed Ledger?

- A distributed ledger is a database that exists across several locations or among multiple participants. By contrast, most companies currently use a centralised database that lives in a fixed location.
- A centralised database essentially has a single point of failure. However, a distributed ledger is decentralized to eliminate the need for a central authority or intermediary to process, validate or authenticate transactions.
- Enterprises use distributed ledger technology to process, validate or authenticate transactions or other types of data exchanges. Typically, these records are only ever stored in the ledger when the consensus has been reached by the parties involved.
- All files in the distributed ledger are then timestamped and given a unique cryptographic signature. All of the participants on the distributed ledger can view all of the records in question. The technology provides a verifiable and auditable history of all information stored on that particular dataset.

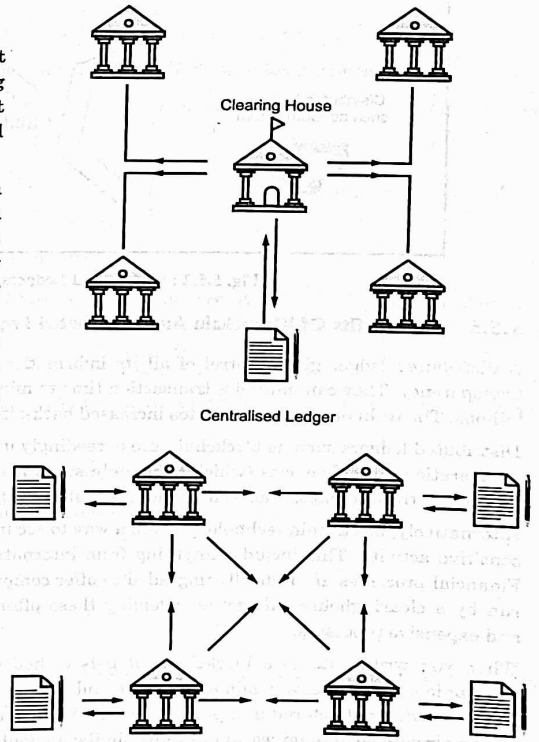


Fig. 5.5.1 : Centerlized and Distributed ledger

5.5.4 How Are Blockchain And Distributed Ledger Different?

- The most important difference to remember is that blockchain is just one type of distributed ledger. Although blockchain is a sequence of blocks, distributed ledgers do not require such a chain. Furthermore, distributed ledgers do not need proof of work and offer – theoretically – better scaling options.
- Removing the intermediary party from the equation is what makes the concept of distributed ledger technology so appealing. Unlike blockchain, a distributed ledger does not necessarily need to have a data structure in blocks. A distributed ledger is merely a type of database spread across multiple sites, regions, or participants.
- On the surface, distributed ledger sounds exactly how you probably envision a blockchain. However, all blockchains are distributed ledgers, but remember that not all distributed ledgers are blockchains. Whereas a blockchain represents a type of distributed ledger, it is also merely a subset of them.

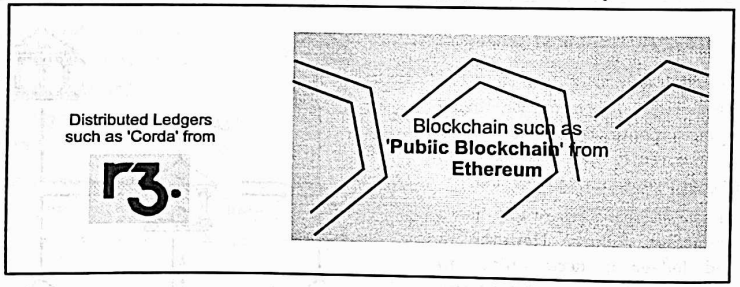


Fig. 5.5.2 : Distributed Ledgers & Blockchain

5.5.5 The Benefits Of Blockchain And Distributed Ledger Technology

- A distributed ledger gives control of all its information and transactions to the users and promotes transparency. They can minimise transaction time to minutes and are processed 24/7 saving businesses billions. The technology also facilitates increased back-office efficiency and automation.
- Distributed ledgers such as blockchain are exceedingly useful for financial transactions. They cut down on operational inefficiencies (which ultimately saves money). Greater security is also provided due to their decentralized nature, as well as the fact that the ledgers are immutable.
- Alternatively, blockchain technology offers a way to securely and efficiently create a tamper-proof log of sensitive activity. This includes anything from international money transfers to shareholder records. Financial processes are radically upgraded to offer companies a secure, digital alternative to processes run by a clearinghouse. Altogether avoiding these often bureaucratic, time-consuming, paper-heavy, and expensive processes.
- When you write data to a blockchain, it gets etched on the network. When you have a series of transactions over time, you gain an accurate and immutable audit trail. This is very useful for financial audits. Having data stored in a place where no single entity owns or controls it, and no one can change what's already written, gives you benefits similar to double-entry book-keeping. Ultimately, this means that there are fewer chances of errors or fraud.

5.6 UMTS SECURITY

- The security in UMTS is built on the security of GSM and GPRS. This means UMTS makes use of the security features used in GSM. This also maintains the compatibility with GSM.
- Since the compatibility in GSM is maintained, handoff and internetworking between GSM and UMTS is easy.
- The security features in UMTS correct the problems with GSM by addressing its real and perceived security weaknesses.
- UMTS uses public keys. In UMTS mutual authentication between the mobile and BS occurs; thus there is no fake BS attack. UMTS has increased key lengths and provides end-to-end security.
- Additional UMTS security features which are not present in GSM security mechanism are mentioned as below :
  - Security against using false base stations with mutual authentication.
  - Encryption extended from air interface only to include Node-B to RNC connection.
  - Security data in the network will be protected in data storages and while transmitting ciphering keys and authentication data in the system.

☞ Mechanism for upgrading security features

- The other security features of UMTS are listed below:
  1. Subscriber individual key K: It is user specific.
  2. Authentication center and USIM share User-specific secret key K, Message authentication functions f_1, f_2 and Key generating functions f_3, f_4, f_5.
- The authentication center has a random number generator. The authentication center has a scheme to generate fresh sequence numbers. USIM has a scheme to verify freshness of received sequence numbers.
- Authentication functions f_1, f_2 are MAC (XMAC) and RES (XRES).
- Key generating functions f_3, f_4, f_5 are as mentioned below:
  1. f_3: ciphering key CK (128 bit);
  2. f_4: integrity key IK (128 bit) and
  3. f_5: anonymity key AK (128 bit).
- Key management is independent of equipment. Subscribers can change handsets without compromising security. Assure user and network that CK / IK have not been used before.
- Integrity function f_9 and ciphering function f_8 are based on the Kasumi block cipher.

5.6.1 UMTS Specification has Five Security Feature Groups

- **Network access security :** The set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link.
- **Network domain security :** The set of security features that enable nodes in the provider domain to securely exchange signalling data and protect against attacks on the wireline network.
- **User domain security :** The set of security features that secure access to mobile stations.
- **Application domain security :** The set of security features that enable applications in the user and in the provider domain to securely exchange messages.
- **Visibility and configurability of security :** The set of features that enables the user to inform himself whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

5.7 SECURITY IN WIRELESS COMMUNICATION

The wired networks and the wireless networks differ in a security point of view because of few differences in them.

- On the wired network the user must gain the access to the physical wire initially.
- The network card has to be connected with the network.
- In wired network there is always the issue of authentication. The user needs to authenticate himself in the network first with password/token /biometric whichever system is applied.
- However on the wireless networks these issues are initially ignored in WEP (Wired Equivalent Privacy).

5.7.1 WEP (Wired Equivalent Privacy)

GQ. Describe WEP and WPA in detail.

- WEP was designed to provide the same privacy that a user would have on a wired network.
- WEP is based on RC4 symmetric encryption standard. It uses either 64 bit or 128 bit key. Actually all 64 or 128 bits are not used for encryption.
- Out of 64 or 128 bits, 24 bits are used for Initialization Vector (IV). Initialization vector is used to encrypt each packet with different keys. It is obtained by adding IV to 40 bit or 104 bit PreShared Key (PSK). It is IV+PSK.
- It reduces the overall key strength of the process as the effective lengths of the keys becomes only 40 or 104 bits.
- PSK can be generated by two different ways.

1. Default key method 2. Key mapping method

1. Default key method

It can share up to four default keys with all the WAPs.

