Mobile Communication & Computing

(Code : CSC702)

(Semester VII : Computer Engineering)
(Mumbai University)

Strictly as Per the Choice Based Credit and Grading System (Rev. 2016) of Mumbai University w.e.f Academic Year 2019-2020

Dipali Y. Koshti

Assistant Professor,
Department of Computer Engineering
Fr. Conceicao Rodrigues College of Engg.(Fr.CRCE), Mumbai,
Maharashtra, India.

Nikahat Mulla

Assistant Professor,
Department of Computer Engineering,
Fr. Conceicao Rodrigues College of Engg. (Fr.CRCE), Mumbai,
Maharashtra, India.

TechKnowledge™ Publications

(Book Code : MO81A)

Mobile Communication & Computing

Dipali Y. Koshti, Nikahat Mulla

(Semester VII : Computer Engineering) (Mumbai University)

First Edition : July 2019

This edition is for sale in India, Bangladesh, Bhutan, Maldives, Nepal, Pakistan, Sri Lanka and designated countries in South-East Asia. Sale and purchase of this book outside of these countries is unauthorized by the publisher.

ISBN 978-93-89424-36-2

Published by

TechKnowledge Publications

Head Office : B/5, First floor, Maniratna Complex,
Taware Colony, Aranyeshwar Corner,
Pune - 411 009. Maharashtra State, India
Ph : 91-20-24221234, 91-20-24225678.

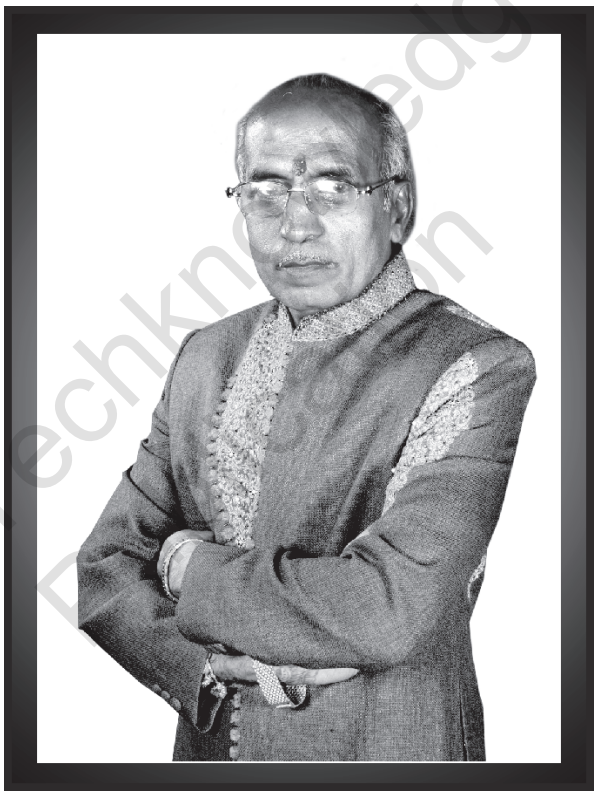
[CSC702] (FID : MO81) (Book Code : MO81A)

We dedicate this Publication soulfully and wholeheartedly,

in loving memory of our beloved founder director

Late Shri. Pradeepsheth Lalchandji Lunawat,

who will always be an inspiration, a positive force and strong support behind us.



Lt. Shri. Pradeepji L. Lunawat

Soulful Tribute and Gratitude for all Your Sacrifices, Hardwork and 40 years of Strong Vision.....

Preface

Dear Students,

We are extremely happy to come out with this edition of **"Mobile Communication & Computing"** for you. We have divided the subject into small chapters so that the topics can be arranged and understood properly. The topics within the chapters have been arranged in a proper sequence to ensure smooth flow and understanding of the subject.

We present this book in the loving memory of **Late Shri. Pradeepji Lunawat,** our source of inspiration and a strong foundation of **"TechKnowledge Publications"**. He will always be remembered in our hearts and motivate us to achieve our new milestone.

We are thankful to Prof. Arunoday Kumar, Mr. Shital Bhandari & Shri. Chandroday Kumar for the encouragement and support that they have extended. We are also thankful to the staff members of TechKnowledge Publications and others for their efforts to make this book as good as it is. We have jointly made every possible efforts to eliminate all the errors in this book. However if you find any, please let us know, because that will help us to improve the book quality further.

We are also thankful to our family members and friends for their patience and encouragement.

- Authors

❑❑❑

(Book Code : MO81A)

SYLLABUS

Course Code	Course Name	Credits
CSC702	Mobile Communication & Computing	4

Course Objectives (CO) :

1. To introduce the basic concepts and principles in mobile computing. This includes major techniques involved, and networks & systems issues for the design and implementation of mobile computing systems and applications.
2. To explore both theoretical and practical issues of mobile computing.
3. To provide an opportunity for students to understand the key components and technologies involved and to gain hands-on experiences in building mobile applications.

Course Outcomes : On successful completion of course learner will be able :

1. To identify basic concepts and principles in mobile communication & computing, cellular architecture.
2. To describe the components and functioning of mobile networking.
3. To classify variety of security techniques in mobile network.
4. To apply the concepts of WLAN for local as well as remote applications.
5. To describe and apply the concepts of mobility management
6. To describe Long Term Evolution (LTE) architecture and its interfaces.

Pre-requisites : Computer Networks

Module No.	Unit No.	Topics	Hrs.
1.0	1.1	Introduction to Mobile Computing, Telecommunication Generations, Cellular systems,	**6**
	1.2	Electromagnetic Spectrum, Antenna ,Signal Propagation, Signal Characteristics, Multiplexing, Spread Spectrum: DSSS & FHSS	
2.0	2.1	GSM Mobile services, System Architecture, Radio interface, Protocols , Localization and Calling, Handover, security (A3,A5 & A8)	**10**
	2.2	GPRS system and protocol architecture	
	2.3	UTRAN , UMTS core network ; Improvements on Core Network,	
3.0	3.1	Mobile Networking : Medium Access Protocol, Internet Protocol and Transport layer	**12**
	3.2	Medium Access Control: Motivation for specialized MAC, , Introduction to multiple Access techniques (MACA)	

Module No.	Unit No.	Topics	Hrs.
	3.3	Mobile IP: IP Packet Delivery, Agent Advertisement and Discovery, Registration, Tunneling and Encapsulation, Reverse Tunneling, Routing (DSDV,DSR)	
	3.4	Mobile TCP : Traditional TCP, Classical TCP Improvements like Indirect TCP, Snooping TCP & Mobile TCP, Fast Retransmit/ Fast Recovery, Transmission/Timeout Freezing, Selective Retransmission	
4.0	4.1	Wireless Local Area Networks : Introduction, Infrastructure and ad-hoc network	**08**
	4.2	IEEE 802.11:System architecture , Protocol architecture, Physical layer, Medium access control layer, MAC management, 802.11a, 802.11b	
	4.3	Wi-Fi security : WEP ,WPA, Wireless LAN Threats, Securing Wireless Networks	
	4.4	HiperLAN 1 & HiperLAN 2	
	4.5	Bluetooth: Introduction, User Scenario, Architecture, protocol stack	
5.0	5.1	Mobility Management : Introduction, IP Mobility, Optimization, IPv6	**06**
	5.2	Macro Mobility : MIPv6, FMIPv6,	
	5.3	Micro Mobility: CellularIP, HAWAII, HMIPv6,	
6.0	6.1	Long-Term Evolution (LTE) of 3GPP : LTE System Overview, Evolution from UMTS to LTE	**10**
	6.2	LTE/SAE Requirements, SAE Architecture	
	6.3	EPS: Evolved Packet System, E-UTRAN, Voice over LTE (VoLTE), Introduction to LTE-Advanced,	
	6.4	System Aspects, LTE Higher Protocol Layers, LTE MAC layer, LTE PHY Layer,	
	6.5	Self Organizing Network (SON-LTE),SON for Heterogeneous Networks (HetNet), Introduction to 5G	
		Total	**52**

❑❑❑

UNIT I

Syllabus :

Introduction to Mobile Computing, Telecommunication Generations, Cellular systems, Electromagnetic Spectrum, Antenna, Signal Propagation, Signal Characteristics, Multiplexing, Spread Spectrum : DSSS & FHSS

UNIT II

Syllabus :

GSM Mobile services, System Architecture, Radio interface, Protocols , Localization and Calling, Handover, security (A3,A5 & A8), GPRS system and protocol architecture, UTRAN, UMTS core network; Improvements on Core Network.

UNIT III

Syllabus :

Mobile Networking : Medium Access Protocol, Internet Protocol and Transport layer, Medium Access Control : Motivation for specialized MAC, Introduction to multiple Access techniques (MACA), Mobile IP: IP Packet Delivery, Agent Advertisement and Discovery, Registration, Tunneling and Encapsulation, Reverse Tunneling, Routing (DSDV,DSR), Mobile TCP : Traditional TCP, Classical TCP Improvements like Indirect TCP, Snooping TCP & Mobile TCP, Fast Retransmit/ Fast Recovery, Transmission/ Timeout Freezing, Selective Retransmission.

UNIT IV

Syllabus :

Wireless Local Area Networks : Introduction, Infrastructure and ad-hoc network, IEEE 802.11:System architecture, Protocol architecture, Physical layer, Medium access control layer, MAC management, 802.11a, 802.11b, Wi-Fi security : WEP, WPA, Wireless LAN Threats, Securing Wireless Networks, HIPERLAN 1 and HIPERLAN 2, Bluetooth : Introduction, User Scenario, Architecture, protocol stack

UNIT V

Syllabus :

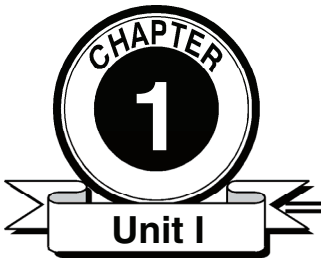
Mobility Management : Introduction, IP Mobility, Optimization, IPv6; Macro Mobility : MIPv6, FMIPv6; Micro Mobility : CellularIP, HAWAII, HMIPv6

UNIT VI

Syllabus :

Long-Term Evolution (LTE) of 3GPP : LTE System Overview, Evolution from UMTS to LTE; LTE/SAE Requirements, SAE Architecture; EPS: Evolved Packet System, E-UTRAN, Voice over LTE (VoLTE), Introduction to LTE-Advanced; System Aspects, LTE Higher Protocol Layers, LTE MAC layer, LTE PHY Layer; Self Organizing Network (SON-LTE),SON for Heterogeneous Networks (HetNet), Introduction to 5G

❑❑❑



Introduction to Mobile Computing

Syllabus

1.1 Introduction to Mobile Computing, Telecommunication Generations, Cellular systems,

1.2 Electromagnetic Spectrum, Antenna, Signal Propagation, Signal Characteristics, Multiplexing, Spread Spectrum : DSSS & FHSS

Introduction to mobile computing

Mobile Computing is a technology that allows transmission of data, voice and multimedia via any wireless enabled device without having to be connected to a fixed physical link. This chapter basically introduces the reader with the basics of mobile computing and communication. It also covers the journey of wireless communication from 1G to 5G and focuses on fundamental aspects of wireless transmission at physical layer such as signals, antenna, modulation, multiplexing. Most of today's wireless telecommunication systems are based on the concept of cellular systems. With billions of mobile phones in use around the globe today, it is necessary to re-use the available frequencies many times over without mutual interference of one cell phone to another.

1.1 Telecommunication Generations

The following section discusses different mobile generations (1G, 2G, 3G,4G and 5G).

First Generation (1G) : 1980s

- Analog cellular systems were the first generation of mobile telephone communication systems.
- They use **analog frequency modulation** and **circuit switched** techniques for voice transmission.
- The individual calls used different frequencies and shared the available spectrum through Frequency Division Multiple Access (FDMA).
- 1G system provided only voice communication.
- 1G was not supporting roaming between different network operators and countries.

  Examples of 1G networks are :
  - AMPS (Advanced Mobile Phone System) USA
  - NMT (Nordic Mobile Telephone) Sweden

Second Generation (2G) – 2.5 Generation (2.5G) : 1990s

- The second generation (2G) of mobile cellular started in the early 1990s.
- It was completely digital and used either Time Division Multiple Access (TDMA) or Code Division Multiple Access (CDMA).

- It provides increased capacity and security due to the uses of digital cellular technology.
- 2G systems support international roaming.
- 2G systems not only provide better voice quality using digital voice telephony but also a new range of low data rate services such as mobile Fax, voice mail, short message service (SMS).
- In addition to digital voice telephony, Cordless, public mobile radio, satellite and wireless-local area network (WLAN) solutions began to emerge.

2.5G

- Between 2G and 3G there was not much change in the technology hence an intermediary phase, 2.5G was introduced in the late 1990s.
- **2.5G** is used to describe 2G-systems that have implemented a packet-switched domain in addition to the circuit-switched domain.
- GPRS (General Packet Radio Service) is a 2G service, which delivers packet-switched data capabilities to existing GSM networks. It allows users to send graphics-rich data as packets.
- The importance of packet-switching increased with the rise of the Internet and the Internet Protocol (IP).
- Another example of 2.5G mobile technology is EDGE (Enhanced Data rates for GSM Evolution). EDGE provides data rate up to 384 kbps which is higher than GSM.

Advantages of 2G over 1G

- 2G standards support roaming between different operators and countries.
- In addition to circuit-switched voice services, 2G enabled the first wave of mobile data and Internet services, now widely adopted by users.
- 2.5G services enable high speed data transfer over upgraded existing 2G networks.

  Some 2G standards are :
  - GSM(TDMA-based)
  - D-AMPS
  - IS-95/CDMAone
  - PDC(Personal Digital Cellular)
  - PHS (Personal Handy Phone System)
  - HSCSD (High Speed Circuits Switched Data) (2.5)
  - GPRS (General Packet Radio Service) (2.5)
  - EDGE (Enhanced Data rates for Global Evolution)(2.5)

Third Generation (3G) - 2000

- The third generation (3G) systems started in 2000.
- The 3G revolution allowed mobile telephone customers to use audio, graphics and video applications.
- Over 3G it is possible to watch streaming video and engage in video telephony.
- They provide the ability to transfer simultaneously both voice data (a telephone call) and non-voice data (such as downloading information, exchanging email and instance messaging).
- 3G mobile technologies support greater number of voice and data customers as well as higher data rates at lower incremental cost than 2G.

3G standards are :

- W-CDMA
- CDMA2000
- UWC-136
- TD-CDMA / TD-SCDMA
- DECT

Fourth Generation (4G) - 2004

- The fourth generation will be fully IP-based integrated systems.
- It will allow accessing the Internet anytime from anywhere, global roaming, and wider support for multimedia applications.
- It will be network of networks achieved after the convergence of wired and wireless networks as well as computer, consumer electronics, communication technology, and several other convergences.
- These networks will be capable of providing 100 Mbps in outdoor environment and 1Gbps in indoor with end-to-end QoS and high security.

4G standards are :

- LTE (Long Term Evolution)
- WiMAX (Worldwide Interoperability for Microwave Access)

Fifth Generation - 5G (2018)

- 5G is not just one technology, it is actually a combination of several technologies in one. The system, however, will be a smart and know when to make use of which technology for maximum efficiency.
- 5G will be much more faster than 4G. It will provide data rate up to 10Gbps. It will provide 100% coverage area. That is better coverage even at the cell boundaries.
- 5G will also provide low network latency (up to 1 msec) which will be helpful for the critical applications like industry, healthcare and medical. 5G technology aims to provide wide range of future industries from retail to education, transportation to entertainment and smart homes to healthcare.
- 5G technology will provide ubiquitous connectivity means everything from vehicles to mobile networks to industries to smart homes will be connected together.
- 5G will utilize Extremely High frequency spectrum band between 3GHz to 30 GHz. These are called millimetre waves. These wave can travel at very high speed but covers short distance since they cannot penetrate obstacles.
- Unlike 4G that requires high powered cellular base stations to transmit signal over long distance, 5G will use a large number of small cell stations that may be located on small towers or building roofs.
- 5G makes the use of Massive MIMO (Multiple Input Multiple Output) standards to make is 100 times faster as opposed to standard MIMO. Massive MIMO makes the use of as much as 100 antennas. Multiple antennas allow for better and faster data transmission. The 5G network will come with 100 times more devices in market.

5G standards

- 5G technology standard are still under development. So, no firm standards is in place at this time; the market is still figuring out the essential 5G features and functionalities.
- The primary 5G standards bodies involved in these processes are the 3rd Generation Partnership Project (3GPP), the Internet Engineering Task Force (IETF), and the International Telecommunication Union (ITU).

Table 1.1.1 : Comparison between 1G, 2G, 3G, 4G and 5G

Parameter	1G	2G	3G	4G	5G
Introduced in	1980	1993	2001	2009	Currently under development expected to roll out by 2020
Technology	AMPS	D-AMPS, IS-95, GSM	W-CDMA CDMA2000 UWC-136 TD-CDMA DECT	LTE , WiMAX	LTE Advanced , OMA and NOMA, WWWW
Multiplexing	FDMA	TDMA/ CDMA	CDMA	CDMA	CDMA
Switching type	Circuit switching	Circuit switching for voice , packet switching for data	Packet switching	All Packet switching	All Packet switching
Speed	2.4 kbps to 14.4 kbps	14.4 kbps	3.1 mbps	100 mbps	>10 Gbps
Services	Voice only	Voice + data	Voice + data + Multimedia, video calling and video streaming	High speed High quality voice over IP, 3D gamming , HD video conferencing, HD multimedia streaming	Super fast internet access, Low latency network for mission critical applications, IoT and surveillance, autonomous driving and many more.
Bandwidth	Analog	25MHz	25 MHz	100 MHz	60GHz
Operating Features	800 MGHz	GSM: 900MHZ, 1800MHz CDMA: 800MHz	2100 MHz	2600 MHz	3 To 90 GHz
Band (Frequency) Type	Narrow band	Narrow Band	Wide band	Ultra Wide band	Extremely high frequency
Hand over	NA	Horizontal	Horizontal	Horizontal/ Vertical	Horizontal/ Vertical
Advantages	Simpler	Multimedia features (SMS, MMS), Internet access and SIM introduced	High security, international roaming	Speed, High speed handoffs, MIMO technology, Global mobility	Super fast internet, Low network latency , Ubiquitous connectivity, Global coverage.

Parameter	1G	2G	3G	4G	5G
Disadvantages	Limited capacity, not secure, poor battery life, large phone size, background interference	Low network range, slow data rates	High power consumption, Low network coverage, High cost of spectrum license	Hard to implement, complicated hardware required	Hard to implement, Many of the old devices would not be competent to 5G, Developing infrastructure needs high cost.
Applications	Voice Calls	Voice calls, Short messages, browsing (partial)	Video conferencing, mobile TV, GPS	High speed applications, mobile TV, Wearable devices	Super High speed mobile networks, Smart Vehicles, IoT, Virtual and Augmented Reality, Low latency mission critical applications etc.

1.2 Cellular Systems

- Cellular systems are mobile systems for two-way wireless communication between the fixed part of the system (transmitters or base stations) and the mobile part of the system (mobile stations) which move in the area covered by each base station.
- In a cellular system, the entire coverage area is divided into 'cells' i.e. they implement SDM (Space Division Multiplexing). Each cell is served by a single base station. Each cell has a size depending on the number of users. More the users, smaller the cell size.
- Cell radii ranges from tens of meters in buildings, and hundreds of meters in cities, up to tens of kilometers in the country side.
- The shapes of cells are never perfect circles or hexagons actually, it depends on environment, on whether conditions etc. Hexagon shape cellular system is shown in Fig. 1.2.1.

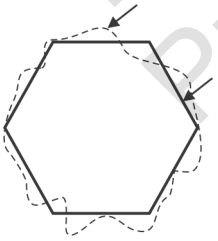


Fig.1.2.1 : Diagrammatic cell

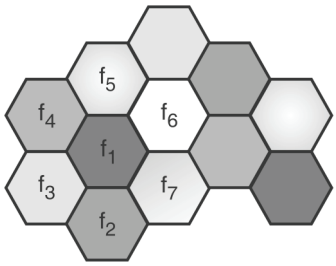


Fig. 1.2.2 : Cellular System with seven cell cluster vs. actual cell coverage

1.2.1 Frequency Reuse in Cellular Systems

MU - May 14

Q. What is frequency reuse concept in cellular communication? **(May 14, 5 Marks)**

- **Frequency reuse** is the technique of using the same radio **frequencies** on radio transmitter sites within a geographic area that are separated by sufficient distance to cause minimal interference with each other.

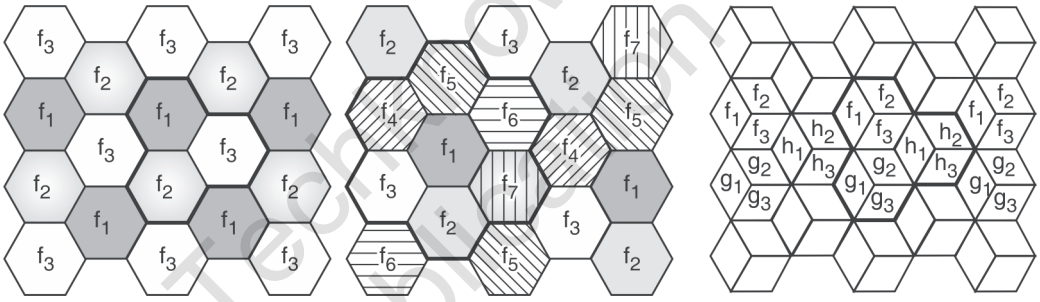
- To avoid interference in cellular system, each cell uses a different set of frequencies as compared to its immediate neighbors. In other words, no two neighbors use the same set of frequencies as there will be interference.
- A set of several cells are further grouped into clusters. Cells within the same cluster do not use the same frequency sets.
- Fig. 1.2.3 shows 3 cell cluster and 7 cell cluster. In Fig 1.2.3 (a) one cell in a cluster uses frequency f1, another cell uses f2 and the third cell uses f3. The same pattern is repeated for another cluster. Fig. 1.2.3 (b) shows a 7 cell cluster.

1.2.1(a) Frequency Reuse Concept

MU - May 17

Q. What is frequency reuse concept in cellular system? **(May 17, 5 Marks)**

- Consider a cellular system which has S full duplex channels available for use.
- Assume that the S channels are divided into N number of cells and each cell is allocated a group of K channels (K<S).
- Thus, total number of channels per cell is K = S/N.
- Therefore, the total number of available channels can be expressed as S = KN
- The N cells which collectively use the complete set of available frequencies is called **cluster**.
- The factor N is called the cluster size and is typically 4, 7 or 12.
- **Frequency reuse factor** of a cellular system is given by reciprocal of the cluster size i.e. 1/N.



(a) 3 cell cluster **(b) 7 cell cluster** **(c) 3 cell cluster with 3 sector per cell 3 sector antennas**

Fig. 1.2.3 : 3 cell cluster, 7 Cell Cluster and 3 cell cluster with sectorized antennas

- If the cluster size N is reduced while the cell size remains constant, more clusters are required to cover that particular area and hence more capacity is achieved.
- A large cluster size indicates that the ratio between cell radius and the distance between co channel cells is small.

Locating Co-channel cells in a cellular System

- For a hexagonal cell structure, it is possible to cluster cells so that no two adjacent cells use the same frequency. This is only achievable for a certain cell-cluster sizes, which can be determined from the relationship

$$N = i^2 + ij + j^2 \text{ Where } i,j = 0,1,2,3 \text{ etc.}$$

- To find nearest co-channel neighbors of a particular cell
  - Move i cells through the center of successive cells.
  - Turn 60^o in the counter clockwise direction.
  - Move j cells forward through the center of successive cells.

- Fig. 1.2.4 shows the process of locating the nearest co-channel neighbors of cell f4 in cluster 1.
- We first move i=2 successive cells in downward direction. From there we turn 60° in counterclock wise direction. And then move j=1 cell forward through the centre of the cell thus locating cell f4 in cluster 3. Similarly we can locate cell f4 in neighboring clusters – cluster 2 and cluster 4.

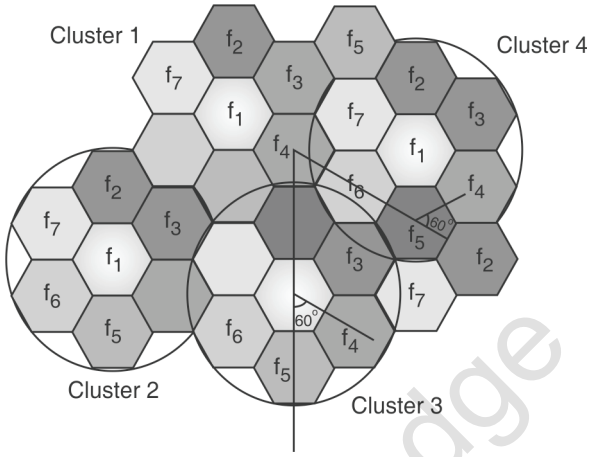


Fig. 1.2.4 : Method of locating co-channel cells in a cellular system (here i=2, j=1)

1.2.1(b) Assignment of Frequencies to Cells

Assignment of frequencies to cells can be done in following three ways.

1. Fixed Channel Allocation (FCA)

- This scheme assigns fixed set of frequencies to each cell or cluster. The scheme is easy to implement but not very efficient if traffic load varies.
- GSM system uses this scheme.

2. Borrowing Channel Allocation (BCA)

- In this scheme, if a one cell has heavy load then it can borrow frequencies from another neighboring cell which is having light load.
- Here cells with more traffic are dynamically allotted more frequencies.

3. Dynamic Channel Allocation (DCA)

- This scheme is similar to BCA. As in BCA here also frequencies can be borrowed from a neighboring cell. In addition to that, the assignment of frequencies is dynamic, that is frequencies can be assigned freely to cells.
- Since frequencies are assigned dynamically to a cell, there is a chance of interference with cells using the same frequencies.
- To avoid interference the 'borrowed' frequencies can be blocked in the neighboring cells.
- This scheme is used in DECT.

1.2.2 Advantages of Cellular Systems with Small Cells

1. Higher capacity

Implementing SDM allows frequency reuse. If one transmitter is far away from another transmitter then the transmitters can use the same frequency without any interference. Thus smaller cells allow more number of users.

2. Less transmission power

If the transmitter is far away from the receiver then it requires high power to transmit the signal. For mobile devices power is the main constraint, so reduced cell size requires less transmission power.

3. Local interference only

With larger cells, the distance between the mobile station and the base station is more and hence there are chances of more interference problems. With small cells, mobile stations and base stations only have to deal with 'local' interference.

4. Robustness

Cellular systems are decentralized and so more robust against the failure of single components. If one antenna fails, it only affects communication within a small area.

1.2.3 Disadvantages of Cellular System with Small Cells

1. Complex infrastructure

Cellular systems require a complex infrastructure to connect to all base stations. If the cell size is small, then it requires many antennas, switches, for call forwarding, location registers to find a mobile station etc. This will make the whole system expensive.

2. Handover needed

When mobile station moves from one cell to another cell, the process called handover is carried out. Depending on the cell size and the speed of movement, this can happen quite often.

3. Frequency Planning

Cellular system needs proper planning of frequency distribution to avoid interference between transmitters.

1.2.4 Why Hexagonal Pattern is Preferred for Cellular System ?

- When considering geometric shapes, which cover an entire region without overlapping or leaving gaps and with equal areas, there are three sensible choices.
  1. Equilateral triangle
  2. Square
  3. Hexagon
- The Table 1.2.1 describes the unit coverage area for each of the above mentioned shapes.

Table 1.2.1 : Unit coverage area for Triangle, square and Hexagon shapes

Cell type	Centre to centre distance	Unit coverage area
Triangle	R	1.3 R^2
Square	R√2	2 R^2
Hexagon	R√3	2.6 R^2

- A study of above table reveals the following points.
- Area coverage of hexagon is twice that of triangular area.
- To cover an area of three hexagonal cells i.e. 7.8 R^2 , 6 triangular cells or 4 square cells are required.
- In other words, if hexagonal area of 7.8 R^2 requires three frequencies, the triangular cells require 6 frequencies and square cells require 4 frequencies.

In general with the Hexagon pattern :

1. The fewest number of cells can cover a given geographical region
2. We can closely approximate a circular radiation pattern which would occur for an omnidirectional base station antenna.

1.2.5 Methods of Increasing Cell Capacity

There are basically three ways of increasing capacity of cellular system.

1. Cell Splitting
2. Cell Sectorization
3. Microcell Zones

1. Cell Splitting

- Cell splitting is the process of dividing the radio coverage of a cell in a cellular system into two or more new cell sites.
- Cell splitting is one of the ways to increase the capacity within the region of the original cell.
- To minimize interference, a certain distance must be maintained between cells using the same frequencies. However, this distance can be reduced without disturbing the cell reuse pattern.
- As the size of the cells are reduced, the same frequencies can be utilized in more cells, which in turn means more subscribers can be accommodated on the system.
- Particularly in congested areas, the cellular operator often splits an existing cell into two or more smaller cells.
- New transceivers are placed and the power of the transmitters are reduced in order to confine the signals to the newly created cells.
- For example, a cell that originally had a radius of 6 m could be split into three cells with each new cell having a 2 m radius.

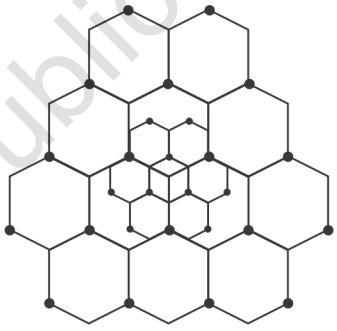


Fig. 1.2.5 : Cell splitting

Cell Sectorization

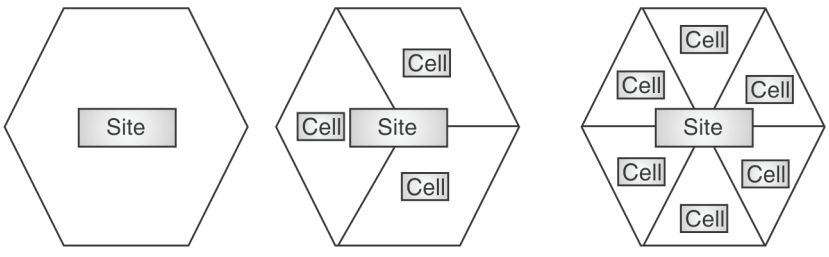


Fig. 1.2.6 : Cell Sectorization

- Another way to increase cellular system's capacity is to replace the omnidirectional antenna at each base station by three or more sector antennas.
- Use of directional sector antennas substantially reduces the interference among co-channel cells.
- This allows denser frequency reuse.
- The base station can either be located at the center of the original (large) cell, or the corners of the original (large) cell.
- Sectorization is less expensive than cell-splitting, as it does not require the acquisition of new base station sites.

Using Micro cell zone

- The disadvantage of cell sectoring concept is the need for an increased number of handoffs.
- The technique known as microcell that uses zones instead of sectors to reduce the number of handoffs.
- As shown in Fig. 1.2.7 this technique employs three antennas that provide coverage into the micro cell. All three antennas are connected to the same base station.

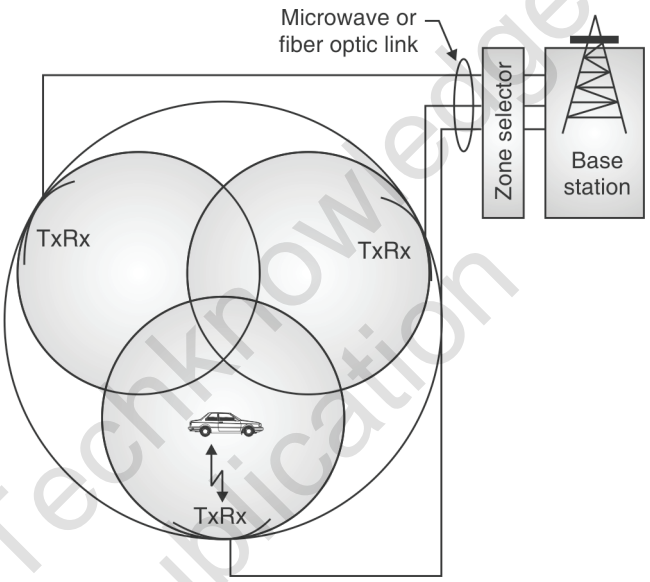


Fig. 1.2.7 : Micro Cell Zone

- The antenna with the best reception of the mobile is used for both the uplink and the downlink. As the mobile travels within a same micro cell it uses the same channel and there is no need for handoff.
- As the mobile moves into another zone the base station simply switches the channel to a different zone.

1.2.6 Cellular System Using CDM

- In cellular systems using CDM users are separated through codes. One of the advantages of these systems is that they don't need complex frequency planning and complex channel allocation schemes.
- But cell planning with CDM faces another problem. In CDM cell size is not fixed. Rather size of cell depends on the current load.
- Under a light load a cell becomes larger while it shrinks if the load increases.
- Mobile station further away from the base station may drop out of the cell.
- Fig. 1.2.8 shows a user transmitting a high bit rate stream within CDM cell.
- Because of this additional user, the cell shrinks. As a result the two users drop out of the cell. CDM cells are commonly said to **breathe**.

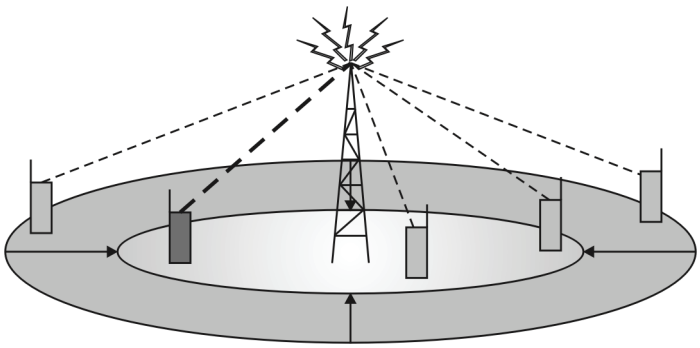


Fig. 1.2.8 : Cell breathing depending on the current load

1.3 Electromagnetic Spectrum

MU – May 15, Dec. 15

Q. Draw and explain electromagnetic spectrum for communication. **(May 15, Dec. 15, 5 Marks)**

- For radio transmission, there are many frequency bands. Each frequency band has some advantages and disadvantages and can be used as per the application.
- Fig. 1.3.1 illustrates the frequency spectrum for radio transmission. Frequencies start at 300Hz and go up to over 300THz.

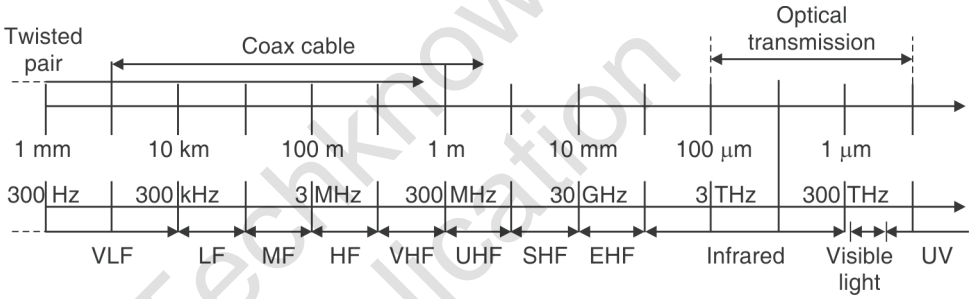


Fig. 1.3.1 : Frequency spectrum

- The relation between frequency **f** and wavelength **λ** is given by the equation

$$\lambda = c / f \quad \text{where, } c = 3 \times 10^8 \text{ m/s (the speed of light in vacuum)}$$

Frequency ranges for wired networks

Table 1.3.1 : Frequency ranges for wired networks

Medium	Frequency Range
Twisted Pair	0-3.5 KHz
Co-axial cable	0 – 500 MHz
Fiber Optics	186 - 370 THz

Frequency ranges for radio transmission

Table 1.3.2 : Frequency ranges for radio transmission

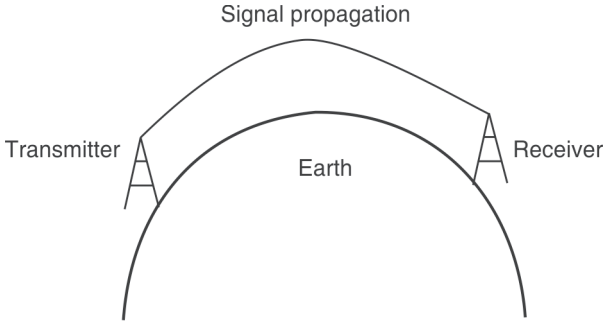
Frequency Band	Frequency Ranges	Propagation Characteristics	Application
VF(Voice Frequency)	300 Hz – 3KHz	GW	Used by telephone system for analog subscriber lines

Frequency Band	Frequency Ranges	Propagation Characteristics	Application
VLF (Very Low Frequency)	3 KHz – 30 KHz	GW	Long-range navigation; submarine communication
LF (Low Frequency)	30 KHZ – 300KHz	GW	Long-range navigation; marine communication radio beacon
MF(medium frequency)	300 KHz – 3 MHz	GW and night SW	Maritime radio; direction fading; AM broadcasting
HF(High Frequency)	3 MHz – 30MHz	SW	Amateur radio; international broadcasting; military communication; Long distance aircraft and ship communication.
VHF (Very High Frequency)	30 MHz – 300 MHz	LOS	VHF television; FM broadcast and two-way radio, AM aircraft communication; aircraft navigational aids
UHF(Ultra High Frequency)	300 MHz – 3GHz	LOS	UHF television; cellular telephone; radar; microwave links; personal communication systems
SHF(Super High Frequency)	3 GHz – 30 GHz	LOS	Satellite communication; radar; terrestrial microwave links; wireless local loop
EHF	30 GHZ – 300GHz	LOS	Experimental; wireless local loop
Infrared	300GHz – 400THz	LOS	Infrared LANs; consumer electronic allocations
Visible light	400 THz – 900 THz	LOS	Optical communication

Note : GW - Ground Wave, LOS - Line-of-Sight., SW - Sky Wave

Depending upon the frequency, the radio waves can exhibit following three types of behavior.

1. **Ground Wave (<2 MHz) :** Low frequency waves usually follow the Earth's surface and can propagate long distance. These waves are used for submarine communication or AM radio.
2. **Sky wave (2-30 MHz) :** These waves are reflected at the atmosphere and hence can bounce back and forth between the ionosphere and the Earth's surface, traveling around the world. They are used for international broadcast.
3. **Line-of-Sight (>30 MHz) :** These waves follow a straight line of sight. They are used in Mobile phone systems. Also, Satellite systems, cordless telephones etc. use these waves.