2. Key mapping method

- It sets up the key mapping relationship between each wireless station with another individual station.
- It adds overhead and reduces throughput. This higher overhead indicates that many systems that use WEP opt to use single shared key on all stations.

5.7.1(A) WEP Process

1. The secret key initializes transmitting and receiving stations. This secret key must be distributed by using an out-of-band mechanisms. The out of band mechanisms are email, posting it on a website, or giving it on a piece of paper.
2. The transmitting station produces a seed. This seed is obtained by appending the 40-bit secret key to the 24-bit Initialization Vector (IV), for input into a Pseudo-Random Number Generator (PRNG).
3. The transmitting station uses the seed as input to the WEP PRNG to generate a key stream of random bytes.
4. The key stream is XORed with plaintext to achieve the cipher text.
5. The transmitting station appends the cipher text to the Initialization Vector (IV) and sets a bit. This bit indicates that it is a WEP-encrypted packet. It completes WEP encapsulation, and the results are transmitted as a frame of data. WEP encrypts only the data. The header and trailer are sent in clear text.
6. The receiving station checks to see whether the encrypted bit of the frame is received is set. If so, the receiving station extracts the Initialization Vector (IV) from the frame and appends the Initialization Vector (IV) to the secret key.
7. The receiver generates a key stream that must match the transmitting station's key. This key stream is XORed with the cipher text to obtain the sent plaintext.

Problems associated with WEP

1. The IVs are not exclusive and are reused. These reused IVs can expose PSK.
2. Wireless vendors work to remove weak IVs but attackers were looking for other ways to crack the encryption standard.
3. WEP doesn't ensure authenticity of the data packets.

5.7.2 WPA (Wi-Fi Protected Access)

- WPA offers more security as compared to WEP. It is actually the solution for the problems associated with WEP.
- WPA makes use of Temporal Key Integrity Protocol (TKIP).
- TKIP scrambles the keys using a hashing algorithm and adds an integrity-checking feature that verifies that the keys haven't been tampered with.

5.7.2(A) Advantages of WPA over WEP

1. The Initialization Vector (IV) is increased from 24 bits in WEP to 48 bits.
2. Rollover has been eliminated. Hence there are less chances of key reuse occurring. Actually WPA makes use of CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). CCMP uses the AES (advanced encryption standard) encryption algorithm. It expands the IV to 48 bits to prevent rollover and detects replayed traffic.
3. Different secrete keys are used for each packet which is not the case on WEP.
4. Message integrity is well achieved in WPA as compared to WEP. WPA addressed Message Integrity Check (MIC) by a method known as Michael. It is designed to detect invalid packets. It can also help in preventing the attacks.
5. WPA is backward compatible with RC4 algorithm. It enables users to upgrade the existing hardware.

5.7.2(B) Different Protocols used in WPA/WPA2

- WPA and WPA2 are the two versions of WPA with minor differences.
- They both can use a variety of security protocols like Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP).
- Extensible Authentication Protocol (EAP) is another authentication protocol used in WPA. It is defined in RFC 3758. EAP is an authentication framework, not an authentication mechanism.EAP rides on top of the Ethernet protocol. It is used to facilitate authentication between the client requesting to be authenticated and the server performing the authentication.
- There is also EAP over LAN (EAPOL). IEEE has approved it as a transmission method to move packets from the client to an authentication server.
- There are four basic types of EAPOL packets:

1.	The EAPOL packet	2.	The EAPOL start
3.	The EAPOL logoff	4.	The EAPOL key

1. The EAPOL packet

This message type is simply a container for transporting EAP packets across a LAN.

2. The EAPOL start

This message is used by the client to inform the authenticator it wants to authenticate to the network.

3. The EAPOL logoff

The message informs the authenticator that the client is leaving the network.

4. The EAPOL key

This message type is used with 802.1x for key distribution. One of the most important protocol used in WPA is TKIP. It is Temporal Key Integrity Protocol (TKIP). TKIP is used to address the known cipher attack vulnerability that WEP was vulnerable to TKIP's role is to ensure each data packet is sent with its own unique encryption key. TKIP uses the RC4 algorithm.

5.7.3 Securing Wireless Networks

The wireless network security works on the same principle as that of wired network security mechanisms. It is the principle of defense in depth.

Defense in Depth

It is based on the concept of building many layers of protection. These layers are

- Encrypting data so that it is hidden from unauthorized individuals.
- Limiting access based on least privilege.
- Providing physical protection and security to the hardware.
- Using strong authentication to verify the identity of the users who access the network.
- Employing layers of security controls to limit the damage, should one layer of security be overcome
- Deploying many layers of security to make it much harder for an attacker to overcome the combined security mechanisms
  - Initially changing SSID is beneficial.
  - Next important measure is to limit the access to the wireless network to specific adapters.
  - Some of the switches and WAPs can perform MAC filtering. MAC filtering uses the MAC address assigned to each network adapter to enable or block access to the network.
  - For increasing the security of the network, WEP devices can be exchanged to WPA or WPA2.

5.8 WIRELESS SECURITY TOOLS: KISMET

5.8.1 Wireless LAN Threats and Tools used for Wireless Security

GQ. Write short note on Wireless LAN threats.

There are four different threats to wireless LAN networks

1.	Wardriving	2.	Eavesdropping
3.	Rogue Aps	4.	Denial of service

1. Wardriving

- Wardriving is the term used to describe someone who uses a laptop and a wireless NIC to look for wireless networks.
- This activity is usually performed by automobile. The war-driver typically uses a Global Positioning System (GPS) device to record the location, and a discovery tool such as NetStumbler.

(i) Warchalking

The act of marking buildings or sidewalks with chalk to show others where it's possible to access an exposed company wireless network.

(ii) War flying

- Similar to wardriving, except that a plane is used rather than a car.
- There are two tools available for site surveys and wardriving activities.

They are

(a) NetStumbler (for Windows) (b) Kismet (for Linux platform)

(a) NetStumbler

- One of the primary tools used to locate wireless networks is NetStumbler. It can be downloaded from the website www.netstumbler.com.
- NetStumbler is a Windows-based GUI tool that you can use as a wireless scanner. It operates by sending out a steady stream of broadcast packets on all channels.
- It's useful for checking the coverage of an organization's wireless LAN.
- NetStumbler can provide the user with a wealth of information such as :
  - MAC address
  - SSID
  - Access point name
  - Channel
  - Vendor
  - Security (WEP on or off)
  - Signal strength
  - GPS coordinates (if GPS device is attached)

(b) Kismet

- It runs on the Linux OS. It can be downloaded from www.kismetwireless.net. Kismet works with many wireless cards and has a similar functionality to NetStumbler's.
- Kismet has the following features:
  - Detection of NetStumbler clients.
  - Cisco product detection via CDP.
  - IP block detection.
  - Hidden SSID decloaking.
- Ethereal file logging
- Air snort-compatible weak key logging
  - Run-time decoding of WEP packets.
  - Grouping and custom naming of SSIDs.

  - Multiple clients viewing a single capture stream.
  - Graphical mapping of data.
  - Manufacturer identification.
  - Detection of default WAP configurations.
  - NetStumbler and Kismet are just two of the tools. available for site surveys and ward riving activities.

2. Eavesdropping

- If a hacker can use NetStumbler or Kismet and find an WAP that is conFig.d with the manufacturer's default configuration, it will likely be a target for the attacker.
- A WAP with even WEP installed is much less appealing for the person doing a random drive-by.
- Even today WAPs are still open everywhere. Anything which is not encrypted is vulnerable to attack.
- Most of the times the computer security is based on passwords.
- Many wireless devices are of open systems authentication which means no authentication needed.
- If used in this state, hackers are not only free to sniff traffic on the network, they are free to connect to it and use it as they see fit. If there is a path to the Internet, the hacker may use the victim's network as the base of attack. Anyone tracing the IP address will be led back to the victim, not the hacker.
- In case of open systems authentications it easy for a hacker to gain unauthorized information, hijack resources, and even introduce back doors onto other systems.
- Tools used for eavesdropping and capturing passwords are

(a) Dsniff (b) Win Sniffer (c) Cain and Abel

(a) Dsniff

- Dsniff is included with BackTrack and can also be downloaded from http://monkey.org/~dugsong/dsniff/.
- Dsniff is actually a collection of tools that includes Dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspy.
- These tools allow the attacker to passively monitor a network for interesting data such as passwords, email, and file transfers.