Ground wave propagation (< 2MHz)

(a)

Fig. 1.3.2 : Contd…

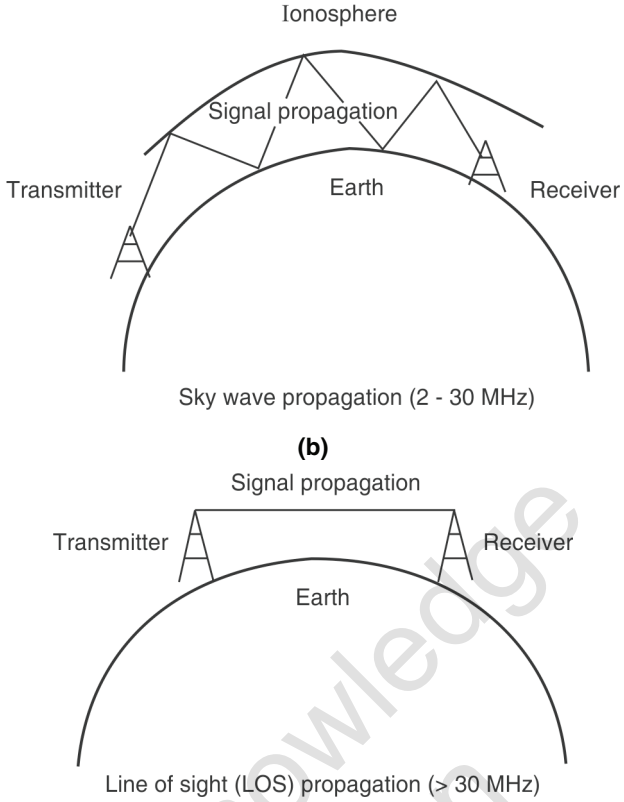


Fig. 1.3.2 : Ground Wave propagation, Sky wave Propagation and Line-of –Sight propagation

- Fig. 1.3.2 shows all three types of signal propagation.

1.4 Antennas

MU – Dec. 14, May 17, Dec. 18

Q.	Write about types of antennas and their radiation pattern.	**(Dec. 14, 5 Marks)**
Q.	What is an antenna? Explain different types of antennae.	**(May 17, 5 Marks)**
Q.	Write a short note on antenna.	**(Dec. 18, 10 Marks)**

- An **antenna** is a device that converts electromagnetic radiation in space into electrical currents in conductors or vice-versa, depending on whether it is being used for receiving or for transmitting, respectively.
- The **radiation pattern** of an antenna describes the relative strength of the radiated field in various directions from the antenna, at a constant distance.
- In reality the radiation pattern is three-dimensional, but usually the measured radiation patterns are a two-dimensional slice of the three-dimensional pattern, in the horizontal or vertical planes.
- There are various types of antennas discussed below.

1.4.1 Isotropic Antenna

- An **isotropic antenna** is a theoretical antenna that radiates its power uniformly in all directions.
- In other words, a theoretical isotropic antenna has a perfect 360 degree spherical radiation pattern. Radiation pattern of isotropic antenna is shown in Fig. 1.4.1.
- It is an **ideal** antenna which radiates equally in all directions and has a gain of 1 (0 dB), i.e. zero gain and zero loss.

- It is used to compare the power level of a given antenna to the theoretical isotropic antenna.
- Fig. 1.4.1 shows a two dimensional cross-section of the real three dimensional pattern.
- Antennas can be broadly classified as **omnidirectional** and **directional** antennas.

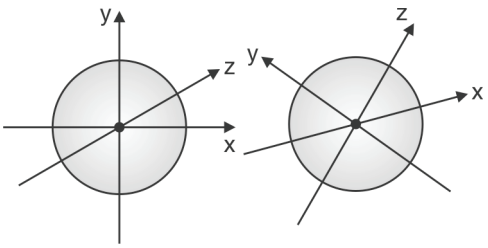


Fig. 1.4.1 : Radiation pattern of Isotropic antenna

1.4.2 Omnidirectional Antennas

- Unlike isotropic antennas, dipole antennas are real antennas. The dipole radiation pattern is 360 degrees in the horizontal plane and approximately 75 degrees in the vertical plane.
- It is also called the "non-directional" antenna because it does not favor any particular direction.
- Dipole antennas are said to have a gain of 2.14 dB, which is in comparison to an isotropic antenna. The higher the gain of the antennas, the smaller the vertical beam width is.
- This type of antenna is useful for broadcasting a signal to all points of the compass or when listening for signals from all points.

Dipoles

- The most commonly used antenna is **Hertzian** dipole.
- The dipole consists of two collinear conductors of equal length, separated by a small feeding gap.
- The length of the dipole is half the wavelength λ of the signal (for efficient radiation of energy).
- Fig. 1.4.2 shows a typical Hertzian dipole.

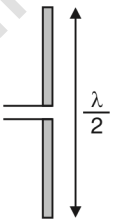


Fig. 1.4.2 : Hertzian dipole

- A λ/2 dipole has a uniform or omnidirectional radiation pattern in one plane and a figure **eight** pattern in the other two planes. This is shown in Fig. 1.4.3.
- This type of antennas are used in area such as mountain, valley etc.
- Although this is a simple antenna, it is difficult to mount on a roof top of a vehicle.

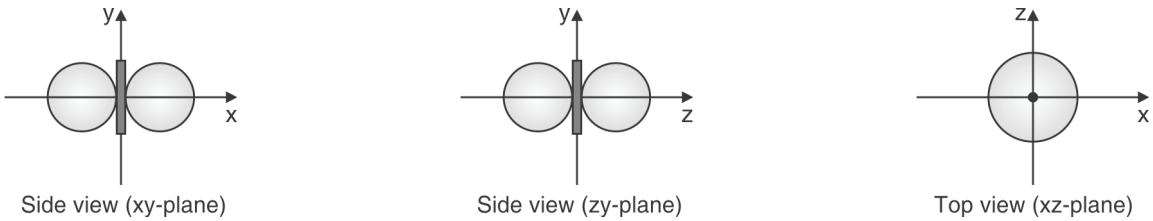


Fig. 1.4.3 : Radiation pattern of Hertzian dipole

Monopoles

- Shown in Fig. 1.4.4 is the ideal vertical monopole antenna.
- It has the length λ/4 and also known as **Markoni** antenna.
- A monopole over an infinite ground plane is theoretically the same as the dipole in free space.
- The flat surface of a vehicle's trunk or roof can act as an adequate ground plane.
- This type of antenna is efficient for mounting on a roof top of a car.

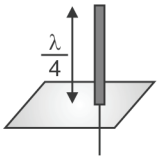


Fig. 1.4.4 : Monopole

Directional Antenna

- A **directional antenna** or **beam antenna** is an antenna which radiates or receives greater power in specific directions.
- This allows increased performance and reduced interference from unwanted sources.
- Unlike omnidirectional antennas, directional antennas must be aimed in the direction of the transmitter or receiver.
- Examples of directional antennas are parabolic and Yagi antenna shown in Fig. 1.4.5 and Fig. 1.4.6 respectively.
- Fig. 1.4.7 shows the radiation pattern of a directional antenna with the main lobe in the direction of X-axis.

Fig. 1.4.5 : Parabolic antenna

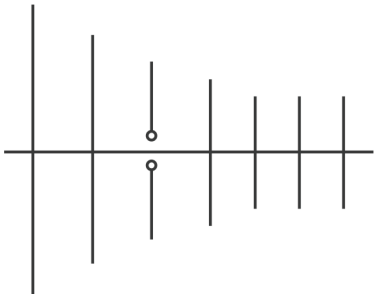


Fig. 1.4.6 : Yagi antenna

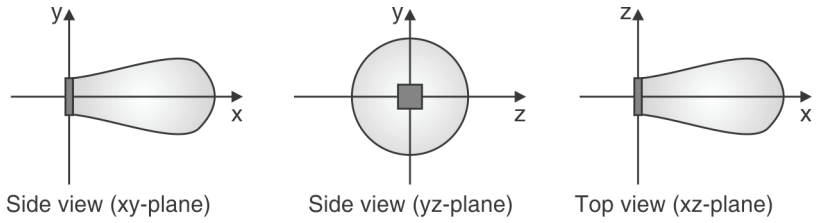


Fig. 1.4.7 : Radiation pattern of directional antennas

Sectorized Antenna

- Several directional antennas can be combined on a single pole to construct a sectorized antenna.
- They are widely used in cellular telephony infrastructure. For example, A cell can be sectorized into three or six sectors. Fig. 1.4.8 shows radiation pattern of these sectorized antennas.

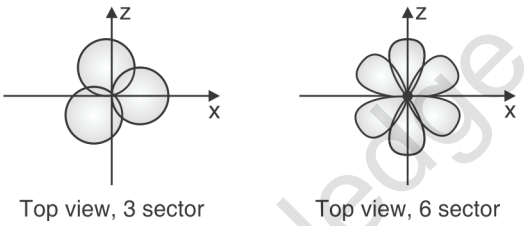


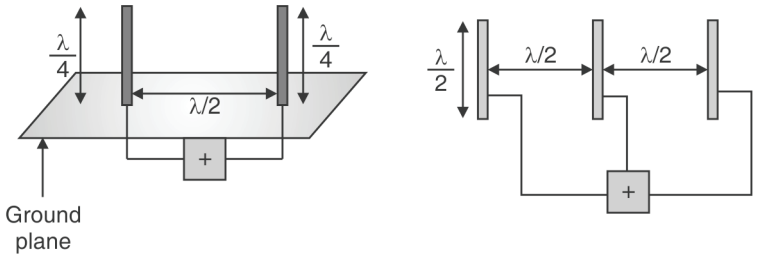
Fig. 1.4.8 : Radiation pattern of sectorized antennas

Antenna arrays

- An antenna array is a configuration of multiple antennas (elements) arranged to achieve a given radiation pattern.
- Multiple antennas allow different diversity schemes to improve the quality and reliability of a wireless link.
- Antenna diversity is especially effective at mitigating effects of multipath propagation.
- This is because multiple antennas allow a receiver several observations of the same signal.
- Each antenna will experience a different interference environment. If one antenna is experiencing a deep fade, it is likely that another has a sufficient signal. Collectively such a system can provide better link.
- Different diversity schemes are possible.
- One such scheme is **selection diversity** where the receiver always uses the antenna element with the largest output.
- The other type of diversity is **diversity combining** in which a combination of power of all the signals is taken to produce gain.

  Fig. 1.4.9 shows two such different schemes.

  - In Fig. 1.4.9 (a) two λ/4 antennas are arranged with a distance of λ/2 between them.
  - In Fig. 1.4.9 (b) three standard λ/2 dipoles are combined with a distance of λ/2 between them.



(a) **(b)**

Fig. 1.4.9 : Diversity antenna systems

1.5 Signal Propagation

MU – Dec. 18

Q. What are various issues in signal propagation ? **(Dec. 18, 10 Marks)**

- Since wireless networks use unguided media such as radio waves, the signal has no wires to determine the direction of propagation, where as signals in wired network only travel along the wire.
- In wired network, one can easily determine the behavior of a signal traveling along this wire such as received power depending on the length.
- For wireless transmission, this predictable behavior is only valid in a vacuum. As shown in Fig. 1.5.1 depending upon the distance from the sender, the transmitted signal can fall into the following ranges.

1. Transmission Range

Within this range the receiver receives the signals with a very low error rate and hence able to communicate.

2. Detection Range

Within this range the receiver can detect the transmission i.e. the transmitted power is large enough to differ signal from background.

3. Interference Range

Within this range, the sender may interfere with other transmissions by adding to background noise. The receiver will not be able to detect the signal but the signal may disturb other signals.

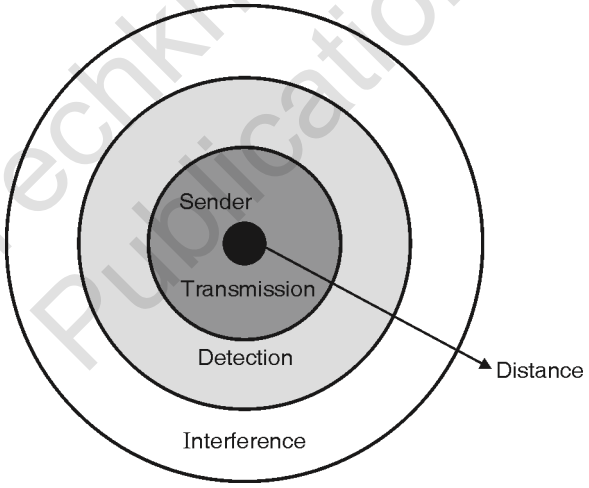


Fig. 1.5.1 : Ranges for transmission, detection and interference of signals

1.5.1 Path Loss of Radio Signals

Free Space Loss

- In free space, the signal follows a straight line. If such a straight line exists between the sender and the receiver, it is called the line of sight (LOS).
- The signal experiences free path loss even if no object exists between the sender and the receiver. This is because the receiver power P_r is proportional to $1/d^2$. Here d is the distance between the sender and the receiver. Hence, as d increases, the received power P_r decreases.

Other Parameters affecting signal Strength

- The received power also depends on the wavelength and the gain of the receiver and transmitter antenna.
- For long distance communication, most radio transmission takes place through air, rain, snow, fog, etc. The atmosphere heavily influences the quality of the signal. E.g. satellite transmission.

1.5.2 Additional Signal Propagation Effects

1. Blocking / Shadowing

- The signals with higher frequency behave like a straight line.
- These signals are blocked by even small obstacles like a wall, a car or a truck on a road. This phenomenon is called blocking or shadowing.

2. Reflection

- When a signal encounters a surface that is large relative to the wavelength of the signal, a phenomenon called reflection occurs.
- The reflected signal is not as strong as the original, as the object can absorb some of the signal's power.

3. Refraction

- This effect occurs because the velocity of the electromagnetic waves depends on the density of the medium through which it travels.
- As shown in Fig. 1.5.2, waves that travel into a denser medium are bent towards the medium.

4. Scattering

- If the object size is in the order of the wavelength of the signal or less, then the signal can be scattered into many small signals.
- Scattered signals are weaker than the original signal.

5. Diffraction

Diffraction occurs at the edge of an impenetrable body that is large as compared to the wavelength of a radio wave.

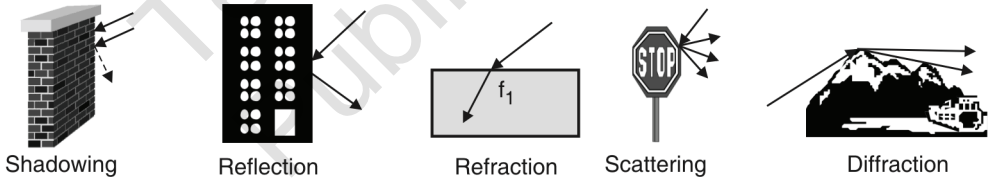


Fig. 1.5.2 : Blocking, reflection, refraction and diffraction of waves

1.5.3 Multi-path Propagation and Fading

1.5.3(a) Multi-path propagation

- The wireless channel is a multipath propagation channel.
- The radio waves that emanate from the transmitter do not reach the receiver only by a single path. The signal can take many different paths from the sender to the receiver due to reflection, scattering and diffraction. This effect is called multi-path propagation.
- Multi-path propagation is one of the most severe radio channel impairments.
- Fig. 1.5.3 shows a sender on the left hand side and one possible receiver on the right hand side.
- A radio wave emitted by a sender can take the LOS path (i.e. travel in straight line), or it may be scattered at small obstacles or reflected at large buildings.

- As a result, we have multiple copies of the same signal being transmitted and received with different delays, different amplitudes and phases.
- This effect caused by multi-path propagation is called **delay spread** i.e. the original signal is spread due to different delays of parts of the signal.

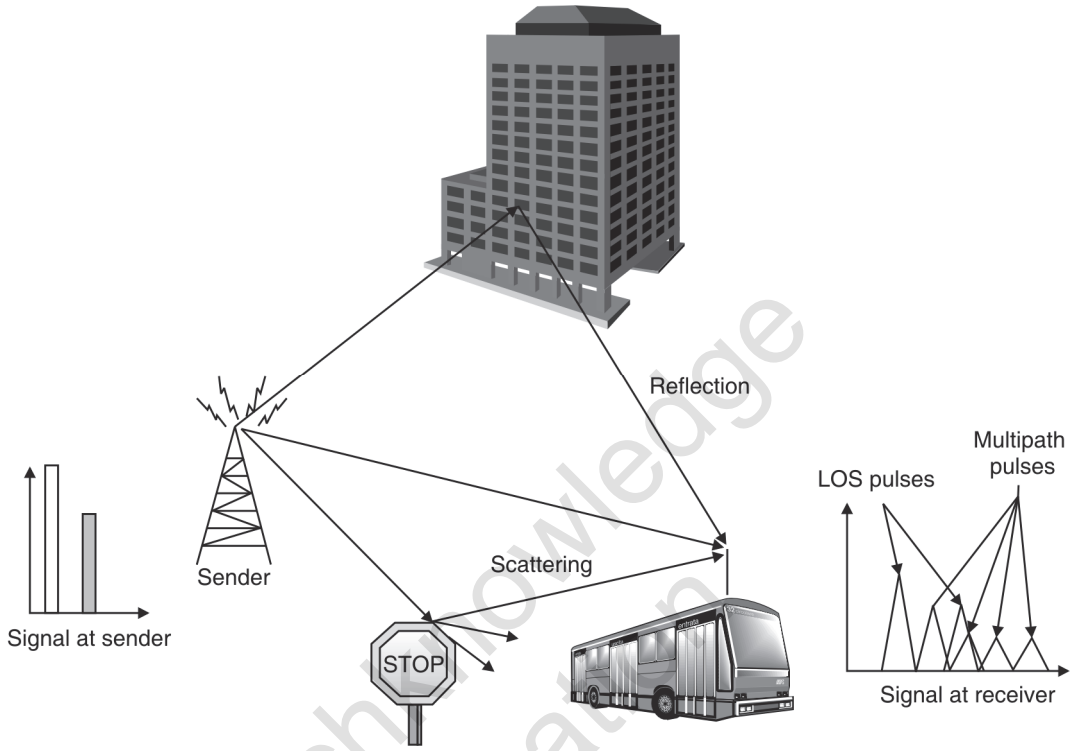


Fig. 1.5.3 : Multi-path propagation and inter-symbol interference

- As shown in Fig. 1.5.3, a short impulse will be smeared out into a broader impulse or into several weaker impulses. As a result, energy intended for one symbol spills over the adjacent symbol. This effect is called **inter symbol interference** (ISI).
- ISI makes detection of the signal difficult at the receiver. In real situation many weaker impulses arrive at the receiver. Some of the received pulses are too weak to be detected and appear as noise.

1.5.3(b) Fading

The term fading means rapid fluctuations of the amplitudes, phases, or multipath delays of a radio signal over a short period or short travel distance.

1. Fading effect due to mobility

In addition to multipath propagation, another problem called fading occurs due to mobility. Following two types of fading may occur due to mobility.

(i) Short-term fading

- Short term fading occurs when receivers or senders or both move. It occurs due to the quick changes in the received power.
- The receiver now has to try to continuously adapt to the varying channel characteristics.
- However, if such changes are too fast then (e.g. driving on a highway through a city) receiver cannot adapt fast enough and the error rate of the transmission increases dramatically. Short term fading is shown in Fig. 1.5.4.

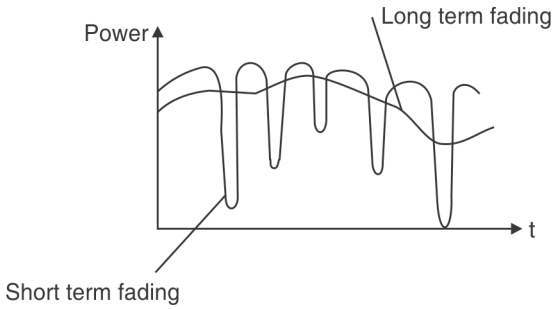


Fig. 1.5.4 : Short term and long term fading

(ii) Long-term fading

- The long term fading occurs when the sender is stationary and the distance of the receiver to the sender varies slowly.
- It occurs due to slow changes in the average power received. This is shown as the average power in Fig. 1.5.4.
- Senders can compensate for long term fading by increasing/decreasing sending power so that the received signal always stays within certain limits.

2. Fading Effects due to Multipath Time Delay Spread

(i) Flat Fading

- Flat fading occurs when the bandwidth of the transmitted signal is less than the coherence bandwidth of the channel.
- Equivalently, the fading is flat fading if the symbol period of the signal is more than the rms delay spread of the channel.

(ii) Frequency Selective Fading

- Frequency selective fading occurs when the signal bandwidth is more than the coherence bandwidth of the mobile radio channel.
- Equivalently the symbols duration of the signal is less than the rms delay spread.

1.6 Signal Characteristics

- Signals are the physical representation of data. Data in a communication system can be exchanged through the signals. Signals are functions of time and location.
- Signal parameters represent the data values. Signal parameters are the Amplitude (A), frequency (f) and phase shift (Φ). The most interesting type of signal for radio transmission is periodic signal (especially sine wave), used as carriers.
- The general function of a sine wave is, $s(t) = At \sin(2 \pi ft t + \varphi t)$

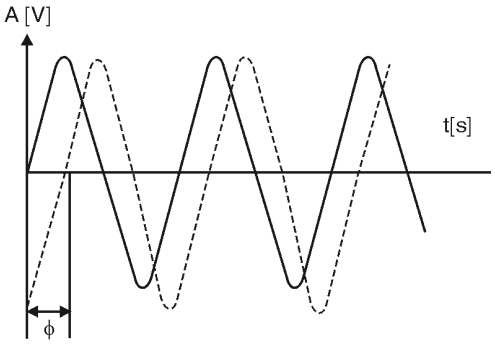


Fig. 1.6.1 : Time Domain representation of a signal (a sine wave without phase shift and with a phase shift ϕ)

1.7 Multiplexing

MU - May 18

Q. Discuss multiplexing in wireless communication. **(May 18, 10 Marks)**

- Multiplexing means the ability to send data coming from multiple sources, users or channels over a common shared transmission medium with minimum interference and maximum utilization. To make efficient use of high-speed communication lines, some form of multiplexing is used.
- Four types of multiplexing are commonly used in communication systems.

1. Space Division Multiplexing (SDM)
2. Time Division Multiplexing (TDM)
3. Frequency Division Multiplexing (FDM)
4. Code Division Multiplexing (CDM)

1.7.1 Space Division Multiplexing (SDM)

- In space division multiplexing, the entire region of transmission is divided into multiple spaces. For exchanging data, each user is allocated a communication channel.
- Fig. 1.7.1 shows six channels k_1 to k_6 and a three dimensional coordinate system. The dimensions are code c, time t and frequency (f). It also shows space S_i represented via circles. Channel k_1 to k_3 can be mapped onto the three spaces S_1 to S_3 which clearly separates the channel.
- It can be noted that there is some space between each channel. This space is called a **guard channel**. For the remaining channels, three additional spaces would be needed.

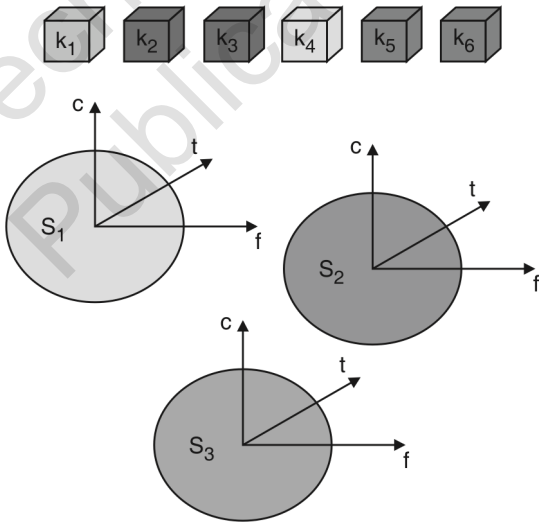


Fig. 1.7.1 : Space Division Multiplexing

Application

- This multiplexing scheme can be used for FM radio stations if a single FM station transmits in a given region (say some city) only. The same transmission ranges can then be shared by different radio stations around the world without interference.
- SDM is also used in cellular systems where the service area is divided into different cells. Each cell is assigned different frequency band such that there is no interference in adjacent cells.

Advantage

SDM is easy to implement.

Problem

If two or more channels are established in the same space (For example, several radio stations want to broadcast into the same city), then SDM alone cannot be used.

1.7.2 Frequency Division Multiplexing (FDM)

- In frequency division multiplexing, the entire frequency range is divided into frequency bands.
- Each channel gets a certain band of the spectrum for the whole time.
- Different frequency bands are separated by guard spaces.

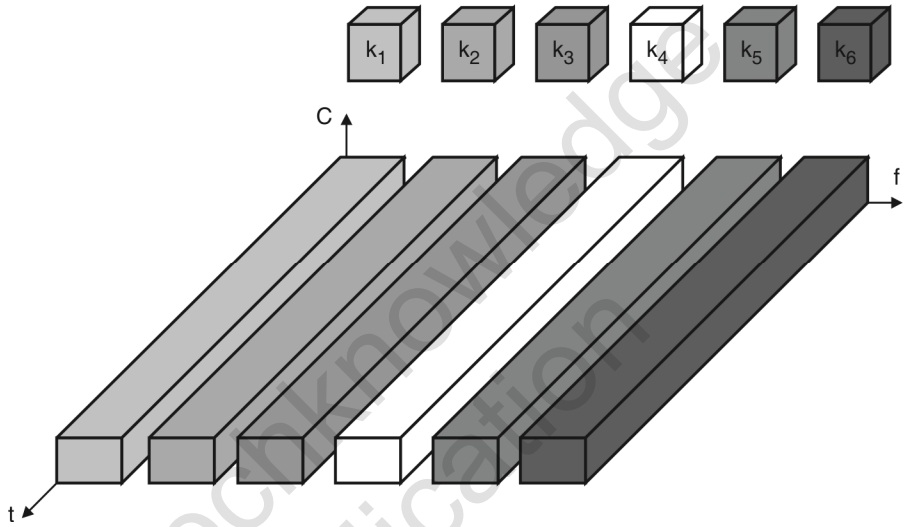


Fig. 1.7.2 : Frequency Division Multiplexing

Application

This scheme is used for radio stations within the same region, where each radio station uses its own frequency.

Advantages

- No complex coordination between sender and receiver is required.
- This scheme works for analog signals as well.

Disadvantages

- The bandwidth is wasted if the traffic is distributed unevenly.
- The scheme is inflexible.

1.7.3 Time Division Multiplexing (TDM)

- In TDM, the entire spectrum is given to a particular channel for a certain time interval.
- As shown in Fig. 1.7.3, a channel k_i is given the whole bandwidth for a certain amount of time.
- Guard spaces are needed in TDM as well, which are now represented by time gaps.
- Thus, in TDM all the channels use the same frequency but at different time.

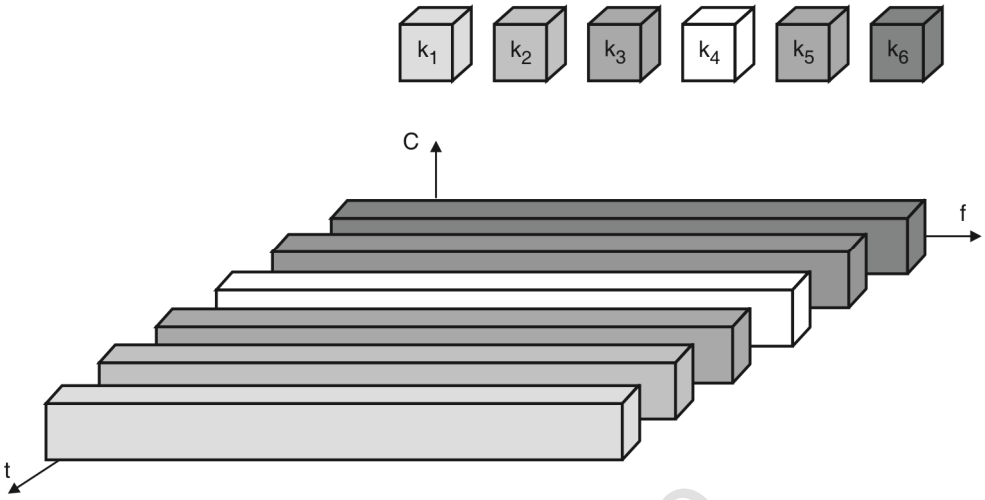


Fig. 1.7.3 : Time division multiplexing

Advantage

There is only one carrier in the medium at any time which results in high throughput even if there are many users.

Disadvantage

1. If two transmissions overlap in time, **co-channel interference** may occur.
2. To avoid co-channel interference, it is required that different senders are precisely synchronized.

1.7.4 Frequency and Time Division Multiplexing

- In this multiplexing scheme, frequency and time division multiplexing are combined.
- As shown in Fig. 1.7.4, channel k_i uses certain frequency band for a certain amount of time. Now guard spaces are required in both dimensions.

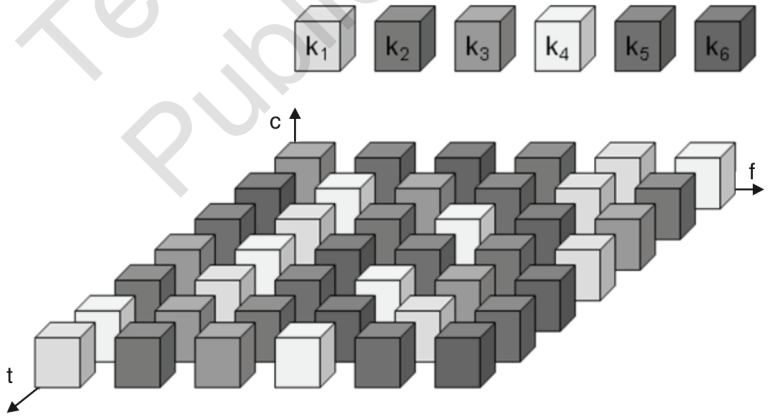


Fig. 1.7.4 : Frequency and time division multiplexing

Application

The scheme is used in GSM (Global System for Mobile Communication)

Advantages

1. Offers better protection against tapping.
2. Provides protection against frequency selective interference.

Disadvantage

Necessary coordination is required between different senders.

1.7.5 Code Division Multiplexing (CDM)

- In this scheme, all channels use the same frequency at the same time for transmission.
- Users are now separated using codes.

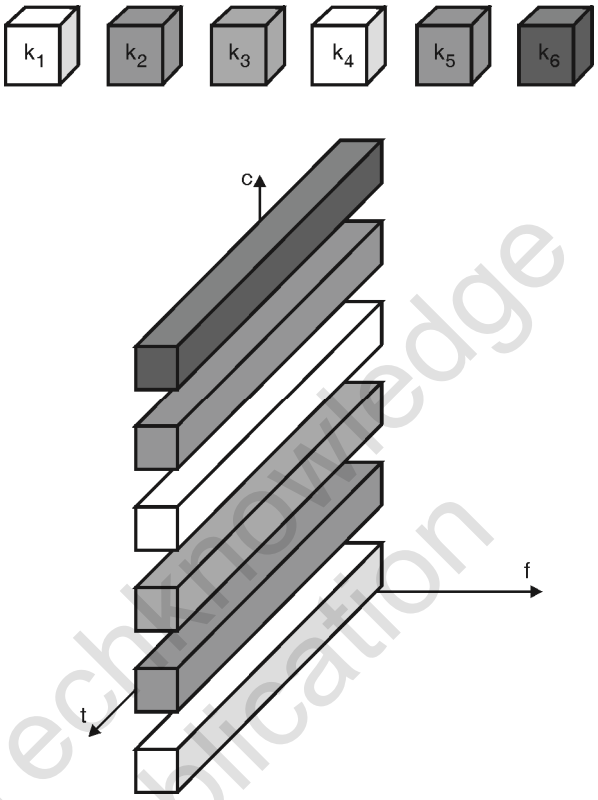


Fig. 1.7.5 : Code division multiplexing

- In this, signals from multiple independent sources can be transmitted at the same time over the same frequency band.
- This task can be achieved via spread spectrum technique in which special codes called as orthogonal codes are used to spread each signal over a large, common frequency band.
- So, in CDM, each channel is assigned a particular orthogonal code and this is how multiplexing is achieved.
- Guard spaces are now required in the code dimension.

Advantages

1. It gives good protection against interference and tapping.
2. Bandwidth utilization is very efficient.
3. No synchronization is needed between the sender and the receiver.

Disadvantages

1. Varying user data rates.
2. More complex signal regeneration and hence high complexity at the receiver.
3. It is implemented using spread spectrum technology.

4. A receiver must be precisely synchronized with the transmitter to apply decoding correctly.
5. Precise power control is required. All signals should reach the receiver with more or less the same power otherwise low power signals could be drained by high power ones.

1.8 Spread Spectrum Techniques

MU - May 12, Dec. 12, May 13, May 14

Q.	What are the main benefits of spread spectrum system ? Explain direct sequence spread spectrum in detail. How can DSSS systems benefit from multipath propagation ?	**(May 12, 10 Marks)**
Q.	What are benefits of Spread Spectrum systems ?	**(Dec. 12, 5 Marks)**
Q.	Explain different types of Spread Spectrum technique used in cellular system.	**(May 13, 5 Marks)**
Q.	What is Spread Spectrum ?	**(May 14, 5 Marks)**

- Spread spectrum is an important form of encoding for wireless communications.
- In contrast to regular narrowband technology, the spread-spectrum process is a wideband technology.
- In this technique the frequency of the transmitted signal is deliberately spread in the frequency domain. The resultant signal has much greater bandwidth than the original signal.
- The process of spreading and de-spreading is shown in Fig. 1.8.1.

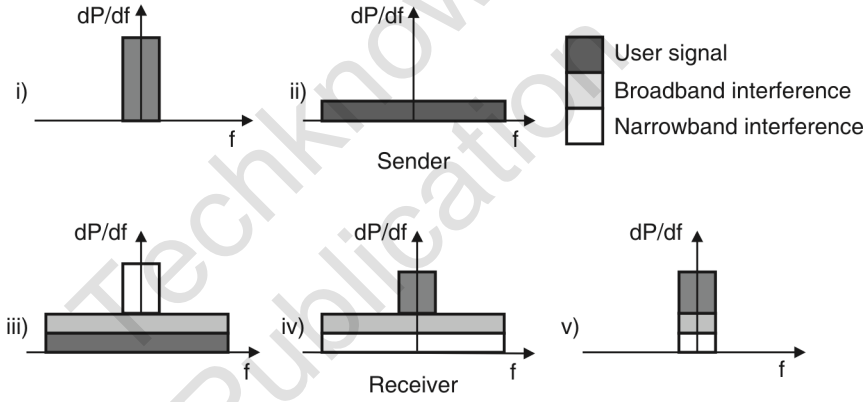


Fig. 1.8.1 : Spread Spectrum: Spreading and despreading

(i) Fig. 1.8.1 (i) shows narrowband signal transmitted form a sender. This is the signal user wants to send.

(ii) dP/df is the power density of this signal. The energy required to transmit the signal is equal to the area covered by the signal.

(iii) Second step is to spread the user signal. The process of spreading the signal is nothing but converting a narrowband signal into broadband signal. This can be achieved by multiplying a PN sequence with the user data. The energy required to transmit the signal is same, but the power level is much lower than the narrowband signal.

(iv) During the transmission, narrow band and broadband interference get added to the signal (shown in Fig. 1.8.1 (iii)).

(v) At the receiver sum of interference and user signals is received (shown in Fig. 1.8.1 (iv)).

(vi) The receiver now despreads the signal i.e. converts the spread user signal into a narrowband signal. This is achieved by multiplying the received signal with the same PN sequence used in step 2 and by using bandpass filter to cut off frequencies left and right of the narrowband signal (shown in Fig. 1.8.1 (v)).

Advantages of Spread Spectrum Techniques

1. Good protection against narrowband interference : A signal with narrow frequency is subject to catastrophic interference that can wipe out narrow band signals for the duration of the interference. Spread spectrum technique spreads the narrow band signal into a broad band signal using a special code to achieve resistance against this narrow band interference.
2. Resistance to interception : A constant-frequency signal is easy to intercept, and is therefore not well suited to applications in which information must be kept confidential. In spread spectrum technique, the signal is spread using a specific, but complicated mathematical function. In order to intercept the signal, a receiver must know how to de-spread the signal.
3. Spread Spectrum systems can co-exist with other radio systems, without being disturbed by their presence and without disturbing their activity. Thus the spread spectrum systems may be operated without the need for license.
4. Spread spectrum techniques can resist multi-path fading.

Disadvantages of Spread Spectrum Techniques

1. Complexity of receiver is increased.
2. Large frequency band is needed for spreading the signal.
3. Spread signals with low strength may interfere with other transmissions and appear as noise.
4. Precise power control is needed.

Spreading the spectrum can be achieved in two different ways

1. Direct Sequence Spread Spectrum (DSSS)
2. Frequency Hopping Spread Spectrum (FHSS)

1.8.1 Direct Sequence Spread Spectrum (DSSS)

– Fig. 1.8.2 shows the transmitter of DSSS.

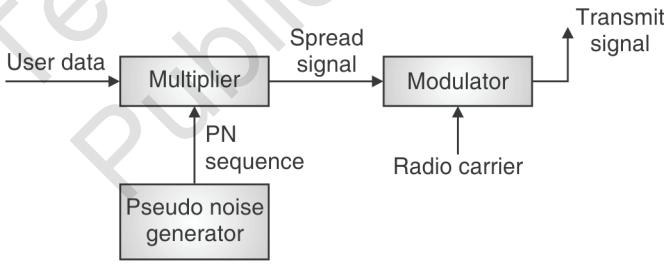


Fig. 1.8.2 : DSSS Transmitter

1. DSSS Transmitter

DSSS transmitter involves two major steps.

Step 1 : Spreading the signal

– Spreading in Direct Sequence modulation is achieved by modulating the carrier signal (user data) with a digital code sequence which has a bit rate much higher than that of the message to be sent.

– This digital code sequence is typically a pseudorandom binary code. It is also known as PN ("pseudo-noise") sequence or chipping sequence.

– Spreading can be done by simply XORing user bit stream with chipping sequence.

– The time period of a single bit in the PN code is termed a *chip*, and the bit rate of the PN code is termed the *chip rate*.

– The spreading process is shown in Fig. 1.8.3.