(b) Win sniffer

- Win Sniffer is a password-capture utility that enables network administrators to capture passwords of any network user.
- Win Sniffer can capture and decode FTP, POP3, HTTP, ICQ, SMTP, Telnet, IMAP, and NNTP usernames and passwords.
- Win Sniffer can be downloaded from ww.winsniffer.com

(c) Cain and Abel

Cain is a multipurpose tool that can perform a variety of tasks, including Windows enumeration, sniffing, and password cracking.

3. Rogue Access Points/Ad-Hoc Networks

- Many a times attackers set up rough access points in WLAN networks. Due to this some of the device may get fooled by this AP and can get connected to it.
- Physical access is usually required in this because if a user associates with a rogue access point then is unable to perform any of their normal duties.
- If an attacker can gain access to a physical port on a company network and then hook the access point into this port, it is possible to get devices to associate with the rogue access point and capture data through it for an extended period of time.
- When the WLAN network targeted only provides Internet access; it becomes easier for a rogue access point to provide simple Internet access. It keeps user away from the vulnerability for long time.
- Same as rough access points, unauthorised access points is also one of threat to WLAN.

Access point spoofing

- Refer Fig. 5.8.1. It shows access point spoofing.

(5D33)**Fig. 5.8.1 : Access point spoofing**

- Access point spoofing occurs when the hacker sets up their own rogue WAP near the target network or in a public place. If the spoofed WAP has the stronger signal, the target computer will choose the spoofed WAP.
- This puts the attacker right in the middle of all subsequent transmissions. Due to this middle position the attacker can attempt to steal usernames and passwords or simply monitor traffic.
- When performed in an open hot spot, this attack is sometimes referred to as the evil twin attack.

Host routing

- It may occur when the wireless device is connected to the wired as well as wireless network at the same time.
- It may expose the host on the trusted wired network to all or any host that connect via the wireless network.
- Just by a simple misconfiguration, an authorized client may be connected to the wired network while unknowingly having its wireless adapter enabled and connected to an unknown WLAN.

4. Denial of Service

- It is nothing but the collided networks. When the collision occurs in the network new packets are denied the access of the network.
- The amount of traffic required to affect a target device can be much higher than the capabilities of a single machine.

- However, the flooding of traffic is not the only way to limit access to services; for wireless networks it can be much easier as the signal can be interfered with through a number of different techniques.
- A denial-of-service attack can also be used in conjunction with a rogue access point.
- Some common denial of service attacks are as follows

a. Authentication flood attack	b. De-authentication flood attack
c. Network jamming attack	d. Equipment destruction attack

a. Authentication flood attack

- This type of DoS attack generates a flood of EAPOL messages requesting 802.1X authentication.
- As a result, the authentication server cannot respond to the flood of authentication requests and consequently fails to return successful connections to valid clients.

b. De-authentication flood attack

- This type of DoS targets an individual client and works by spoofing a de-authentication frame from the WAP to the victim.
- The victim's wireless device would attempt to reconnect, so the attack would need to send a stream of de-authentication packets to keep the client out of service.

c. Network jamming attack

- This type of DoS targets the entire wireless network.
- The attacker simply builds or purchases a transmitter to flood the airwaves in the vicinity of the wireless network.

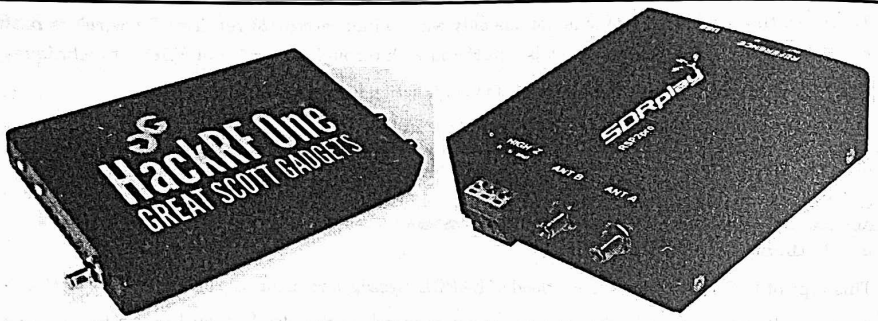
d. Equipment destruction attack

- This type of DoS targets the AP. The hacker uses a high-output transmitter with a directional high-gain antenna to pulse the AP.
- High-energy RF power will damage electronics in the WAP, resulting in its being permanently out of service.

5.8.2 Universal Radio Hacker

GQ. Write a Short note on URH.

- The Universal Radio Hacker (URH) is a tool for analyzing unknown wireless protocols. With the rise of Internet of Things (IoT) such protocols often appear in the wild. Many IoT devices operate on frequencies like 433.92 MHz or 868.3 MHz and use proprietary protocols for communication.
- Reverse-engineering such protocols can be fascinating (»What does my fridge talk about?«) and reveal serious security leaks, e.g. when bypassing smart alarm systems and door locks.
- So how can we join this game? **Software Defined Radios** (SDR) are the answer for this. Such devices allow sending and receiving on nearly arbitrary frequencies. Fig.5.8.2 shows two examples. Both devices cost about 200 euro



(a) HackRF One can send and receive on frequencies from 1 MHz to 6 GHz.

(b) SDRplay RSP2pro can receive on frequencies from 1 kHz to 2 GHz.

Fig. 5.8.2: Two examples for Software Defined Radios.

- Like the name suggests, SDRs need software to be properly operated. This is where the **Universal Radio Hacker** comes into play: It takes the samples from the SDR and transforms them into binary information (bits). But this is only the beginning: URH is designed to help you throughout the entire process of attacking the wireless communication of IoT devices.

Chapter Ends...

□□□

UNIT VI

CHAPTER 6

Recent Trends and Applications in Wireless Technology

Syllabus

5G NR (New Redio): Working, Benefits. Holographic MIMO Surfaces for 6G Wireless Networks, Simultaneous Transmission and Reflection (STAR) for 360° Coverage, Quantum technology for 5G/6G Wireless Networks. Applications of Wireless Technology.

6.1 5G NR (NEW REDIO)

6.1.1 What is 5G New Radio (NR)?

- 5G New Radio, or 5G NR, is a set of standards that replace the LTE network 4G wireless communications standard. An important goal of 5G NR is to support the growth of wireless communication by enhancing electromagnetic radiation spectrum efficiency for mobile broadband.
- 5G NR is designed to support fiber-equivalent bandwidth transmissions required for hungry applications like streaming video, as well as low-bandwidth transmissions used in machine-to-machine communications at massive scale where needed. 5G NR will also support transmissions with extremely low latency requirements -- an important consideration in vehicle-to-vehicle and vehicle-to-infrastructure communications.
- Similar to its predecessors, the 5G NR standard was created by the 3rd Generation Partnership Project (3GPP), a coalition of telecommunications organizations that create technical standards for wireless technology. The first iteration of 5G NR appeared in 3GPP Release 15.

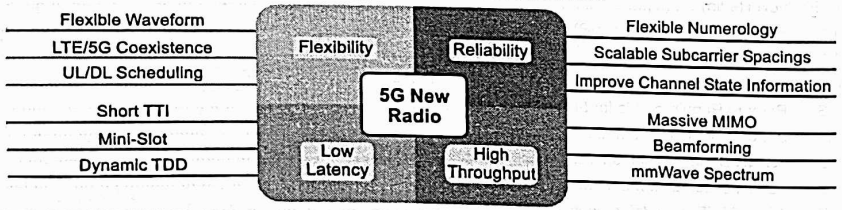


Fig 6.1.1 : The Major Characteristics of 5G NR

6.1.2 How does 5G NR work?

GQ. How does 5G NR work?

- 5G NR employs a raft of new engineering techniques that move more data through the core network faster and revolutionize the discrete operations of the air interface, which is the client device's interaction with the network provider radio hardware.
- Some of the improvements that 5G NR introduces are the following :
  - Diversity of spectrum that ranges from several hundred kilohertz to millimeter wave (mmWave) to enable various use cases, cell sizes and data rates;
  - Modulation -- new orthogonal frequency-division multiplexing methods -- and channel-coding techniques;
  - Frequency reuse algorithms, even in dense environments;
  - Massive multiple input, multiple output and evolved beamforming capabilities; and
  - Slot time operations developed to deliver ultralow-latency communications.
- All of these capabilities are underpinnings of 5G NR's significant gains in capacity, throughput and coverage.