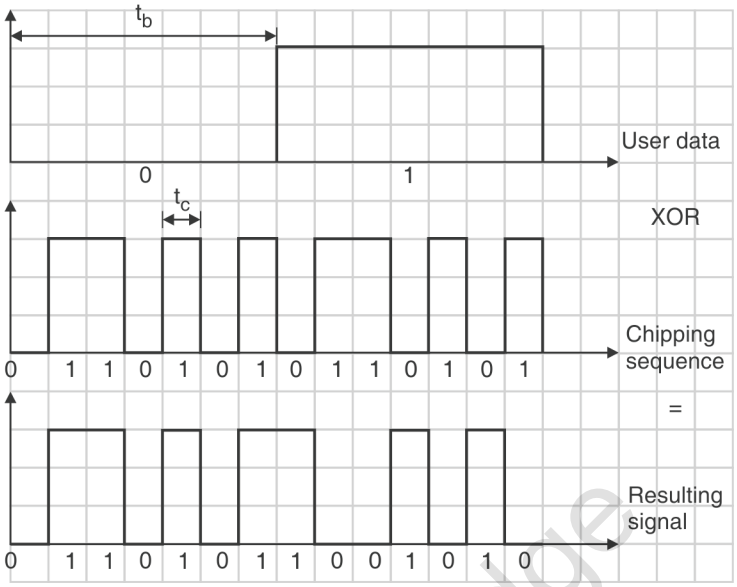


Fig. 1.8.3 : Spreading with DSSS

- Consider the chipping sequence as 0110101.
- If the user bit is 0 the result of XORing is the chipping sequence itself.
- If the user bit is 1 the result is the complement of chipping sequence.
- If the bit duration of user data is t_b and the duration of one chip in chipping sequence is t_c, then the spreading factor $s = t_b / t_c$ determines the bandwidth of a signal.
- If the original signal has bandwidth **w** then the resulting signal needs (**s . w**) bandwidth.

Step 2 : Radio modulation

- The spread signal is now modulated with a radio carrier.
- The radio carrier shifts this signal to the carrier frequency.
- This signal is then transmitted.

2. DSSS Receiver

The DSSS receiver involves three steps :

(i) Demodulation

(ii) Correlation

(iii) Decision Making

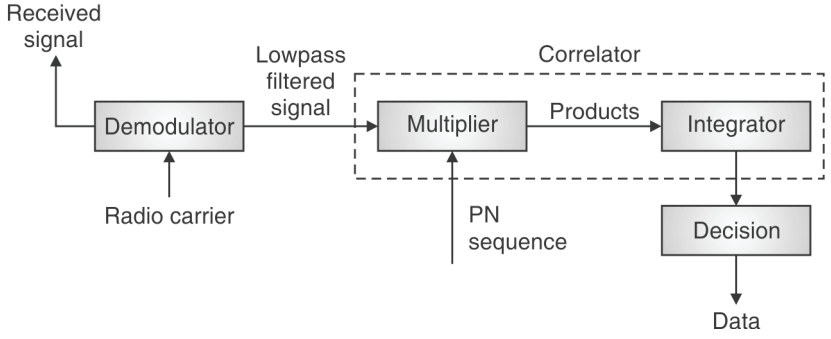


Fig. 1.8.4 : DSSS Receiver

(i) Demodulator

Demodulation of the received signal is achieved by using the same carrier as the transmitter, reversing the modulation process. Bandwidth of the resultant signal is approximately same as that of the original spread spectrum signal.

(ii) Correlator

Here the receiver uses the same pseudo random sequence (Chip sequence) as the transmitter. Pseudo random sequences at the sender and the receiver have to be precisely synchronized because the receiver calculates the product of a chip (XOR operation) with the incoming signal. During a bit period an integrator adds all these products.

(iii) Decision Unit

Finally the decision unit decides if the sum represents binary 0 or 1, based on the sum generated by the integrator during each bit period.

DSSS and Multipath fading

- We know that in multipath propagation there exist several paths with different delays between a transmitter and a receiver. As a result the receiver may receive multiple copies of the signal, each with different delays.
- **Rake receivers** can be used to mitigate the effect of multipath propagation.
- A rake receiver uses **n** correlators called **fingers** for **n** strongest paths.
- Each correlator is synchronized to the transmitter plus the delay on that specific path.
- As soon as the receiver detects a new path which is stronger than the currently weakest path, it assigns this new path to the correlator with the weakest path.
- The outputs of the correlators are then combined and fed into the decision unit.

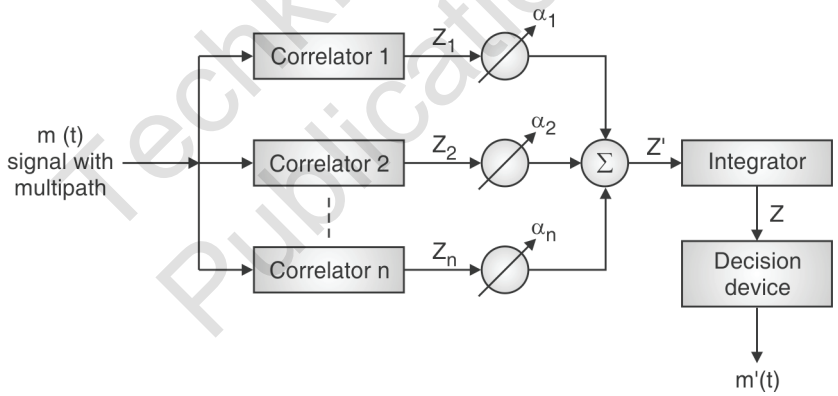


Fig. 1.8.5 : Rake receivers

Example of DSSS

User Data : 01

Chip : 10110111000 (11-chip Barker code)

XOR of bit 0 with chip: 10110111000

XOR of bit 1 with chip: 01001000111

Spread signal : 101101110000101001000111

Received signal : 101101110000101001000111

XOR of received signal with chip:

(10110111000101101110000) XOR (10110111000010010001111) = (00000000000111111111111)

Result of Integrator: 0 , 11

Result of Decision unit: 0 < 4 so bit is 0

11 > 7 so bit is 1

Decoded data: 01

Even if error occurs during transmission, received signal can still be decoded correctly.

For e.g. fourth, fifth, seventh and fourteenth bit in received signal is changed, then the received signal would be 101**01**1**0**100001**1**01000111

Now XOR of received signal with chip :

(10110111000101101110000) XOR (101**01**1**0**100001**1**01000111) = (00011010000 11011111111)

Result of integrator: 3, 10

Result of Decision unit: 3 < 4 so bit is 0

10 > 7 so bit is 1

Decoded data: 01

Note : Decision maker decides on to 0 if the sum is between 0-4 and 1 if sum is between 7-11.

Advantages of DSSS

1. Resistance to narrow band interference and anti-jamming effects.
2. Resistance to Interception.
3. Resistance to Fading (Multipath Effects).

Disadvantages of DSSS

1. Precise power control necessary.
2. Overall system is complex.
3. Is required between the sender and the receiver.

Applications of DSSS

The DSSS Communications are widely used today for Military, Industrial Scientific, and Civil uses. The applications include the following :

1. CDMA radios

It is useful in multiple access communications wherein many users communicate over a shared channel.
For example, CDMA.

2. WLAN

Wireless LAN widely use spread spectrum communications. IEEE 802.11 is a standard that is developed for mobile communication, and widely implemented throughout the world. The standard defines three types of Physical Layer communications. These are Infrared (IR) Communications, Direct Sequence Spread Spectrum Communications, Frequency Hopping Spread Spectrum communications.

3. Cordless Phones

Several manufacturers implement Spread Spectrum in Cordless phones due to their advantages like security, immunity to noise and longer range.

1.8.2 Frequency Hopping Spread Spectrum (FHSS)

- FHSS implements TDM plus FDM.
- In this scheme total available bandwidth is split into many channels of smaller bandwidth.
- Transmitter and receiver stay on one of these channels for some predefined time and then hop to another channel.
- The pattern of channel uses (frequency pattern) is called the **hopping sequence**.
- Time spent on a channel with certain frequency is called the **dwell time**.
- There are two variants of FHSS called slow and fast hopping.

1. Slow hopping

- Transmitter uses one frequency for several bit periods. Fig. 1.8.6 shows six user bits with a period t_b. Transmitter uses frequency f_2 for transmitting the first three bits and takes dwell time t_d. Then transmitter hops to the next frequency f_3.
- Slow hopping is cheaper and has relaxed tolerance.
- It is less immune to narrowband interference.

2. Fast hopping

- Transmitter changes frequency several times during a bit period. In Fig. 1.8.6 the transmitter hops three times during a bit period.

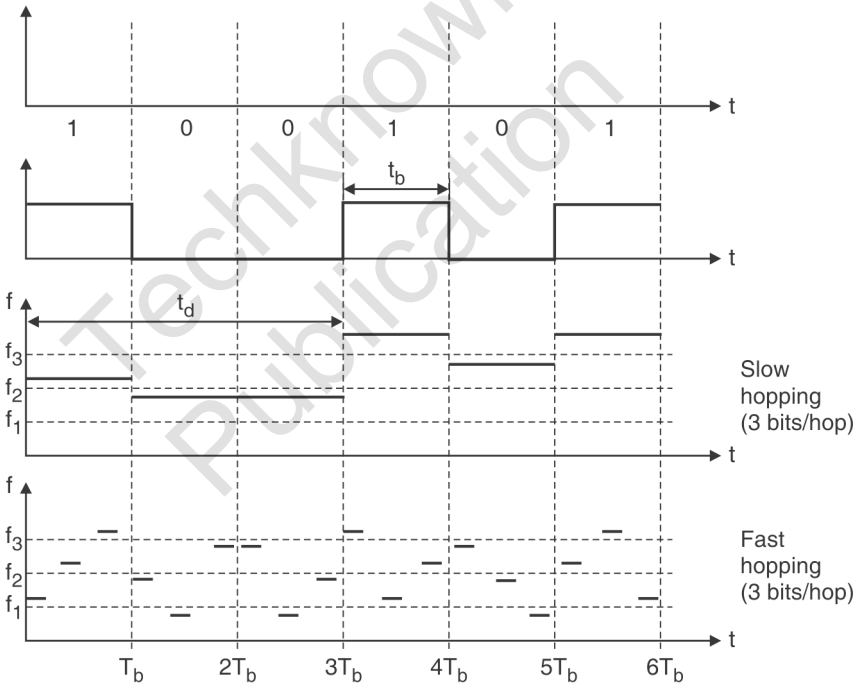


Fig. 1.8.6 : Slow and fast frequency hopping

- Fast frequency hopping systems are more complex to implement because transmitter and receiver should stay synchronized.
- These systems have better resistance against narrowband interference and frequency selective fading.

FHSS Transmitter

Fig. 1.8.7 shows simplified block diagram of FHSS transmitter.

Step 1 : Modulate user data using digital-to-analog modulation such as FSK or BPSK. For example, frequency f_0 is used for a binary 0 and f_1 is used for binary 1.

Step 2 : Frequency hopping is performed by using hopping sequence. The hopping sequence is fed into a frequency synthesizer generating the carrier frequency f_i.

Step 3 : Second modulation is done. It uses modulated narrowband signal and carrier frequency to generate a new spread signal with frequency of $f_i + f_0$ for a bit 0 and $f_i + f_1$ for a bit 1.

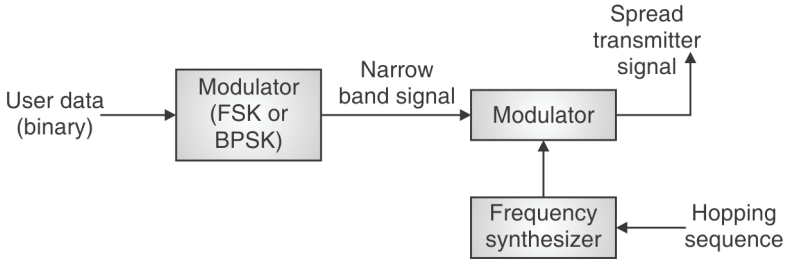


Fig. 1.8.7 : FHSS transmitter

FHSS Receiver

FHSS receiver performs reverse functions to reconstruct user data.

Step 1 : Demodulate received data by using hopping sequence and convert signal into narrowband signal.

Step 2 : Perform analog-to-digital modulation to reconstruct user data.

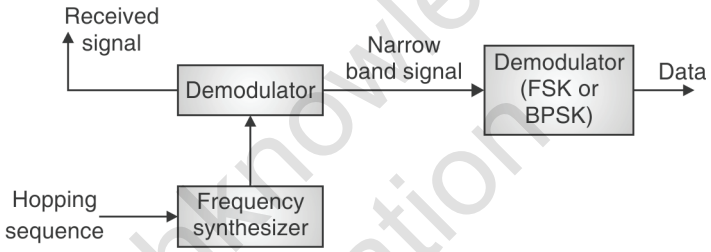


Fig. 1.8.8 : FHSS receiver

Slow hopping Vs. Fast hopping

Table 1.8.1 : Slow hopping Vs. Fast Hopping

Parameter	Slow Hopping	Fast Hopping
Main Idea	Several bits are transmitted using a same frequency.	One bit is transmitted using several different frequencies.
Resistance to narrowband interference	Provides lesser resistance to narrowband interference.	Better resistance to narrowband interference and frequency selective fading.
Security	Lower security as compared to fast hopping.	More secured since one bit is transmitted using several different frequencies.
Complexity	Less complex to implement as compared to fast hopping.	More complex as compared to slow hopping.

Applications of FHSS

1. GSM uses slow frequency hopping to avoid co-channel interference and to increase the channel capacity.
2. Bluetooth uses FHSS. It uses 79 frequencies with 1600 hops/sec.
3. WLAN : Most of the Wireless LAN standards define three types of Physical Layer communications. These are Infrared (IR) Communications, Direct Sequence Spread Spectrum Communications, Frequency Hopping Spread Spectrum communications.

1.8.3 Comparison between DSSS and FHSS

Table 1.8.2 : Difference between DSSS and FHSS

Parameter	DSSS	FHSS
Complexity	Spreading and dispreading is simple.	It requires a complex frequency synthesizer in order to generate the hops.
Bandwidth utilization	Always uses total bandwidth.	Use only a portion of total bandwidth at a time.
Resistance to interference	DSSS works best for large data packets in a low to medium interference environment.	FHSS works best for small data packets in high interference environment.
Effect of multipath fading	DSSS systems operate over wider bands, transmitting their signal over a group of frequencies simultaneously. As long as the average level of the received signal is high enough, the DSSS receiver will be able to detect the radio signal.	FHSS systems operate with narrow band signals located around different carrier frequencies. If at a specific moment, the FHSS system is using a carrier frequency significantly faded as a result of multipath, the FHSS receiver could not get enough energy to detect the radio signal.
Effect of delay spread	In DSSS systems, the chipping process generates a high rate transmitted signal. The symbols of this transmitted signal are much shorter / narrower (in time) than the symbols generated by an FHSS system transmitting the same data rate. These narrow pulses are more sensitive to delays than a wider pulse used in FHSS systems.	FHSS systems have better chances to be undisturbed by the presence of multipath effects (delay spread).
Power control	Near far problem exists in DSSS and therefore precise power control is required.	It is not much affected by near far problem as in DSSS hence power control is not a problem
Acquisition Time	Due to long PN codes it requires long acquisition time	It has relatively short acquisition time because the chip rate is considerably less in the frequency hopping system.

Review Questions

Q. 1 What types of mobile and wireless devices are available in the market ?

Q. 2 Explain the needs of mobile communication with its applications.

Q. 3 Explain multi-path propagation and Different types of path losses and signal propagation effects in wireless transmission.

Q. 4 Explain various wideband modulation techniques employed in cellular / mobile technologies.

Q. 5 Draw the block diagram of FHSS transmitter and receiver. Differentiate between slow hopping and fast hopping.

Q. 6 Explain what is spread spectrum? How spreading can be achieved? What are the merits of spread spectrum technique?

Q. 7 Explain different methods to increase the capacity of an analog cellular system and without increasing number of antennas.

Q. 8 What are the advantages of cellular System? Explain cellular system in detail also explain frequency reuse concept in cellular system.

Q. 9 What do you mean by frequency reuse concept? Explain.

Q. 10 What is CDMA? How does it suit to mobile cellular systems ?

Q. 11 Discuss different multiplexing techniques.

❑❑❑

GSM

Syllabus

2.1 GSM Mobile services, System Architecture, Radio interface, Protocols , Localization and Calling, Handover, security (A3, A5 & A8)

2.2 GPRS system and protocol architecture

2.2 UTRAN, UMTS core network; Improvements on Core Network

2.1 GSM

Global System for Mobile communication (GSM) is the most successful digital mobile telecommunication system in the world today. It is used by over 1000 million people in more than 190 countries. The primary goal of GSM was to provide a mobile phone system that allows users to roam throughout Europe and provides voice service that is compatible to ISDN and PSTN. This chapter gives an insight of GSM system including its services, architecture, call set up procedure, handover and other important aspects such as security and authentication.

2.1.1 GSM Overview

MU - Dec. 12

Q. List and explain GSM services. **(Dec. 12, 5 Marks)**

- Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication. It is an ETSI standard for 2G pan-European digital cellular system with international roaming.
- The basic version of GSM (i.e. GSM 900) was founded in 1982.
- Now it is the most successful mobile communication system in the world and over 1.2 billion users use the system.
- The main goal of GSM was to provide voice services that are compatible to ISDN and other PSTN systems at the same time allowing users of the system to roam throughout Europe.
- GSM is a second generation 2G system, replacing the first generation analog systems.
- The initial version of GSM was designed in Europe using **890-915MHZ** for **uplink** and **935-960 MHz** for **downlink**. This system is called **GSM 900**.
- Another version of GSM called Digital Cellular System 1800 (DCS 1800) uses 1710-1785 MHz for uplink and
- 1805-1880 MHz for downlink.
- GSM at 1900 MHz (1850-1910 MHz uplink and 1930-1990 MHz downlink) used in US is called PCS (Personal Communication Services) 1900.

Modifications and Derivatives of GSM

- The system evolution of GSM can be divided into three phases.
  - **Phase 1 (1991-1994) :** The basic version of the GSM system was in operation.

- **Phase 2 (1994-1995) :** The system specification was verified in order to allow future gradual modifications and new improvements.
- **Phase 3 (from 1995) :** The modifications to the original GSM900 are being introduced.

– Following are the derivatives of the original GSM 900.

DCS 1800

– One important modification to the original GSM900 was the development of **Digital Cellular System** (DCS 1800).

– DCS 1800 is primarily devoted to the operation in areas with high traffic such as urban and suburban areas.

– It is called as DCS in United Kingdom and PCS in Hong Kong.

– The main difference between GSM900 and DCS1800 was in the lower power of the base station and mobile station. As a result the cell size becomes smaller.

– The bandwidth assigned to the DCS1800 was much higher than the GSM900. This implies that up to 374 carrier frequency channels can be assigned to the DCS1800. Thus the capacity of DCS1800 is much higher than the GSM900. But this also implies twice as high sensitivity to Doppler effects. This limits the maximum vehicle speed in DCS1800 up to 130km/hr.

– Another essential enhancement of the DCS1800 is the possibility of roaming inside the country. This was not possible with initial GSM900 due to organization reason.

– Table 2.1.1 summarizes the basic difference between GSM900 and DCS1800.

Table 2.1.1 : Difference between GSM 900 and DCS 1800

Feature	GSM 900	DCS 1800
Frequency range	Uplink 890-915 MHz Downlink 935-960 MHz	Uplink 1710-1785 MHz Downlink 1805-1880 MHz
Number of duplex channels	124	374
Maximum Base station power	320W	20W
Maximum Mobile station power	8W	1W
Spacing between uplink and downlink frequencies	45MHz	95MHz
Maximum vehicle speed	250km/hr	130km/hr
MS classes	20W (not implemented) 8W (car/ transportable phone) 5W (car/ transportable phone) 2W (handheld) 0.8 W (handheld	1W (handheld) 0.25 W (handheld)

– Table 2.1.2 lists the key milestones of the GSM system and its derivatives.

GSM 400

– Another promising modification and enhancement of the original GSM 900 system was GSM 400. It has been observed that the analog systems operating in the 400 MHz bands are now becoming absolute. They are losing their customers as most of them moved to the 2G systems.