6.1.3 Primary Requirements for 5G NR

- In order for a connection to qualify as 5G NR, several performance and connectivity requirements must be met. Some of these requirements are the following:
- The connection must support wireless mobile connections.
- Connectivity must support the internet of things (IoT), a concept that includes all of the various devices and wired or wireless connections that make up a user's digital experience, as well as sensor-type headless client devices.
- It must implement a lean signaling design. This means that signals are only switched on when needed, lowering the overall processing power required of the client devices.
- The connection must use adaptive bandwidth, which enables devices to switch to a low bandwidth and lower power whenever possible, saving energy for when higher bandwidths are necessary.
- 5G NR should also enforce strict data transmission requirements. By forcing all users and connections to respect specific rules, it makes the entire network faster and more efficient.

6.1.4 Benefits of 5G NR

The benefits of 5G New Radio over even the best Long-Term Evolution (LTE)networks include the following :

- Larger wireless area capacity;
- Increased energy savings per device;
- Lower period of time between updates -- i.e., reduced average service creation time cycle;
- Improved links connecting larger number of users;
- Improved technology for maintaining the quality of a connection over a broad geographical area;
- Enhanced speed and data rates, meaning more bits are processed over a unit of time; and
- Improved efficiency in data sharing.

6.1.5 5G NR Deployment Modes

- As is often the case with new wireless technology rollouts, there are various ways that 5G NR can be brought to life at a given site. Which deployment mode to use depends on several factors, including the existing infrastructure, whether or not a greenfield project is in play and what client types are expected in the 5G NR service area.
- The three main 5G NR deployment modes are the following:
  (1) For **standalone mode**, the full 5G technical paradigm is deployed. No residual 4G technical underpinnings are involved. And, if the clients can take advantage of the deployment, then all 5G benefits are realized.
  (2) In **nonstandalone mode**, a site is essentially a hybrid. Some 4G network infrastructure stays in place. While the radio frequency side of 5G NR presents benefits, what it uplinks into means a lesser overall experience, compared with standalone mode. This model permits carriers to phase in full 5G architecture at sites, enabling them to tout their 5G progress.

(3) In the third deployment mode, **dynamic spectrum sharing**, the same frequency can do time-sliced duty in both 4G and 5G modes, using advanced antenna and transceiver processing. This means no single spectrum band has to be dedicated to just 4G or 5G.

6.1.6 5G NR spectrum

- The 5G NR standard supports a number of low-, mid- and high-frequency bands. They are broken into frequency range 1, which includes frequency bands that are less than 6 gigahertz; frequency range 2, which includes bands with a low range combined with a high bandwidth; and mmWave.
- The bands supported by 5G NR also include licensed spectrum and unlicensed spectrum 5G NR-U, which include bands than can be accessed by anyone. This wide diversity of spectrum slices is unique to 5G NR but helps to meet the demands of the spectrum-intensive technology.

6.1.7 5G and LTE: Key differences and bridging the gap

GQ. What is Key Difference between 5G and LTE ?

- As LTE's incumbency yields to 5G, it's important to understand how the two technologies compare.
- 5G NR network architecture will diverge from LTE's tower-centric model somewhat because the higher frequencies in use require high quantities of smaller pole- and building-mounted nodes to get the network to users. While carrier mobile networks go through the rigors of updating their infrastructures for 5G NR, consumers and businesses can follow the progress at a number of websites.
- For private 5G NR deployments, Citizens Broadband Radio Service provides a compelling option. It's also worth noting that 5G networks need compatible clients to truly take advantage of the new technology's promise, and we are seeing ever more 5G client devices. Lastly, 5G NR continues to develop in phases, just as 4G/LTE did. So, not all 5G NR networks will be the same from a capability and capacity standpoint at any given time.
- 5G NR brings advancements in cellular technologies not found in 4G. These advancements deliver impressive benefits and fulfill the ultimate goal of being ultrareliable. Some of the advancements are the following :
  - **Flexible numerology** is a complex engineering concept that enables dynamic adaptation of time slots and subcarrier spacing to achieve low latency for applications that need it, as well as provide coexistence between LTE and NR where required.
  - **Hybrid automatic repeat request (HARQ)** is occasionally mentioned in 5G NR discussions. HARQ works at the lowest network layers to adaptively optimize forward error correction and retransmit functions for lower bit error rates.
  - **Time-division duplexing (TDD)** is a technique in which uplink and downlink functions happen on the same frequency. As expected, in 5G NR, TDD has been retooled for speed and flexibility.
  - **Inactive state** is a power-saving enhancement in 5G NR that augments 4G's idle and connected At its simplest, the new inactive state reduces load on the control plane at scale where many devices need to come out of sleep mode to transmit data.

6.2 HOLOGRAPHIC MIMO SURFACES FOR 6G WIRELESS NETWORKS

GQ. Explain Concept of Holographic MIMO surface.

GQ. Explain different hmimos design models.

GQ. Enlist and explain application of Holographic MIMO surface.

6.2.1 Introduction

- Future wireless networks, namely beyond fifth Generation (5G) and sixth Generation (6G), are required to support massive numbers of end-users with increasingly demanding Spectral Efficiency (SE) and Energy Efficiency (EE) requirements.
- In recent years, research in wireless communications has witnessed rising interests in massive Multiple Input Multiple Output (MIMO) systems, where Base Stations (BSs) are equipped with large antenna arrays, as a way to address the 5G throughput requirements. However, it is still a very challenging task to realize massive MIMO BSs with truly large-scale antenna arrays (i.e., with few hundreds or more antennas) mainly due to the high fabrication and operational costs, as well as due to the increased power consumption.
- **Future 6G wireless communication systems are expected to realize an intelligent and software reconfigurable paradigm, where all parts of device hardware will adapt to the changes of the wireless environment.** Beamforming-enabled antenna arrays, cognitive spectrum usage, as well as adaptive modulation and coding are a few of the transceiver aspects that are currently tunable in order to optimize the communication
- Holographic MIMO Surfaces (HMIMOS) aim at going beyond massive MIMO, being based on low cost, size, weight, and low power consumption hardware architectures that provide a transformative means of the wireless environment into a programmable smart entity.

6.2.2 Hmimos Design Models

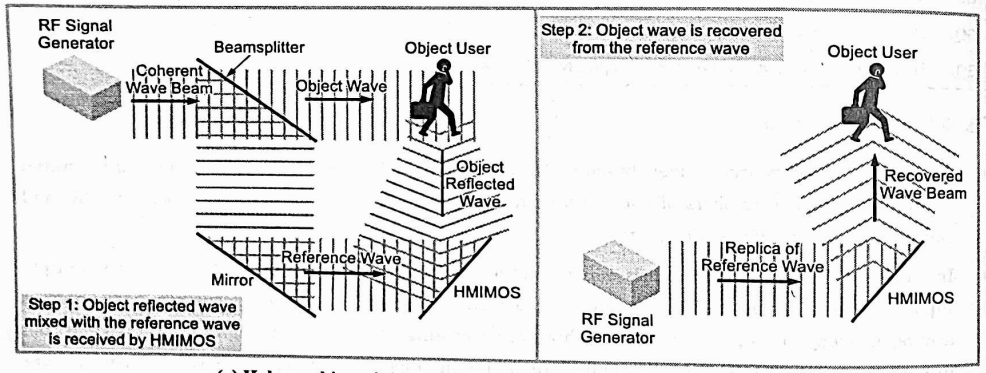
In this section, we present available hardware architectures, fabrication methodologies, and operation modes of HMIMOS systems that render them a flexibly integrable concept for diverse wireless communication applications.

(A) Categorization based on the Power Consumption

(1) Active HMIMOS

- To realize reconfigurable wireless environments, HMIMOS can serve as a transmitter, receiver, or reflector. When the transceiver role is considered, and thus energy-intensive Radio Frequency (RF) circuits and signal processing units are embedded in the surface, the term active HMIMOS is adopted.

- On another note, active HMIMOS systems comprise a natural evolution of conventional massive MIMO systems, by packing more and more software-controlled antenna elements onto a two-Dimensional (2D) surface of finite size.