- After shutting these analog systems completely, this frequency range can be used for another GSM version.
- ETSI standardized the GSM system operating in the band around 450 and 480 MHz called GSM 400.
- The whole infrastructure will remain same however software needs to be changed.
- The basic feature of GSM 400 are listed below:
  - Frequency allocation : Uplink : 450.4-457.6 MHz
    Downlink : 460.4-496.0 MHz
  - Duplex separation : 10 MHz
  - Carrier spacing : 200KHz

Table 2.1.2 : Key milestones of the GSM system and its derivatives

Year	Milestone
1982	Groupe Special Mobile established by CERT to develop the pan-European cellular mobile system standards.
1985	Basic list of recommendations to be generated by the group was adopted.
1986	Field tests undertaken to prove which techniques should be adopted for the new system.
1987	TDMA approach adopted as the main access method for GSM. Frequency division is also used between channels, but time division is used in each individual frequency channel.
1988	GSM system validation undertaken.
1989	ETSI, European telecommunications Standards Institute takes on responsibility for managing the GSM standards.
1990	Phase 1 of the GSM specifications released.
1991	Commercial launch of the GSM service.
1993	Coverage of main roads GSM services start outside Europe.
1995	Phase 2 of the GSM specifications released.
2004	GSM subscriptions reach 1 billion.

2.1.2 Mobile Services

- GSM is an integrated voice-data service that provides various services beyond cellular telephone.
- GSM Mobile services are divided into categories.
  1. Bearer services
  2. Tele services
  3. Data services
  4. Supplementary services
- Fig. 2.1.1 shows the reference model of GSM Mobile teleservices and bearer services.

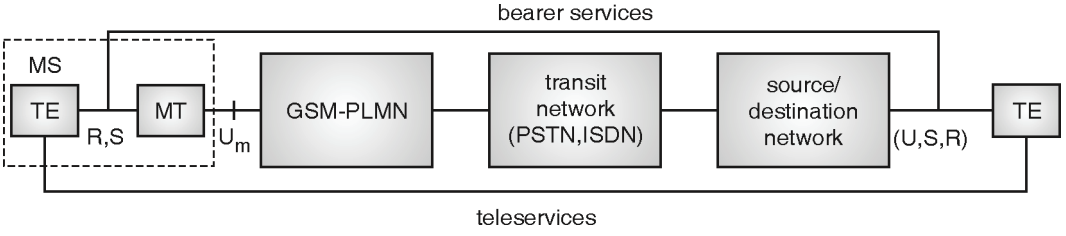


Fig. 2.1.1 : GSM Mobile services

1. Bearer services

- Bearer services are telecommunication services that provide capabilities to transfer user data and control signals between two pieces of equipment in a network.
- GSM provides basically four types of bearer services :
  - Transparent
  - Non-transparent
  - Synchronous data transmission
  - Asynchronous data transmission

(i) Transparent bearer services

- These types of bearer services use the functions of physical layer to transmit data.
- To improve the transmission quality, it uses forward error correction (FEC) at physical layer.

(ii) Non-transparent bearer services

- Non transparent bearer services use functions of both layer 2 and layer 3 to improve transmission quality.
- It implements layer 2 and layer 3 protocols for error correction and flow control.
- It also uses radio-link protocol (RLP) that comprises mechanism of **High Speed Data Link Control (HDLC)** and special **selective-reject** mechanism to trigger retransmission of data.
- The bit-error rate is less than 10^{-7}, and throughput and delay may vary depending upon transmission quality.
- Different data rates for voice and data that can be achieved are listed below.

2. Data Services

(i) Data service (circuit switched)

- Synchronous : 2.4, 4.8 or 9.6 kbit/s
- Asynchronous: 300 - 1200 bit/s

(ii) Data service (packet switched)

- Synchronous : 1.2, 2.4, 4.8 or 9.6 kbit/s
- Asynchronous : 300 - 9600 bit/s

3. Tele services

- Tele services include encrypted voice transmission, message services, and basic data communication with terminals.
- The GSM was basically designed to provide high quality digital voice transmission, offering at least the bandwidth
- 3.1 kHz of analog phone systems.

The various teleservices are :

(i) Emergency number

- It is mandatory for all service providers to implement Emergency number service.
- This number is the common number that can be used throughout country.
- Like police (100) or ambulance number and this number is free of charge.
- This connection has the highest priority and will automatically be set up with closest emergency center.

(ii) Short message services (SMS)

- SMS allows transmission of text messages up to 160 characters.

- SMS uses unused capacity in the signaling channels instead of standard data channels.
- It is possible to send or receive SMS during voice or data transmission.
- SMS can be used for displaying road conditions, e-mail headers or stock quotes etc.
- SMS are also used for updating mobile phone software or for implementation of push services.

(iii) Enhanced Message Service (EMS)

Enhanced message service (EMS) allows transmission of larger messages, formatted text, animated pictures, small images, and ringtones in a standardized way.

(iv) Multimedia Message service (MMS)

MMS allows transmission of larger pictures such as JPEG, GIF, WBMP files and also short video clips.

(v) Group 3 Fax

- In this service, fax data is transmitted as digital data over the analog telephone network using modems.
- It uses ITU-T standards T.4 and T.30 for transmission.
- Fax data and fax signaling is transmitted via transparent bearer service.

4. Supplementary services

- Supplementary services offer various enhancements of the standard telephony services and may vary from provider to provider.
- Supplementary services are additional services that are provided by the GSM system other than teleservices or bearer services.
- These services include facilities such as call forwarding, caller identification, call waiting, multi-party conversations, and barring of outgoing (international) calls, among others. Some supplementary services are :
  - Multiparty Service or conferencing
  - Call Waiting
  - Call Hold
  - Call Forwarding
  - Call Barring
  - Number Identification
  - Advice of Charge (AoC)
  - Closed User Groups (CUGs)
  - Unstructured supplementary services data (USSD) : This allows operator-defined individual services.

Table 2.1.3 : GSM services

Service Category	Service
Tele services	Telephony Emergency call Short message services Videotext access Teletex, Fax Half rate speech coder Enhanced full rate

Service Category	Service
Bearer services	Synchronous data Asynchronous data Synchronous packet data
Supplementary services	Call forwarding Call barring Calling line identification Connected line identification Call waiting Call hold Multiparty communication Closed user group Advice of charge Operator determined call barring

2.1.3 GSM System Architecture

MU - Dec. 12, May 13

Q. Draw a neat diagram of GSM system architecture and explain with different types of interfaces. **(Dec. 12, 10 Marks)**

Q. What is the use of HLR and VLR registers in Mobile computing? **(May 13, 5 Marks)**

- Fig. 2.1.2 shows the simplified view of the GSM system architecture.
- The GSM network architecture can be grouped into three main sub systems :

1. Radio subsystem (RSS)
2. Network and switching subsystem (NSS)
3. Operation subsystem (OSS)

1. Radio subsystem

Radio subsystem comprises all radio entities. Entities of RSS are explained below.

(i) Base station subsystem (BSS)

- A GSM network comprises many BSSs.
- BSS contains one or more radio cells, each one is controlled by a base transceiver station (BTS).
- One or more BTSs in turn are controlled by an element called Base station controller (BSC). Thus there are two main architectural elements in each BSS **BTS** and **BSC.**
- **BSS functions** are to :
  - Maintain radio connection to MS
  - Coding/decoding of voice
  - Rate adaptation to/from the wireless network part

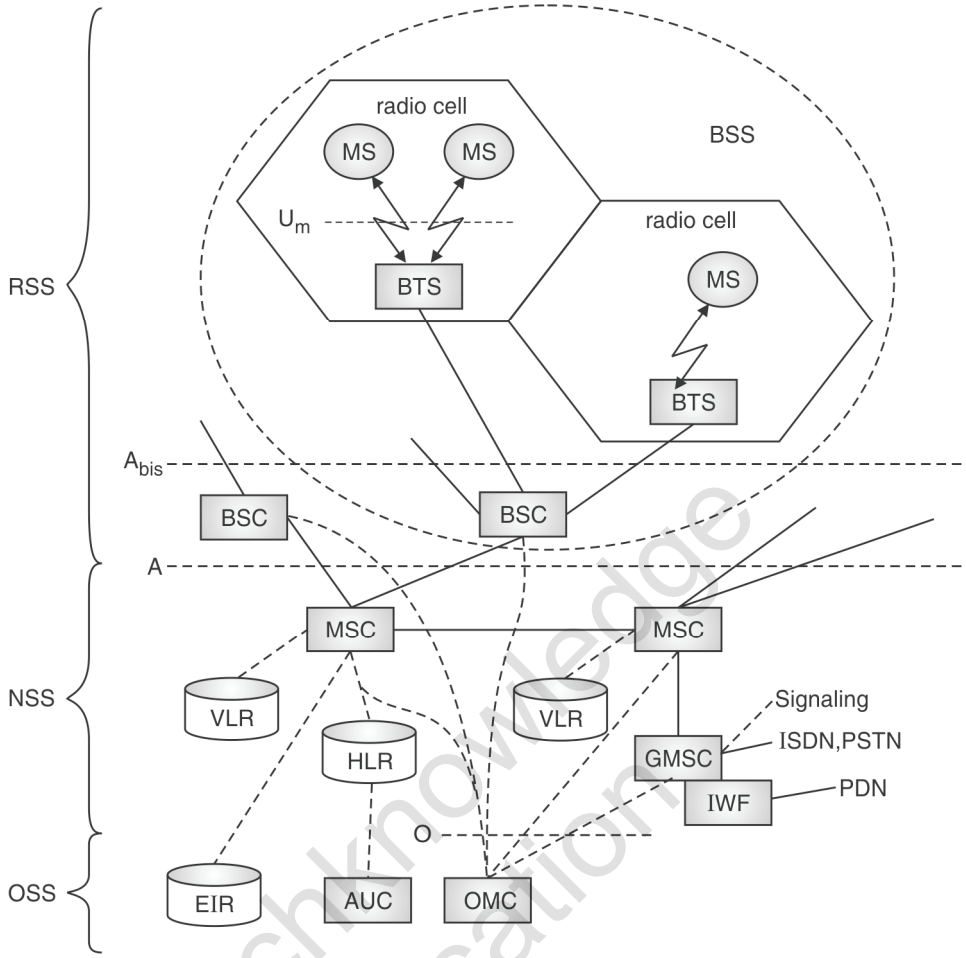


Fig. 2.1.2 : GSM system architecture

(ii) Base transceiver station (BTS)

- A BTS (also called base station) comprises all radio equipments, i.e. antennas, signal processing, amplifiers etc.
- BTS can form a single radio cell or several cells by using sectorized antennas.
- BTS is connected to MS via the **U_m interface** and to the BSC via the **A_{bis} interface**.
- **Functions of BTS** are :
  - Encoding, encrypting, multiplexing, modulating, and feeding the RF signals to the antenna
  - Transcoding and rate adaptation
  - Time and frequency synchronization
  - Voice through full- or half-rate services
  - Decoding, decrypting, and equalizing received signals
  - Random access detection
  - Uplink channel measurements

(iii) Base station controller (BSC)

- The BSC manages the radio resources for one or more BTSs.
- **Functions of BSC** are :
  - Handles radio channel setup, frequency hopping, and handovers.

- Assigns and releases frequencies and time slots for the MS.
- Handles inter cell handover.
- Controls the power transmission of the BSS and MS in its area.

– **Additional functions** include :

- Performing traffic concentration to reduce the number of lines from the MSC
- Reallocation of frequencies among BTSs
- Time and frequency synchronization
- Power management
- Time-delay measurements of received signals from the MS

(iv) Mobile station (MS)

– The MS comprises all user hardware and software needed for communication with a GSM network.

– International mobile equipment identity (IMEI) is used to identify an MS. Device specific mechanism like theft protection uses the IMEI number.

– MS consists of two elements mobile equipment (ME) and SIM.

– Mobile equipment (ME) is the hardware that is the mobile handset.

– The second component of MS is **subscriber identity module (SIM)**.

– SIM stores all user specific data relevant to GSM.

– All the calls in GSM are SIM based and they are directed to the SIM rather than terminal.

– All the data like SMS, contact numbers are also stored in SIM card.

– User specific functions like charging, authentication are also based on the SIM.

– Without SIM only emergency calls are possible.

– The SIM card contains many identifiers, and tables such as card type, serial number, a list of subscribed services,

– **A Personal Identification Number (PIN), PIN Unblocking Keying (PUK),** an **authentication key K_i** and the **International Mobile Subscriber Identity (IMSI)**.

– The mobile station also stores the dynamic information while logged onto the GSM system such as **cipher key K_c** and a **Temporary Mobile Subscriber Identity (TMSI)**, and the **Location Area Identification (LAI)**.

2. Network and Switching Subsystem (NSS)

– The NSS connects the radio network with the standard public mobile networks.

– The NSS includes the main switching functions of GSM, important databases (such as HLR, VLR) required to manage user profile and user mobility.

– The NSS contains the following functional elements.

(i) Mobile service switching center (MSC)

– MSC is the heart of the GSM architecture.

– They are high-performance digital ISDN switches.

– Each MSC controls one or more BSSs.

– MSC sets up the connections to other MSCs and to the BSCs via the **A interface**.

The MSC performs following functions

- Switching of calls between the mobile and other fixed or mobile network users
- Management of mobile services
- Registration
- Authentication
- Location updating
- Handovers
- Call routing to a roaming subscriber
- Toll ticketing
- Network interfacing
- Common channel signaling

- MSCs are connected with each other and also to the Gateway MSCs (GMSC).
- **Gateway MSC** is responsible for communication with the external fixed networks such as PSTN and ISDN.
- MSC can also connect to public data networks (PDN) such as x.25 by using additional interworking functions (IWF).

(ii) Home Location Register (HLR)

- The HLR register is the central database that stores and manages the permanent information of the subscriber.
- When an individual buys a subscription in the form of SIM, all the information about this subscription is registered in the HLR of that operator.
- HLR contains the following static and dynamic information.

(a) Static information

- Mobile subscriber ISDN number (MSISDN)
- International mobile subscriber identity (IMSI)
- List of services to which user has subscribed such as call forwarding, roaming restriction, GPRS etc.

- All these user-specific information is entered once for each user in a single HLR at the time of subscription.
- HLR also maintains some dynamic information that is used for locating the user.

(b) Dynamic information

- The current location area (LA) of MS
- The mobile subscriber roaming number (MSRN)
- Current VLR and MSC

- As soon as MS leaves its current LA, the VLR that is currently responsible for the MS informs HLR about its new location.

(iii) Visitor Location Register (VLR)

- The VLR is associated to each MSC.
- It is a database containing records of all mobile stations currently registered with the attached MSC.
- When a mobile station roams into a new MSC area, the VLR connected to that MSC will request data about the mobile station from the HLR.
- Later if the mobile station makes a call, the VLR need not contact HLR each time since the VLR has all the information needed to set up the call.
- The VLR avoids the frequent HLR access/updates, as all the user information required is available in VLR.

3. Operation Sub System (OSS)

- The OSS is the functional entity which is used to monitor and control the overall GSM network.
- It is also used to control the traffic load of the BSS.
- OSS contains the following entities.

(i) Operation and Maintenance Center (OMC)

- The operations and maintenance center (OMC) is connected to all equipment in the switching system and to the BSC.
- The OMC monitors and controls all other network entities via the ***O interface***.
- Here are some of the OMC functions :
  - Administration and commercial operation (subscription, end terminals, charging and statistics).
  - Security Management.
  - Network configuration, Operation and Performance Management.
  - Maintenance Tasks.
  - Traffic monitoring
  - Status reports of network entities

(ii) Authentication Center (AUC)

- The Authentication Center is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and ciphering of the radio channel.
- The AUC protects network operators from different types of fraud.
- AUC contains the algorithms for authentication as well as the keys for encryption and generates the values needed for user authentication in the HLR.

(iii) Equipment Identity Register (EIR)

- The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipments on the network. It stores International Mobile Equipment Identity (IMEI) number for each valid mobile equipment.
- The EIR has a black list of stolen mobile devices.
- If a particular mobile is stolen or is not type approved then corresponding IMEI is marked as invalid in the EIR.

2.1.4 GSM Radio Interfaces

MU - Dec. 15

Q. Explain the U_m interface of GSM. **(Dec. 15, 5 Marks)**

Different elements of GSM network communicate to each other using well defined interface between them.

Um Interface :

- The **U_m interface** is the **air interface** for the **GSM** mobile telephone standard.
- It is the **interface** between the mobile station (MS) and the Base transceiver station (BTS).
- It is called **Um** because it is the mobile analog to the U **interface** of ISDN.
- **Um** is **defined** in the **GSM** 04.xx and 05.xx series of specifications.
- The GSM air interface is based on Time Division Multiple Access (TDMA) with Frequency Division Duplex (FDD).
- TDMA allows multiple users to share a common RF channel on a time-sharing basis, while FDD enables different frequencies to be used in uplink (MS to BTS) and downlink (BTS to MS) directions.

- Most of the implementations use a frequency band of 900 MHz. The other derivative of GSM is called Digital cellular system uses 1800 MHz (DCM1800).
- The used frequency band is divided into 200KHz carriers or RF channels in both the uplink and downlink direction.
- Each RF channel is then further subdivided into eight different timeslots, i.e., 0 to 7, by TDMA techniques.
- A set of these eight timeslots is referred to as a TDMA frame.
- Each frame lasts 4.615 msec.
- The physical channels are further mapped to various logical channels carrying user traffic and control information between the MS and the BTS.
- The following section describes the Um interface protocols used at the MS and the BTS side.

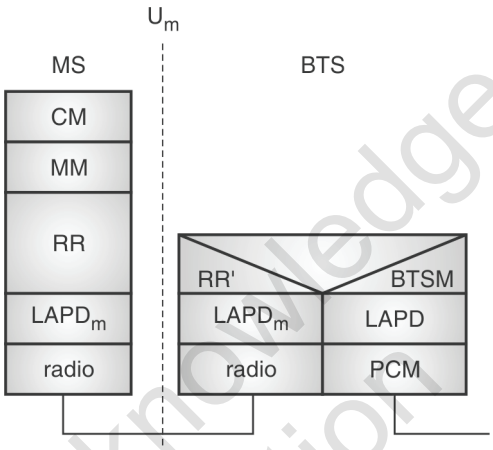


Fig. 2.1.3 : The Um interface between MS and BTS

Physical layer

Layer 1, which is a radio interface, provides the functionality required to transfer the bit streams over the physical channels on the radio medium. The services provided by this layer to the above layers include :

- Channel mapping (logical to physical)
- Channel coding and ciphering
- Digital modulation
- Frequency hopping
- Timing advance and power control

Data link layer

- Signaling Layer 2 is based on the LAPDm protocol, which is a variation of the ISDN LAP-D protocol.
- The main task of LAPDm is to provide a reliable signaling link between the network and the mobile station.
- The LAP-D protocol has been modified to adapt in the mobile environment.

Network layer

- Signaling Layer 3 takes care of signaling procedures between an MS and the network. It consists of three sublayers with distinct signaling procedures.
  - Radio resource management (RR)
  - Mobility management (MM)
  - Connection management (CM)

- Radio resource management (RR) comprises procedures required to establish, maintain, and release the dedicated radio connections. The RR sub layer functions include :
  - Channel assignment and release
  - Ciphering
  - Modification of channel modes, e.g., voice and data
  - Handover between cells
  - Frequency redefinition to enable frequency hopping
  - MS measurement reports
  - Power control and timing advance
  - Paging
  - Radio channel access
- The mobility management (MM) sublayer handles functions and procedures related to mobility of the mobile user. This includes procedures for Authentication and Location registration and periodic updating.
- The connection management (CM) sublayer contains the functions and procedures for call control. This includes procedures to establish, release, and access services and facilities.