(a) Holographic training (b) Holographic communicating

Fig. 6.2.1 : The two generic steps of holographic training and holographic communication

- In, where the spacing between adjacent surface elements reduces when their number increase, an active HMIMOS is also termed as Large Intelligent Surface (LIS).
- A practical implementation of active HMIMOS can be a compact integration of an infinite number of tiny antenna elements with reconfigurable processing networks realizing a continuous antenna aperture. This structure can be used to transmit and receive communication signals across the entire surface by leveraging the hologram principle. Another active HMIMOS implementation is based on discrete photonic antenna arrays that integrate active optical-electrical detectors, converters, and modulators for performing transmission, reception, and conversion of optical or RF signals.

(2) Passive HMIMOS

- Passive HMIMOS, also known as Reconfigurable Intelligent Surface (RIS) , or Intelligent Reflecting Surface (IRS) , acts like a passive metal mirror or 'wave collector,' and can be programmed to change an impinging EM field in a customizable way.
- Compared with its active counterpart, a passive HMIMOS is usually composed of low cost passive elements that do not require dedicated power sources. Their circuitry and embedded sensors can be powered with energy harvesting modules, an approach that has the potential of making them truly energy neutral.

(B) Categorization based on the Hardware Structure

(1) Contiguous HMIMOS

- A contiguous HMIMOS integrates a virtually uncountably infinite number of elements into a limited surface area in order to form a spatially continuous transceiver aperture. For the better understanding of the operation of contiguous surfaces and their communication models.
- Holography is a technique that enables an EM field, which is generally the result of a signal source scattered off objects, to be recorded based on the interference principle of the EM wave.
- The recorded EM field can be then utilized for reconstructing the initial field based on the diffraction principle. It should be noted that wireless communications over a continuous aperture is inspired by the optical holography, which is sketched in Fig. 6.2.1.
- In the training phase, the generated training signals from an RF source are split via a beamsplitter into two waves, the object and reference waves.
- The object wave is directed to the object, and some of the reflected wave mixed together with the reference wave beam that does not impinge on the object, are fed to the HMIMOS.
- In the communication phase, the transmitted signal is transformed into the desired beam to the object user over the spatially continuous aperture of the HMIMOS. Since the continuous aperture benefits from the integrated infinite number of antennas that is the asymptotic limit of Massive MIMO, its potential advantages are to achieve higher spatial resolution, and enable the creation and detection of EM waves with arbitrary spatial frequency components, without undesired side lobes.

(2) Discrete HMIMOS

- The discrete HMIMOS is usually composed of many discrete unit cells made of low power software-tunable metamaterials.
- The means to electronically modify the EM properties of the unit cells range from off the shelves electronic components to using liquid crystals, microelectromechanical systems or even electromechanical switches, and other reconfigurable metamaterials. This structure is substantially different from the conventional MIMO antenna array.
- One embodiment of a discrete surface is based on discrete 'meta-atoms' with electronically steerable reflection properties.
- As mentioned earlier, another type of discrete surface is the active one based on photonic antenna arrays. Compared with contiguous HMIMOS, discrete HMIMOS have

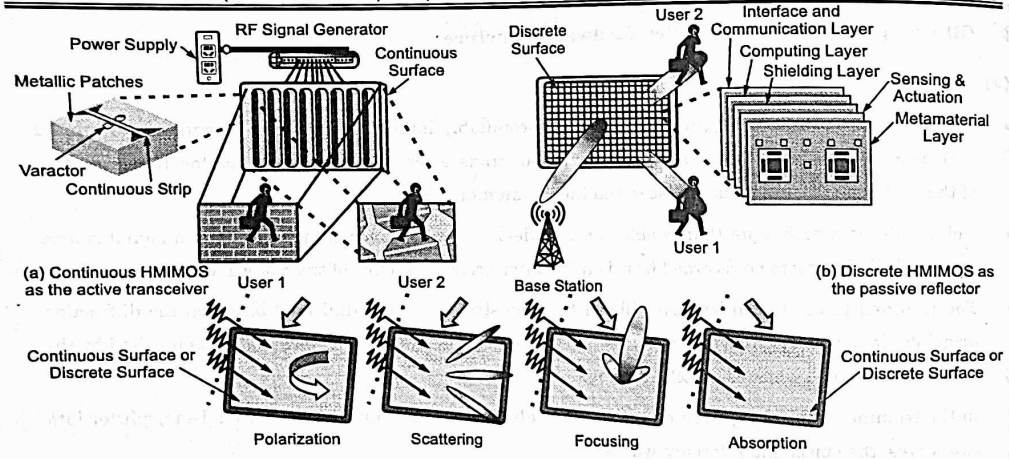


Fig. 6.2.2 : The two operation modes of HMIMOS systems along with their implementation and hardware structures.

- Continued prototyping development is highly desired to both prove the HMIMOS concept with even brand new holographic beamforming technologies and discover potentially new issues that urgently need research.

(C) Operation Modes

The following four operation modes for HMIMOS are usually considered :

(1) Continuous HMIMOS as an active transceiver;
(2) Discrete HMIMOS as a passive reflector;
(3) Discrete HMIMOS as an active transceiver; and
(4) Continuous HMIMOS as a passive reflector.

1) Continuous HMIMOS as Active Transceivers:

- According to this mode of operation, the continuous HMIMOS performs as an active transceiver. The RF signal is generated at its backside and propagates through a steerable distribution network to the contiguous surface constituted by the infinite software-defined and electronically steerable elements that generate multiple beams to the intended users.
- A distinct difference between active continuous HMIMOS and passively reconfigurable HMIMOS is that the beamforming process of the former is accomplished based on the holographic concept, which is a new dynamic beamforming technique based on software-defined antennas with low cost/weight, compact size, and a low-power hardware architecture.

2) Discrete HMIMOS as Passive Reflectors:

- Another operation mode of HMIMOS is the mirror or 'wave collector,' where the HMIMOS is considered to be discrete and passive.
- In this case, the HMIMOS include reconfigurable unit cells, as previously described, which makes their beamforming mode resembling that of conventional beamforming, unlike continuous transceiver HMIMOS systems.
- It is worth noting that most of the existing works focus on this HMIMOS operation mode which is simpler to implement and analyze.

6.2.3 Applications

(1) **Outdoor Applications :** Consider the discrete passive HMIMOS as an indicative example that comprises a finite number of unit elements, and intended for forwarding suitably phase-shifted versions of its impinging signals to users over different outdoor scenarios, such as typical urban, shopping malls, and international airports, as illustrated in the upper part of Fig. 6.2.2. We assume that HMIMOS are planar structures of few centimeters thickness and variable sizes that can be easily deployed onto nearly all environmental objects.

A1 : Building connections : HMIMOS can extend the coverage from outdoor BSs to indoor users, especially in cases where there is no direct link between the users and BS, or the link is severely blocked by obstacles.

A2 : Energy-efficient beamforming : HMIMOS are capable of recycling ambient EM waves and focusing them to their intended users via effective tuning of their unit elements. In such cases, surfaces are deployed as relays to forward the information bearing EM field to desired locations via efficient beamforming that compensates for the signal attenuation from the BS or co-channel interference from neighboring BSs.

A3 : Physical-layer security : HMIMOS can be deployed for physical layer security in order to cancel out reflections of the BS signals to eavesdroppers.

A4 : Wireless power transfer : HMIMOS can collect ambient EM waves and direct them to power-hungry IoT devices and sensors enabling also simultaneous wireless information and power transfer.

(2) **Indoor Applications :** Indoor wireless communication is subject to rich multipath propagation due to the presence of multiple scatters and signal blocking by walls and furniture, as well as RF pollution due to the highly probable densification of electronic devices in confined spaces. As such, providing ubiquitous high throughput indoor coverage and localization is a challenging task. HMIMOS has the potential of being highly beneficial in indoor environments, leveraging from its inherit capability to reconfigure EM waves towards various communication objectives. An illustrative general example is sketched in the lower part of Fig. 6.2.2. In the left corner of this example where a HMIMOS is absent, the signal experiences pathloss and multipath fading due to refraction, reflection, and diffusion, which deteriorates its sufficient propagation to the target user. However, in the right corner of Fig. 6.2.2,

signal propagation can be boosted using HMIMOS coated in the wall so as to assist the signal from the access point to reach the intended user with the desired power level.