(i) **A_{bis} Interface :** BSC and BTS communicate via A_{bis} interface. The A_{bis} interface is associated with the information exchange related to the radio transmission such as distribution of radio channels, connection supervising, the queuing of messages before transmission, frequency hopping control, channel coding, decoding etc.

(ii) **A interface :** The A interface is used to provide communication between the BSS and the MSC. It is based on **circuit switched PCM-30** systems. It carries up to 3064 kbits/s connections. The interface carries information to enable the channels and timeslots allocated to the mobile equipments. The messaging required within the network to enable handover is also carried over this interface.

(iii) **O interface :** The RSS is connected with OSS by **O interface**. O interface uses the **Signaling system No. 7 (SS7)** based on X.25 and carries management data to/from the RSS.

Other interfaces that are used in GSM are :

(i) **B interface :** B interface exist between the MSC and the VLR. It uses a protocol known as the **MAP/B protocol**. We know that most VLRs are collocated with an MSC. This makes the interface purely an "internal" interface. The interface is used whenever the MSC needs to communicate with the VLR in order to access data regarding an MS located in its area.

(ii) **C interface :** The C interface is used to provide communication between the HLR and a GMSC. The call that is originating from outside the network has to pass through the gateway so that routing information required to complete the call may be gained. This interface uses **MAP/C protocol.**

(iii) **D interface :** The VLR and the HLR communicates via D interface. It uses the **MAP/D** protocol. The information related to the location of MS is exchanged between the VLR and HLR over this interface.

(iv) **E interface :** The E interface provides communication between two MSCs. It uses **MAP/E** protocol to exchange data related to handover between the anchor and relay MSC.

2.1.5 GSM Protocols and Signaling Architecture

MU - May 14

Q. Explain the GSM protocol architecture. **(May 14, 10 Marks)**

- Fig. 2.1.4 presents the protocol architecture of GSM with signaling protocols and interfaces.

Based on the interface, the GSM signaling protocol is assembled into three general layers :

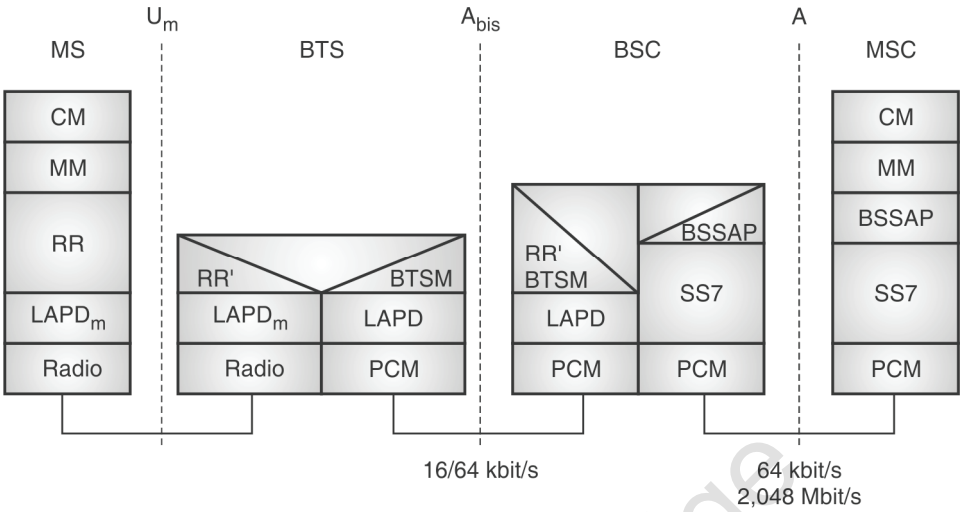


Fig. 2.1.4 : GSM protocol stack for signaling

Layer 1 : The physical layer, which uses the channel structures over the air interface.

- The main functions of physical layer are :
  - Handles all radio-specific functions
  - Creation of bursts
  - Multiplexing of bursts into TDMA frames
  - Synchronization with the BTS
  - Detection of idle channels
  - Measurement of the channel quality on downlink.
- The physical layer at U_m interface uses GMSK for digital modulation and performs encryption/decryption of data.

Layer 2 : The data-link layer

- The data-link layer uses LAPDm (Link access protocol on the D_m channel) protocol across the Um interface,
- LAPD (Link access protocol for the D channel) is the ISDN protocol for D channel.
- $LAPD_m$ is a modified version of LAPD for mobile stations. It does not need synchronization flags or check sum for error detection.
- $LAPD_m$ offers following functionality :
  - Reliable data transfer over connections
  - Re-sequencing of data frames
  - Flow control
  - Segmentation and reassembly of data
  - Acknowledged/unacknowledged data transfer.

Layer 3 : The third layer of the GSM signaling protocol is divided into three sub layers:

- Radio Resource management (RR)
- Mobility Management (MM) and
- Connection Management (CM).

The MS to BTS Protocols

- The RR layer takes care of the establishment of a link, both radio and fixed, between the MS and the MSC.
- The main functional components involved are the MS, the BSS, and the MSC.
- The **RR layer** is concerned with the management of an RR-session, which is the time that a mobile is in dedicated mode and is configuring the radio channels.
- The **MM layer** is built on top of the RR layer and handles the functions that arise from the mobility of the subscriber. It also handles authentication and security aspects.
- The **CM layer** is responsible for call control (CC), supplementary service management, and Short Message Service (SMS) management. Each of these may be considered as a separate sub layer within the CM layer.

BSC Protocols

- After the information is passed from the BTS to the BSC, the A_{bis} interface is used between the BTS and the BSC.
- At this level, the radio resources at the lower portion of Layer 3 are changed from the RR to the Base Transceiver Station Management (BTSM).
- The BTS management layer is a relay function at the BTS to the BSC.
- The **RR protocols** provide the procedures for the use, allocation, reallocation, and release of the GSM channels.
- The BSC still has some radio resource management in place for the frequency coordination, frequency allocation, and the management of the overall network layer for the Layer 2 interfaces.
- From the BSC to MSC, the relay is using SS7 protocols and the BSS mobile application part (BSSAP) is used to communicate from the BSC to MSC.

MSC Protocols

- At the MSC, the information is mapped across the A interface.
- Here the equivalent set of radio resources is now called the BSS Application Part (BSSAP).
- This completes the relay process. Through the control-signaling network, all the MSCs interact to locate and connect to users throughout the network.
- Location registers are included in the MSC databases to assist in the role of determining how and whether connections are to be made to roaming users.

Signaling system No. 7 (SS7)

SS7 is used for signaling between MSC and a BSC. This protocol is used to transfer all management information between MSCs, HLR,VLRs, AuC, EIR, and OMC.

2.1.6 Localization and Calling Description of the Call Setup Procedure

GSM supports automatic, worldwide localization of users. The system always knows location of the user, and the same phone number is valid worldwide. As soon as mobile station moves to a new area, its VLR change. The HLR sends all user data needed to the new VLR.

To locate mobile station and to address the MS, several numbers are needed :

1. Mobile Station International ISDN Number (MSISDN)

- This is the mobile phone number of the user.
- This number consists of the **country code (CC)** followed by national **destination code** (NDC) (address of service provider) and the **subscriber number (SN)** (e.g. +91 973 1234567).

2. International Mobile Subscriber Identity (IMSI)

- GSM uses IMSI for internal unique identification of a subscriber.
- IMSI consists of a mobile country code (MCC), the mobile network code (MNC) (the code of service provider), and the mobile subscriber identity number (MSIN).

3. Temporary Mobile Subscriber Identity (TMSI)

- To hide the IMSI over radio interface, GSM uses 4 byte TMSI for local subscriber identification.
- TMSI is selected by the current VLR and is valid for temporarily and within the location area of the VLR.
- VLR may change TMSI periodically.

4. Mobile Station Roaming Number (MSRN)

- MSRN is a temporary address generated by VLR that is used to hide the identity and location of a subscriber.
- The VLR generates this address on request from the MSC.
- This MSRN address is also stored in the HLR.
- MSRN contains the current **Visitor Country Code (VCC)**, the identification of the **current MSC** and the **subscriber number**.
- All these above mentioned numbers are needed to locate a mobile station and maintain connection with it.

2.1.6(a) Initialization

- Whenever a mobile station (MS) is powered on, sequence of operations have to be performed in order to activate the mobile in the given network.
- First, MS looks for the carrier on which the broadcast channel is transmitted.
- In order to do this, MS scans all 124 channels and measures their received power level. The carrier containing the broadcast channel is emitted at a much higher power than other carriers in the same cell.
- The MS lists the measured carriers according to their decreasing power.
- In the next step, the MS listens to the subsequent carriers from the list and searches for the frequency correction channel (FCCH). This is done by scanning 0^{th} slot of the broadcast carrier.
- The MS carrier frequency is then adjusted to that frequency.
- MS then finds other important control information by scanning 0^{th} slot of subsequent frames.
- At this moment the passive part of the MS activation in the network is completed.

2.1.6(b) Registration and Location Update

- In order to initiate a call or to be paged, MS has to register itself with the network.
- Registration takes place if the Location Area Identity (LAI) number received by the MS from the BTS is different than what is stored in the MS.
- The location update takes place in following cases:
  - When the MS has been switched off and wants to become active, or
  - When it is active but not involved in a call, and it moves from one location area to another.
  - After a regular time interval.
- The **Location Update process** consists of the following phases :
  1. Request for service
  2. Authentication
  3. Ciphering
  4. Update HLR/VLR
  5. TMSI re-allocation

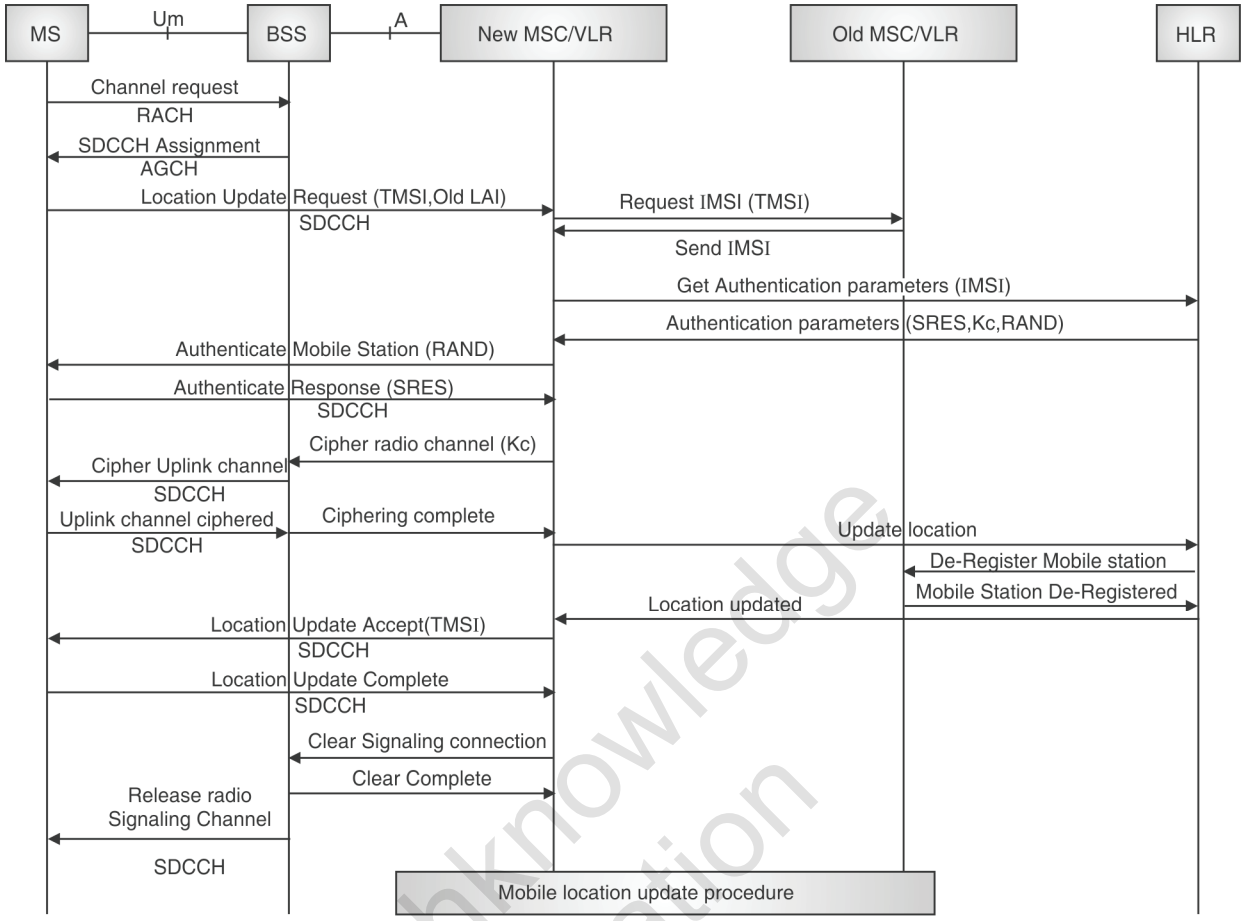


Fig. 2.1.5 : Registration and location update

- At this point, we are ready to inform the HLR that the MS is under control of a new VLR and that the MS can be de-registered from the old VLR. The location of the user is updated in the HLR.
- The new LAI and TMSI is sent to the MS. MS confirms the new LAI and TMSI. Here the location update procedure is complete. The SDCCH channel is released.
- The step by step procedure is illustrated in Fig. 2.1.5.
- The first task an MS has to do is to acquire a channel for registration. The MS does this by transmitting the RACH in which the MS requests the BTS for a channel to be used for registration.
- The BTS transfers this request to the BSC.
- In turn the BSC informs the BTS to assign a free Standalone Dedicated Control Channel (SDCCH) to the MS.
- The BTS sends the confirmation to MS on Access grant channel (AGCH) and allocates SDCCH to MS.
- In turn the MS sends the location update request on newly assigned SDCCH. The request contains TMSI and old LAI.
- This request is forwarded to the new MSC and corresponding VLR through the BTS and BSC.
- If the VLR already contains the user's TMSI, it updates its data.
- If no TMSI exist for that user then the LAI sent by the user is decoded. The LAI indirectly describes the VLR that previously served the MS.

- The current VLR takes all the user's parameters such as IMSI number, authentication and encryption parameters from the previous VLR.
- If the previous VLR does not contain this information then the MS needs to transmit its IMSI on SDCCH.
- The MS sends its IMSI through air only once. This happens at the first entry to the network.
- The IMSI number determines the ***address of the user data in the HLR***. This information from the HLR is loaded in the current VLR. The information contains authentication parameters for the user.
- After that the new VLR initiates the user authentication process and the user replies are verified.
- The new MSC/VLR requests the BSS to cipher the radio channel. The BSS upon ciphering the downlink channel sends a cipher complete message to the MSC.

2.1.6(c) Mobile Terminated Call (MTC)

MU - May 14, Dec. 15

Q. Describe the call initiation and call termination procedure in GSM systems. **(May 14, 10 Marks)**

Q. Explain Mobile Call termination in GSM, detailing the need and the use of MSRN, IMSI, TMSI nos. **(Dec. 15, 10 Marks)**

This is the situation where a terminal from a fixed network calls a mobile station. This involves the following steps (Fig. 2.1.6).

Step 1 : A PSTN user dials the phone number of a GSM subscriber. The fixed network (PSTN) notices that the number is of the GSM network and forwards call setup to the Gateway MSC (GMSC).

Step 2 : GMSC identifies the HLR (from the IMSI number of the called MS) for the subscriber and signals the call setup to the HLR.

Step 3 : The HLR now checks whether the number exists and whether the user has subscribed to the requested service.

Step 4 : HLR requests a Mobile subscriber roaming number (MSRN) from the current VLR.

Step 5 : HLR receives MSRN. And the HLR can determine responsible MSC for the MS.

Step 6 : The HLR forwards this information to GMSC.

Step 7 : The GMSC forwards call setup request to the MSC.

Step 8, 9 : The MSC first requests the current status of the MS from the VLR.

Step 10 : If the MS is available, the MSC initiates paging in all cells.

Step 11 : The BTSs of all BSSs transmit this paging signal to the MS.

Step 12, 13 : The MS answers.

Step 14, 15 : The VLR does security checks.

Step 16, 17 : The Connection is setup.

Fig. 2.1.7 illustrates the messages exchange between the MS and the BTS taken place during the connection setup.

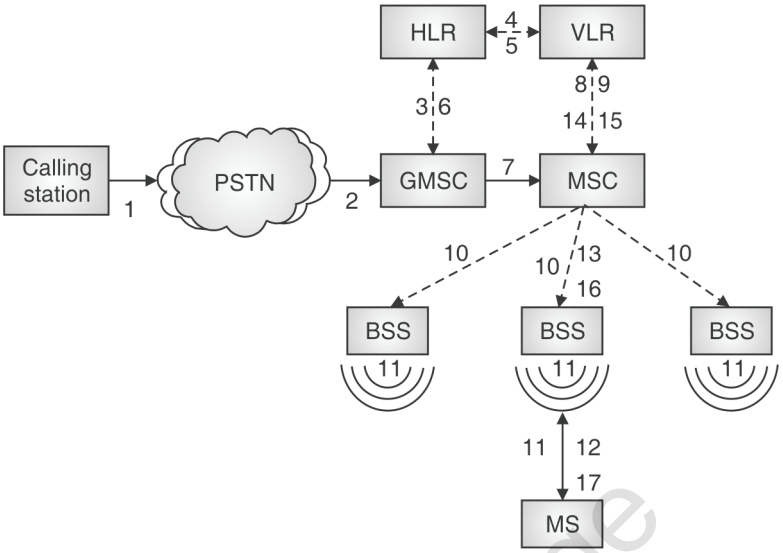


Fig. 2.1.6 : Mobile terminated call

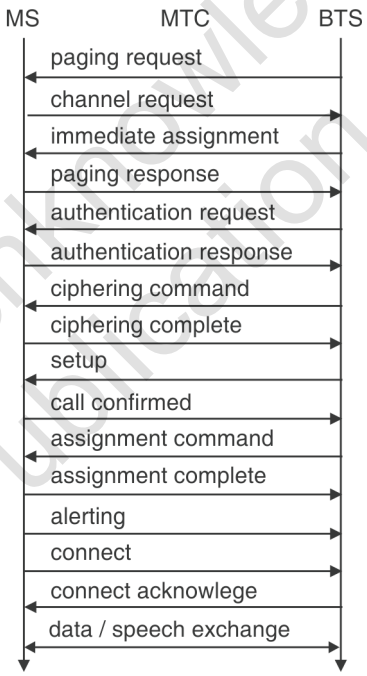


Fig. 2.1.7 : Message flow for MTC

- Note that the location area is served by many base stations. So after determining this area, the MSC sends a paging request to all BSCs operating in the determined location area.
- If the mobile station detects the paging directed to it, it requests the BTS for the channel on RACH.
- The BSC then assigns the SDCCH channel to the MS and informs MSC about the assignment.
- MS sends the paging response on this assigned SDCCH.
- Now VLR initiates the MS **authentication** process that involves the MSC, BSC an MS.
- After the MS has been authenticated, the VLR issues a command to MSC to start **data encryption**. The MSC in turn transfers this command to the MS through BSC and BTS.

- After the initiation of the encryption in the MS, a new TMSI number is assigned to the MS for the time of connection. The MS acknowledges reception of this number.
- At this moment the MSC initiates the **connection setup** with the MS by sending a set up message to it. The MS acknowledges the receipt of this message.
- MSC then informs BSC to assign a traffic channel to the MS. MS receives the carrier number, a time slot and a training sequence for the connection. MS acknowledges these parameters.
- The MS then starts ringing and the MSC is informed about it.
- The MSC then sends the ringing signal to the calling user.
- After the MS accepts the call, actual data transfer starts.