A5 : Enhanced in-building coverage : As previously discussed, indoor environments can be coated with HMIMOS to increase the throughput offered by conventional Wi-Fi access points. • A6: High accurate indoor positioning: HMIMOS has increased potential for indoor positioning and localization, where the conventional Global Positioning System (GPS) fails. Large surfaces offer large, and possibly continuous, apertures that enable increased spatial resolution. There has been lately increasing research interest in wireless communication systems incorporating HMIMOS.

6.3 SIMULTANEOUS TRANSMISSION AND REFLECTION (STAR) FOR 360° COVERAGE

GQ. Explain Simultaneous Transmission and Reflection (STAR) for 360° Coverage in details.
GQ. Differences between reflecting-only riss and star-riss.
GQ. Enlist and Explain applications of star-riss in 6G.

6.3.1 Introduction

- With the rapid development of metasurfaces and the corresponding fabrication technologies, reconfigurable intelligent surfaces (RISs) and their diverse variants have emerged as promising techniques for sixth-generation (6G) wireless networks.
- Generally speaking, RISs are two-dimensional (2D) structures and are comprised of a large number of low-cost reconfigurable elements. By employing a smart controller (e.g., a field-programmable gate array (FPGA)) attached to the RIS, both the phase and even the amplitude of these reconfigurable elements can be beneficially controlled, thus reconfiguring the propagation of the incident wireless signals and realizing a "Smart Radio Environment (SRE)".
- Since no radio frequency (RF) chains are required, RISs are more economical and environmentally friendly than the family of conventional multi-antenna and relaying technologies. Given these beneficial RIS characteristics, extensive industrial and academic research efforts have been devoted to the investigation of RISs, including but not limited to the design of energy efficient communication, the mitigation of blockages in millimeter wave (mmWave)/terahertz (THz) communications , and their artificial intelligence (AI) aided implementation.
- However, the existing contributions mainly focus on RISs whose only function is to reflect an incident signal, hence both the source and the destination have to be at the same side of the RISs, i.e., within the same half-space of the SRE.
- Unfortunately, this topological constraint limits the flexibility of employing conventional RISs. To address this issue, we advocate the concept of simultaneously transmitting and reflecting RISs (STAR-RISs), where the incident wireless signals can be reflected within the half-space of the SRE at the same side of the RIS, but they can also be transmitted to the other side of the RIS. As a result, a full-space SRE can be created by STAR-RISs.

From Conventional Reflecting-Only RISs to STAR-RISs

- Three types of signal propagation, namely full reflection, full transmission, as well as simultaneous transmission and reflection, based on a prototype developed by researchers from NTT DOCOMO, Japan. Fig. 6.3.1(a) depicts NTT DOCOMO's prototype, where a metasurface is covered by a transparent substrate made of glass. By modifying the distance between the metasurface and the transparent substrate, the aforementioned three types of signal propagation can be achieved, as shown in Figs. 6.3.1(b)-6.3.1(d).
- For the full reflection scenario of Fig. 6.3.1(b), the incident signals are completely reflected and cannot penetrate the surface. This type of wireless signal manipulation is widely investigated for conventional reflecting-only RISs. By contrast, for the full transmission scenario of Fig. 6.3.1(c), all incident signals pass through the surface into the transmission space, while no signal is reflected.
- Finally, for the simultaneous transmission and reflection scenario of Fig. 6.3.1(d), the incident signals are divided into two parts by the surface. Part of the signal is reflected to the reflection space, while the remaining part is radiated into the transmission space, thus facilitating the full-space manipulation of signal propagation.

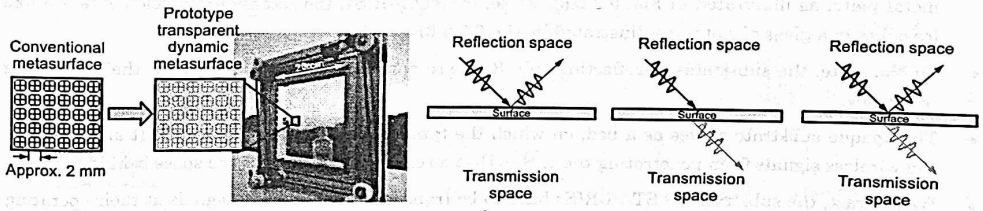


Fig. 6.3.1 : Signal propagation in STAR-RIS

- Key Advantages and Motivations for Employing STAR-RISs in Wireless Communication Systems Considering the above unique features, the employment of STAR-RISs has the following advantages in wireless communication systems :
  (1) Thanks to their capability of simultaneously transmitting and reflecting the incident signals, the coverage of STAR-RISs is extended to the entire space, thus serving both half-spaces using a single RIS, which is not possible for conventional reflecting-only RISs.
  (2) STAR-RISs provide enhanced degrees-of-freedom (DoFs) for signal propagation manipulation, which significantly increases the design flexibility in satisfying stringent communication requirements.
  (3) Since STAR-RISs are generally designed to be optically transparent, they are aesthetically pleasing and readily compatible with existing building structures, such as windows. Therefore, STAR-RISs will have no undesired aesthetic effect, which is of vital importance for practical implementations. Note that the joint manipulation of transmission and reflection is not a completely new idea, especially from the perspectives of the physics and metasurface technology. Apart from the above

NTT DOCOMO prototype , the suthors of have also proposed concepts similar to 'STAR'. Frequency-selective refection and transmission of signals by using a dual-band bi-functional metasurface structure. For the STAR-RISs considered, the transmitted and reflected signals can be simultaneously reconfigured by each element via two generally independent coefficients, namely the transmission and reflection coefficients. This distinct characteristic facilitates the flexible design of STAR-RIS-aided wireless networks. However, the wireless communication design of STAR-RISs is still in its infancy. This motivates us to provide a systematic introduction to STAR-RISs, including their fundamental differences wrt conventional reflecting-only

6.3.2 Key Differences Between Reflecting-Only Riss And Star-Riss

Hardware Design Differences

- Reflecting-only RISs and STAR-RISs are different both in terms of their equipped elements and substrates.
- The following analogy illustrates the structural differences between reflecting-only RISs and STAR-RISs. For reflecting-only RISs, the reconfigurable elements on the substrate are like biscuits placed on a metal plate, as illustrated in Fig. 6.3.2(a), while, for STAR-RISs, the reconfigurable elements are like ice cubes in a glass of water, as illustrated in Fig. 6.3.2(b).
- To elaborate, the substrates of reflecting-only RISs are opaque for wireless signals at their operating frequency.
- The opaque substrate serves as a bed, on which the tunable elements are integrated. It also prevents the wireless signals from penetrating the RIS so that no energy is leaked into the space behind the RIS.
- By contrast, the substrates of STAR-RISs have to be transparent for wireless signals at their operating frequency.

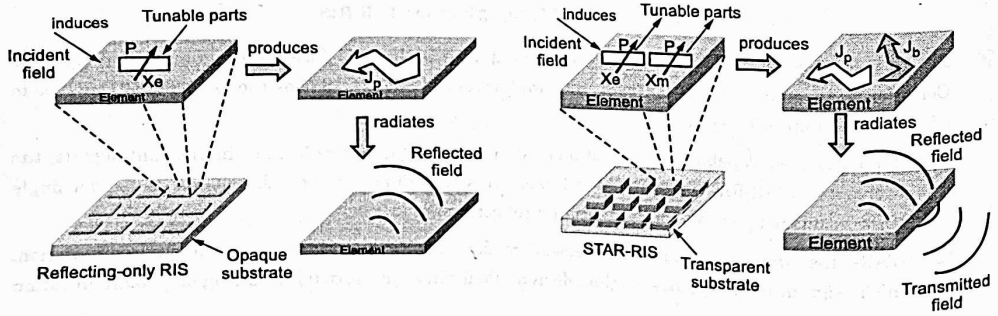


Fig 6.3.2 : Key Differences Between Reflecting-Only Riss And Star-Riss

Promising applications of star-riss in 6G

Applications of STAR-RISs in next-generation networks for both outdoor and indoor environments, as illustrated in Fig. 6.3.3.

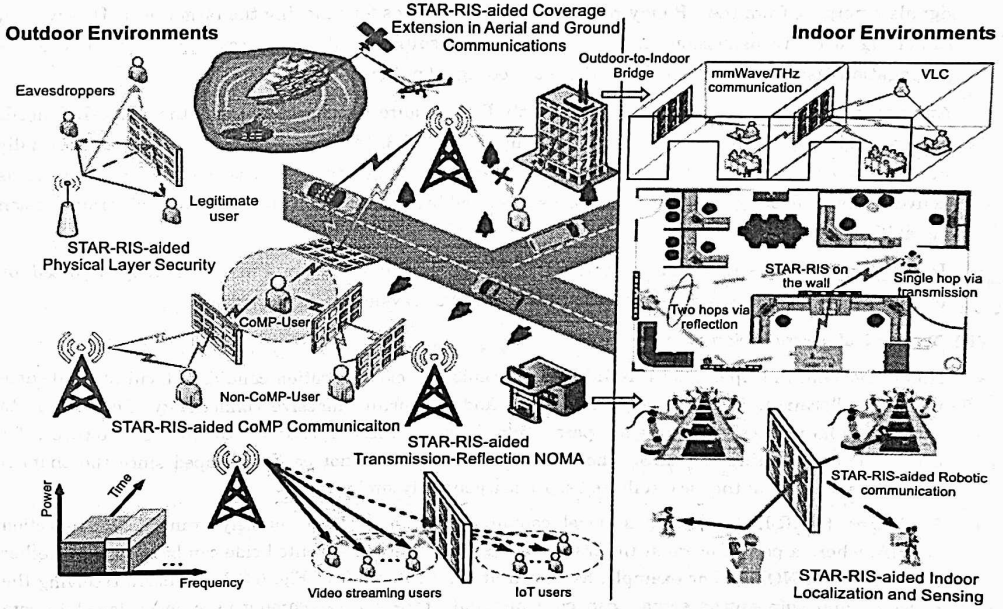


Fig. 6.3.3 : Illustration of application scenarios of STAR-RISs in wireless communications for outdoor and indoor environments.

(A) Outdoor, Outdoor-Indoor, and Indoor Coverage

- Extension One of the most promising applications of STAR-RISs is to improve the coverage area/quality of wireless networks, especially when the links between the base stations (BSs) or access points (APs) and users are severely blocked by obstacles (e.g., trees along roads, buildings, and metallic shells of vehicles). As shown at the top right of Fig. 6.3.3, STAR-RIS aided coverage extension can be loosely divided into three scenarios, namely outdoor, outdoor-to-indoor, and indoor. In outdoor communications, similar to conventional reflecting-only RISs, STAR-RISs can be mounted on building facades and roadside billboards to create an additional communication link. More innovatively, STAR-RISs can also be accommodated by the windows of vehicles (e.g., cars, aircraft, and cruise ships) to enhance the signal strength received inside by exploiting their transmission capability, thus extending the coverage area/quality of BSs and satellites.
- For outdoor-to-indoor communications, the severe penetration loss caused by building walls gravely restricts the coverage provided by outdoor BSs, especially in mmWave and THz communications.

- In fact, STAR-RISs constitute an efficient technique for creating an outdoor-to-indoor bridge as illustrated in Fig. 6.3.3. For indoor communications, STAR-RISs are more appealing than conventional reflecting-only RISs. As conventional reflecting-only RISs merely achieve half-space coverage, the signals emerging from the AP may require multi-hop bounces for reaching the target user. However, by exploiting both transmission and reflection, the resultant full space coverage may reduce the propagation distance, thus increasing the received signal power.
- An example, where conventional reflecting-only RISs require two hops, whereas the STAR-RIS needs only a single hop, is illustrated at middle right of Fig. 6.3.3. In a nut shell, STAR-RISs substantially outperform conventional reflecting-only RISs, since they do not only possess the same capabilities as conventional reflecting only RISs but also support additional design options due to their transmission capability.
- Depending on the application scenarios, transmission and reflection can be suitably adjusted by employing the three operating protocols proposed in the previous section.

(B) Transmission-Reflection NOMA

- Non-orthogonal multiple access (NOMA) is a promising next-generation candidate facilitating flexible resource allocation, high spectrum efficiency, and supporting massive connectivity. For NOMA to achieve a large performance gain pair users having different channel conditions. However, for conventional reflecting-only RISs, the benefits of NOMA may not be fully reaped since the channel conditions of users in the local reflected space are generally similar.
- Exploiting STAR-RISs enables a novel communication framework, namely transmission-reflection NOMA, where a pair of users at the transmission- and reflection-oriented side can be grouped together for facilitating NOMA. For example, as shown at the bottom left of Fig. 6.3.3, the users receiving the reflected and transmitted signals can be a high-data rate video-streaming user and a low-data rate Internet-of-Things (IoT) user, respectively.
- By carefully optimizing the element based energy splitting ratio of the proposed ES protocol or the element-based mode selection of the proposed MS protocol, sufficiently different transmitted and reflected channel conditions can be achieved. As a result, the proposed STARRIS- aided transmission-reflection NOMA framework is well suited to support the heterogenous quality-of-service (QoS) requirements of the two types of users.

(C) Coordinated Multi

Point Communication via Transmission and Reflection For realistic multi-cell communication networks, the performance of cell-edge users cannot be guaranteed due to the strong inter-cell interference. Coordinated multi-point (CoMP) communication efficiently mitigates the inter-cell interference.

(D) Full-space Physical Layer Security

- RISs are also capable of improving the physical layer security (PLS), where the channel conditions of the eavesdroppers can be degraded by degrading their signal propagation. However, for conventional reflecting-only RISs aided secure communication, the legitimate users and eavesdroppers are assumed to be located at the same side of the RISs, even though this idealized simplifying assumption may not hold in practice.

- Fortunately, STAR-RISs come to the rescue. Observe at the top left of Fig. 6.3.3, with the assistance of full-space STAR-RIS propagation, PLS can be enhanced, regardless of the eavesdropper location.

(E) Indoor Localization and Sensing

- By overcoming signal blockages and providing full-space coverage, STAR-RISs are capable of improving both the localization and sensing capability of wireless networks, especially in indoor environments. As illustrated at the bottom right of Fig. 6.3.3, the employment of STAR-RISs in smart factories improves the positioning of mobile robots and the data-rate of control links.
- There are also other promising application scenarios for STAR-RISs in 6G networks, such as STAR-RIS-aided simultaneous wireless information and power transfer (SWIPT), STAR-RIS-assisted visible light communications (VLCs), STAR-RIS-aided mmWave/THz communications, and STARRIS- augmented robotic communications. These applications constitute interesting future research directions.

6.4 QUANTUM TECHNOLOGY FOR 5G/6G WIRELESS NETWORKS

6.4.1 Introduction to Quantum Technology For 5G/6G Wireless Networks

- In the last several years, quantum technology rollout has accelerated at an unparalleled rate. Added to this, the implementation of low-latency and ultra-broadband network infrastructures such as 5G networks has led to a global digitization of various fields. However, only Beyond-5G (B5G) networks will be able to provide completely intelligent network orchestration in order to provide revolutionary services. Thus, 5G exhibits many fascinating capabilities but 6G will be needed in the coming time for providing novel telecommunication services with high productivity.
- Researchers and tech enthusiasts are thus working profoundly in laying the foundation for 6G networks. Quantum Computing will play a major role in this transition from 5G to 6G communications systems, consequently paving way for smart systems and advanced computing.
- Quantum computers exploit benefits of quantum parallelism, which enables exponentially faster processing than classical computing and, in some cases, quantum supremacy such as in some optimization problems.
- Quantum Processing Units will be the name for next-generation processor units that use quantum computing (QPUs). Google's Sycamore, for example, is a QPU.

6.4.2 Quantum Information Technology

- Quantum Information Technology will harness quantum physics' capacity to usher in a revolutionary new era of technology.
- The theoretical groundwork and the building blocks for quantum communications, quantum computers, quantum sensing, and quantum metrology is laid by Quantum mechanics.

6.4.3 Quantum Computing

- Quantum Computing is the computing concept built upon the principles of quantum theory like superposition and entanglement.
- Instead of classical bits, qubits (quantum analogue of classical bits) are used for computing. These qubits reflect the behavior of material energy at different atomic and subatomic levels and can exist in more than one state (both "0" and "1" at the same time).
- Quantum Computing is based on 2 principles: Superposition and Entanglement. Entanglement, for example, may be used not just for quantum communications. It may also be used for quantum sensing and quantum computation.
- Furthermore, quantum communications and quantum computing may complement one another and be merged to transform the traditional internet into the quantum internet of the future. Quantum Communications is the domain of QIT aims at efficient and secure transfer of information through quantum computing. It is based on the principles of quantum mechanics, quantum information processing and quantum teleportation.
- The quantum cryptographic model which is developed using all these principles helps in secure transmission of qubits between 2 different quantum servers. Quantum key distribution (QKD) is the most well-known application of quantum cryptography.
- Quantum Sensing and Metrology is domain aims at eliminating or reducing all sorts of noise produced by quantum fluctuations by using the principles of quantum physics. It involves measurement of the magnitude and direction of tiny magnetic fields and interferometric measurements of phase shifts using atomic ensembles, trapped ions, solid-state atom like systems and cold atoms. It has been proposed that qubits used for sensing quantum components and energies on the basis of their quantum states will set the foundation of new hardware for sensing and metrology.

6.4.4 Quantum Computing in 5G/6G Communication Systems

- In the future, the progressively demanding performance fulfillment of the deployment of new technologies like may finally be triggered by emerging networks from surfaces with very large intelligence, electron-orbital angular momentum, visible light communications and cell-free technology communication.
- The field of quantum communication has also been picking up steam in recent years and is likely to contribute substantially towards two of the essential criteria of 5G/6G, as it enhances data security and reliability. The inherent security of quantum entanglement, which cannot be duplicated or accessed without tampering, suggests that it is suitable for systems that use 6G and beyond. Quantum communication is not the answer to all security and privacy concerns, however. Many works have demonstrated the feasibility of Quantum Key Distribution (QKD) and associated protocols.
- Another advantage of quantum communications is that they can be adapted to wide area communications. Even though quantum cryptography for quantum communication has advanced significantly over the past few years, long-distance quantum communication is still difficult due to the attenuation of fibers and operational errors. The current repeater concept, however, will not work for quantum communication since entanglement cannot be cloned.

6.5 APPLICATIONS OF WIRELESS TECHNOLOGY

GQ. Enlist and Explain Applications of Wireless Technology

☞ **Following is a list of applications in wireless Technology :**

Vehicles

Many wireless communication systems and mobility aware applications are used for following purpose:

- Transmission of music, news, road conditions, weather reports, and other **broadcast information** are received via digital audio broadcasting (DAB) with 1.5Mbit/s.
- For **personal communication,** a universal mobile telecommunications system (UMTS) phone might be available offering voice and data connectivity with 384kbit/s.
- For **remote areas,** satellite communication can be used, while the current position of the car is determined via the GPS (Global Positioning System).
- A local ad-hoc network for the fast **exchange of information** (information such as distance between two vehicles, traffic information, road conditions) in emergency situations or to help each other keep a safe distance. Local ad-hoc network with vehicles close by to prevent guidance system, accidents, redundancy.
- Vehicle data from buses, trucks, trains and high speed train can be transmitted in advance for **maintenance.**
- In ad-hoc network, car can comprise personal digital assistants (PDA), laptops, or mobile phones connected with each other using the Bluetooth technology.

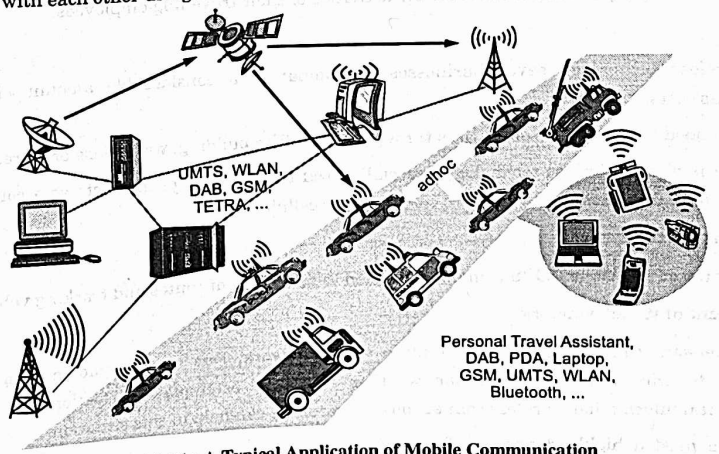


Fig. 6.5.1 : A Typical Application of Mobile Communication

☞ **Emergency**

Following services can be provided during emergencies:

- **Video communication :** Responders often need to share vital information. The transmission of real time situations of video could be necessary. A typical scenario includes the transmission of live video footage from a disaster area to the nearest fire department, to the police station or to the near NGOs etc.
- **Push To Talk (PTT) :** PTT is a technology which allows half duplex communication between two users where switching from voice reception mode to the transmit mode takes place with the use of a dedicated momentary button. It is similar to walkie-talkie.
- **Audio/Voice Communication :** This communication service provides full duplex audio channels unlike PTT. Public safety communication requires novel full duplex speech transmission services for emergency response.
- **Real Time Text Messaging (RTT) :** Text messaging (RTT) is an effective and quick solution for sending alerts in case of emergencies. Types of text messaging can be email, SMS and instant message.

☞ **Business**

Travelling Salesman

- Directly access to customer files stored in a central location.
- Consistent databases for all agents
- Mobile office
- To enable the company to keep track of all the activities of their travelling employees.

☞ **In Office**

- **Wi-Fi** wireless technology saves businesses or companies a considerable amount of money on installations costs.
- There is no need to physically setup wires throughout an office building, warehouse or store.
- **Bluetooth** is also a wireless technology especially used for short range that acts as a complement to Wi-Fi. It is used to transfer data between computers or cellphones.

☞ **Transportation Industries**

In transportation industries, GPS technology is used to find efficient routes and tracking vehicles.

☞ **Replacement of Wired Network**

- Wireless network can also be used to replace wired network. Due to economic reasons it is often impossible to wire remote sensors for weather forecasts, earthquake detection, or to provide environmental information, wireless connections via satellite, can help in this situation.
- Tradeshows need a highly dynamic infrastructure, since cabling takes a long time and frequently proves to be too inflexible.

- Many computers fairs use WLANs as a replacement for cabling.
- Other cases for wireless networks are computers, sensors, or information displays in *historical* buildings, where excess cabling may destroy valuable walls or floors.

☞ **Location dependent service**

It is important for an application to know something about the location because the user might need location information for further activities. Several services that might depend on the actual location can be described below:

Competitive questions on Structures in HindiKeep Watching

☞ **Follow-on Services**

- **Location aware services :** To know about what services (e.g. fax, printer, server, phone, printer etc.) exist in the local environment.
- **Privacy :** We can set the privacy like who should get knowledge about the location.
- **Information Services :** We can know about the special offers in the supermarket. Nearest hotel, rooms, cabs etc.

☞ **Infotainment : (Entertainment and Education)**

- Wireless networks can provide information at any appropriate location.
- Outdoor internet access.
- You may choose a seat for movie, pay via electronic cash, and send this information to a service provider.
- Ad-hoc network is used for multiuser games and entertainment.

☞ **Mobile and Wireless devices**

Even though many mobile and wireless devices are available, there will be many more devices in the future. There is no precise classification of such devices, by sizes, shape, weight, or computing power. The following list of given examples of mobile and wireless devices graded by increasing performance (CPU, memory, display, input devices, etc.)

- **Sensor :** Wireless device is represented by a sensor transmitting state information. 1 example could be a switch, sensing the office door. If the door is closed, the switch transmits this information to the mobile phone inside the office which will not accept incoming calls without user interaction; the semantics of a closed door is applied to phone calls.
- **Embedded Controller :** Many applications already contain a simple or sometimes more complex controller. Keyboards, mouse, headsets, washing machines, coffee machines, hair dryers and TV sets are just some examples.
- **Pager :** As a very simple receiver, a pager can only display short text messages, has a tiny display, and cannot send any messages.

- **Personal Digital Assistant :** PDAs typically accompany a user and offer simple versions of office software (calendar, notepad, mail). The typically input device is a pen, with built-in character recognition translating handwriting into characters. Web browsers and many other packages are available for these devices.
- **Pocket computer :** The next steps towards full computers are pocket computers offering tiny keyboards, color displays, and simple versions of programs found on desktop computers (text processing, spreadsheets etc.)
- **Notebook/laptop :** Laptops offer more or less the same performance as standard desktop computers; they use the same software - the only technical difference being size, weight, and the ability to run on a battery. If operated mainly via a sensitive display (touch sensitive or electromagnetic), the device are also known as notepads or tablet PCs.

Chapter Ends...

❑❑❑