2.1.6(d) Mobile Originated Call (MOC)

MU - May 16, Dec. 16

Q. Explain how Mobile Originated Call (MOC) work. **(May 16, Dec. 16, 10 Marks)**

It is much simpler to perform a mobile originated call (MOC) compared to MTC. This follows the following steps (Refer Fig. 2.1.8).

Step 1 : The MS transmits the request for a new connection. This is realized by the MS sending a random access burst on RACH logical channel.

Step 2 : The BSS forwards this request to the MSC.

Step 3, 4 : MSC then checks if this user is allowed to setup a call with the requested service.

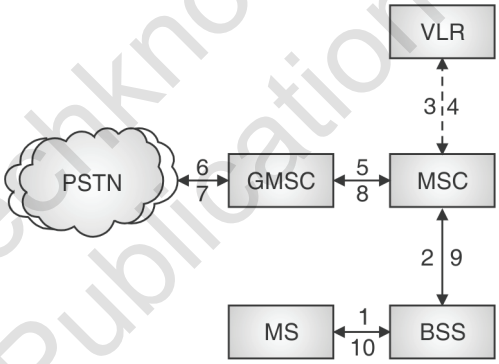


Fig. 2.1.8 : Mobile originated call

Step 5-8 : The MSC checks the availability of resources through GSM network and into the PSTN.

Step 9, 10 : If all resources are available, the MSC sets up a connection between MS and the fixed network.

In addition to the above steps, other messages are exchanged between an MS and BTS during connection setup. Fig. 2.1.9 shows the messages for MOC.

- MS has to receive an access grant on AGCH in response to the channel request sent on RACH. This AGCH contains the number of the SDCCH assigned to the MS to be used for connection set up.
- All subsequent communication between the MS and the BTS will happen on this assigned SDCCH.
- The MS sends call set up request to the BSC via BTS.
- The BSC transfers this message to the MSC.
- MSC in turn informs the VLR associated with it about the call set up request issued by the MS.

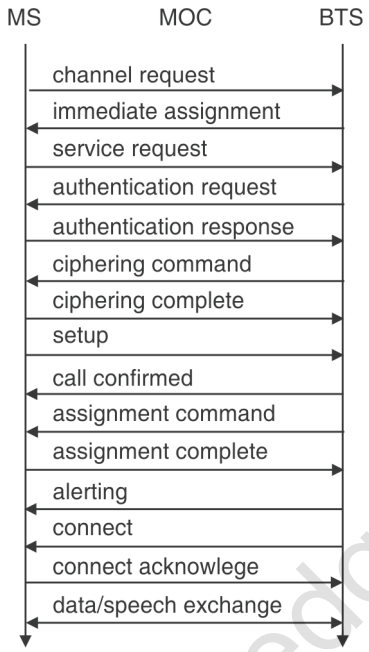


Fig. 2.1.9 : Message flow for MOC

- In turn VLR initiates authentication process.
- After the MS has been authenticated, the encryption procedure is started by the VLR.
- A new TMSI number is assigned to the MS. The MS acknowledges the reception of TMSI. The MSC then assigns a fixed link to the call and a traffic channel to the MS.
- MS acknowledges the channel assignment. This information reaches the MSC.
- MSC sends the alert message to the MS through BSC and BTS when the called mobile station starts ringing.
- When the called mobile station accepts the call, the MS is informed about it by sending connect message.
- Finally MS acknowledges this connect message and data transfer starts.

2.1.7 Handover in GSM

MU - May 15, May 16

Q.	Explain various types of handoffs in GSM network.	**(May 15, 5 Marks)**
Q.	What are the different types of handover in GSM ?Explain in detail intra-MSC handover ?	**(May 16, 10 Marks)**

- When a mobile user is engaged in conversation, the MS is connected to the BTS via radio link. If the mobile user moves to the coverage area of another BTS, the radio link to the old BTS is eventually disconnected, and a radio link to the new BTS is established to continue the conversation. This process is called handover or handoff.
- Handover is required in cellular networks, as a single base station do not cover the whole service area.
- The number of handovers to be performed depends on two factors :
  - **Cell size :** The smaller is the size of cell more the handovers required.
  - **Speed of MS :** Higher the speed of MS more handovers are required.

There are two basic reasons for handover :

1. MS moves out of the range of BTS

- As a mobile station is moved out of the range of BTS, the received signal level falls below the minimal requirement of communication.
- The error rate grows due to interference and low signal strength.
- All these effects may diminish the quality of radio link and make communication impossible.

2. Load balancing

- If the traffic in one cell is too high then the MSC or BSC shifts some MS to other cells.
- Fig. 2.1.10 shows the four possible handover scenarios in GSM.

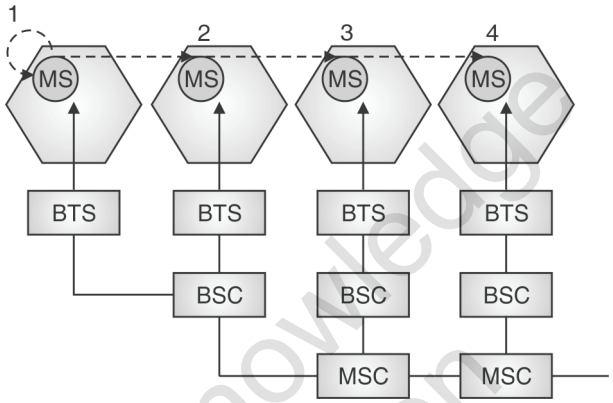


Fig. 2.1.10 : Handover scenario in GSM

(i) Intra-cell handover : This handover takes place within a cell. This handover is performed in order to optimize the traffic load in the cell or to improve the quality of the connection by changing the carrier frequency (scenario 1).

(ii) Inter-cell, intra-BSC handover : This handover occurs when a mobile station moves from one cell to another cell, but stays within the control of same BSC. The BSC then performs the handover, it assigns a new radio channel in the new cell and releases old one (scenario 2).

(iii) Inter-BSC, intra-MSC handover : This handover takes place between two cells managed by different BSCs. This handover is controlled by MSC (scenario 3).

(iv) Inter MSC handover : Inter MSC handover takes place between two cells belonging to different MSCs. Both MSCs perform the handover together (scenario 4).

Inter-BSC, Intra-MSC handover

- Fig. 2.1.11 shows the typical signal flow during an inter-BSC, intra-MSC handover.
- The MS sends its periodic measurement reports to the BTS_{old}.
- The BTS_{old} forwards these reports to the BSC_{old} together with its own measurements.
- Based on these values the BSC_{old} decides to perform a handover and sends the message HO_required to the MSC.
- The MSC then requests the resources needed for the handover from the new BSC.
- This BSC_{new} checks, if enough resources are available. If the resources are available then it activates a physical channel at the BTS_{new} for the MS.
- BTS_{new} sends acknowledgement of successful channel activation to BSC_{new}. and BSC_{new} acknowledges the handover request.
- The MSC then issues a handover command that is forwarded to the MS.

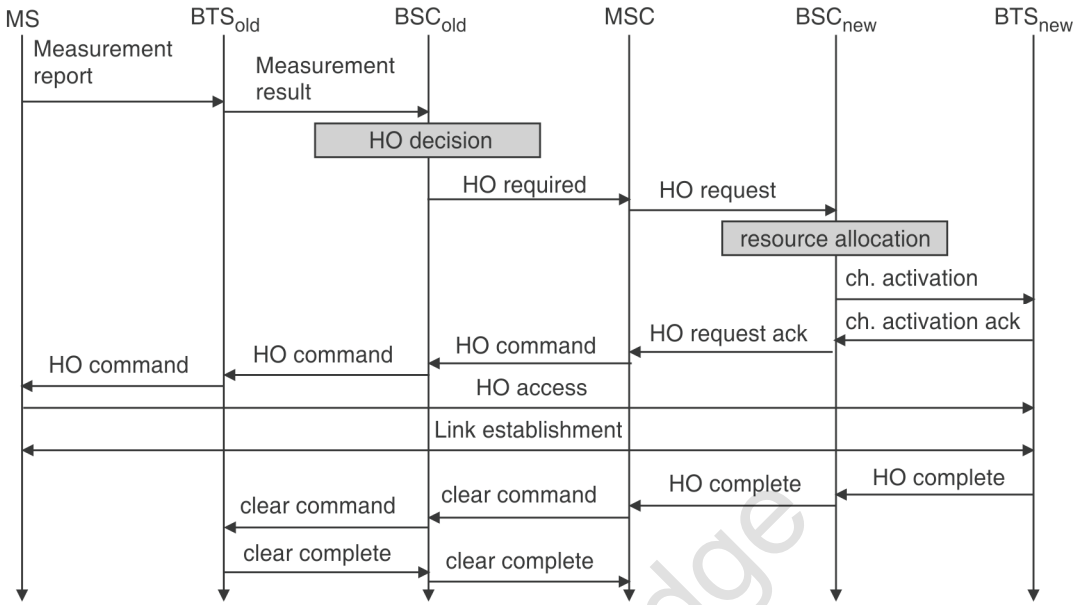


Fig. 2.1.11 : Intra MSC, inter BSC Handover process

- The MS now breaks the old connection and accesses the new BTS. Now a new radio link is established between the MS and BTS$_{new}$.
- All the reserved resources at the old BSC and BTS are released.
- Note that in the GSM systems the measurements are performed by both MS and the BTS.
- The quality and the power level of the received signal are measured in both the directions. The MS performs regular measurements of the 16 strongest carriers transmitting the BCCH.
- The measurements of the six best carriers are transmitted to the BTS every 0.48 sec.

2.1.8 GSM Security

MU - May 12, Dec. 14, May 15, Dec. 16

Q.	What are the functions of Authentication and Encryption in GSM ?	**(May 12, 10 Marks)**
Q.	Describe how data encryption is done is GSM system, with diagram explaining the role of SIM, A3, A5 and A8 algorithm.	**(Dec. 14, 10 Marks)**
Q.	Write a short note on Privacy and authentication in GSM.	**(May 15, 10 Marks)**
Q.	Explain in detail how Subscriber Authentication is done GSM.	**(Dec. 16, 10 Marks)**

GSM offers several security services using confidential information stored in the **AuC** and the **SIM**. These security services offered by GSM are explained as follows.

1. Access control and authentication

- This includes the authentication of a valid user for the SIM. The user needs to enter a secret PIN to access a SIM.
- The GSM network also authenticates the subscriber. This is done through the use of a challenge-response mechanism.

2. Confidentiality

- In GSM, confidentiality of user data is achieved by encrypting the data over air interface.
- After authentication MS and BTS apply encryption to voice, data, and signaling information.
- The confidentiality exists between MS and BTS only. It does not exist end-to-end.

3. Anonymity

- To provide anonymity the identity of a subscriber is always hidden over the air interface. All data is encrypted before transmission and user identifiers are not used over the air.
- To ensure subscriber identity confidentiality, the Temporary Mobile Subscriber Identity (TMSI) is used. VLR may change this TMSI at any time.
- Three algorithms are used to provide security services in GSM.
  - **Algorithm A3** is used for authentication.
  - **Algorithm A5** is used for encryption.
  - **Algorithm A8** is used for generation of cipher key.
- Earlier only algorithm A5 was publically available, where as A3 and A8 were secret. However A3 and A8 are no longer secret they were published on the Internet in 1998.
- These algorithms are not very strong however network providers can use stronger algorithms.
- Algorithm A3 and A8 are located on the SIM and in the AuC.
- Algorithm A5 is implemented in the device.
- Hence algorithm A3 and A8 can differ but algorithm A5 is common for all service providers.

Authentication

- Before accessing any GSM service the user must be authenticated.
- Authentication is based on SIM that stores the individual **authentication key Ki, the user identification IMSI** and the **algorithm A3**.
- Authentication process uses challenge-response method.

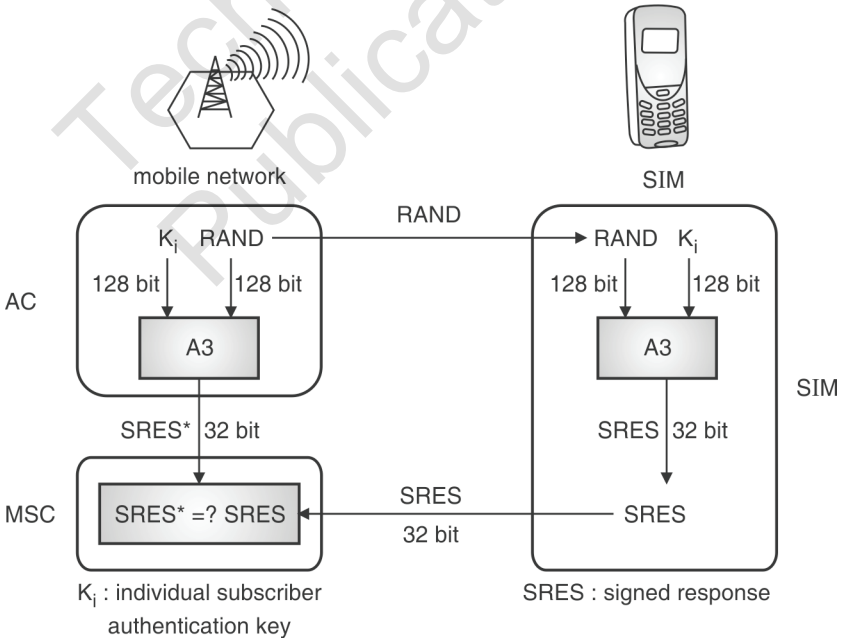


Fig. 2.1.12 : Authentication in GSM

- Steps involved in authentication process are illustrated in Fig. 2.1.12.

1. The access control (AC) generates a 128 bit random number RAND as challenge.
2. VLR sends this 128-bit random number (RAND) to the MS.

3. The MS computes the 32-bit signed response (SRES) based on the random number (RAND) with the authentication algorithm (A3) using the individual subscriber authentication key (Ki).
4. MS sends this SRES to the MSC.
5. Similarly, access control also calculates the signed response called SRES.
6. Now MSC compares the values of signed response received by AC and MS. If the values are same then the subscriber is accepted, otherwise subscriber is rejected.

Encryption

To ensure privacy, all messages containing user-related information are encrypted in GSM over the air interface.

- Once authentication is done, MS and BSS can initiate encryption.
- Steps involved in Encryption process are described in Fig. 2.1.13.

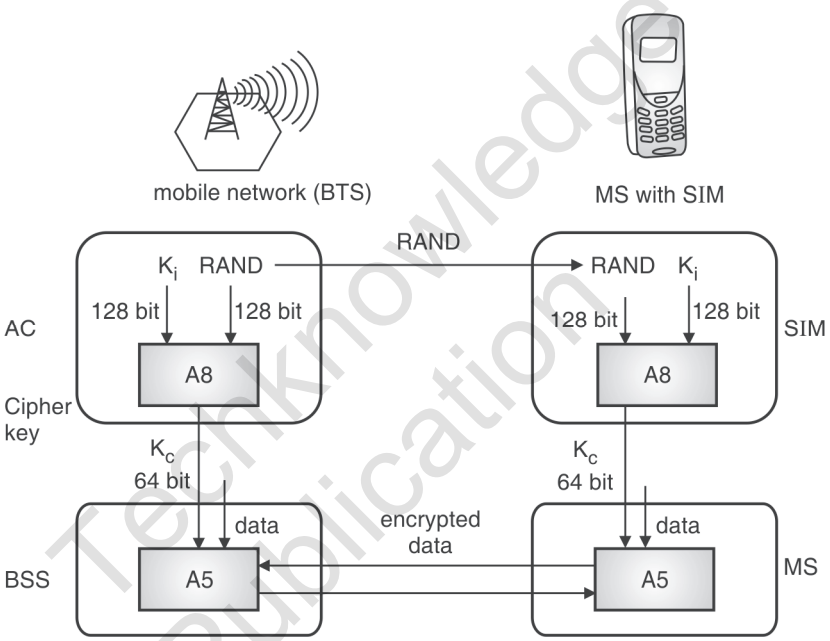


Fig. 2.1.13 : Data encryption in GSM

- The SIM and access control (AC) generate the 64 bit **cipher key Kc** by using the authentication key K_i and 128 bit random number RAND and applying algorithm A8.
- The MS and BTS can now encrypt and decrypt data using algorithm A5 and the cipher key K_c.
- The K_c which is 64 bit is not very strong but just enough to provide protection against simple eavesdropping.
- In certain implementations it so happen that 10 out of 64 bits are always set to 0, so that the real length of the key now is only 54. Hence the encryption is much weaker.

2.2 General Packet Radio System (GPRS)

MU - May 12, Dec. 12, Dec. 13, Dec. 14

Q. How much of the original GSM network does GPRS need? Which elements of the network perform the data transfer? **(May 12, 5 Marks)**

Q. Short note on GPRS. **(Dec. 12, 5 Marks)**

Q. Which components are new in GPRS as compared to GSM ? What is their purpose? **(Dec. 13, 10 Marks)**

Q. What are the modifications require to an existing GSM network to be upgraded to GPRS ? Explain with the help of diagram. **(Dec. 14, 10 Marks)**

- General Packet Radio System (GPRS) standard was defined by European Telecommunications standards Institute (ETSI).
- It is a major improvement and extension to the standard GSM system.
- GSM is a circuit-switched network which is ideal for the delivery of voice but not suitable for transmitting data that is bursty and asymmetric in nature.
- GPRS added packet-switched functionality to existing networks as a result the users of the system can be online, allowing to make voice calls and access internet on-the-go.
- GPRS uses unused time slots of GSM system to transmit packet data.
- GPRS can allocate one to eight time slots within a TDMA frame.
- Allocation of time slots is an on demand basis instead of fixed and predetermined. This allocation depends on current network load and the operator preference.
- Depending upon the coding, the transfer rate up to **171.2 kbits/s** is possible.
- GPRS operators offer a minimum of one time slot per cell to ensure at least minimum data rate.
- Charging in GPRS is based on the volume of data exchanged and not on the connection time.
- GPRS also includes several security services such as authentication, access control, confidentiality of user identity and user data.
- The available user data rate depends upon the coding scheme and the number of TDMA time slots allocated. Table 2.1.3 lists the data rates available in GPRS if it used with GSM.

Table 2.1.3 : GPRS data rates

Coding scheme	1 slot	2 slots	3 slots	4 slots	5 slots	6 slots	7 slots	8 slots
CS-1	9.05	18.1	27.15	36.2	45.25	54.3	63.35	72.4
CS-2	13.4	26.8	40.2	53.6	67	80.4	93.8	107.2
CS-3	15.6	31.2	46.8	62.4	78	93.6	109.2	124.8
CS-4	21.4	42.8	64.2	85.6	107	128.4	149.8	171.2

Key Features of GPRS

1. **Always online feature :** Since GPRS uses packet switched network, it removes the dial-up process. Users now can be online all the time.
2. **An upgrade to existing systems :** Operators do not have to replace their equipment; rather, GPRS is added on top of the existing infrastructure.
3. **Volume based charging :** In circuit switched services, billing is based on the duration of the connection. This is unsuitable for applications with bursty traffic. The user must pay for the entire airtime, even for idle periods when no packets are sent. With packet switched services, billing can be based on the amount of transmitted data. The advantage for the user is that he or she can be "online" over a long period of time.
4. **An integral part of future 3G systems :** GPRS is the packet data core network for 3G systems EDGE and WCDMA.

2.2.1 Architecture

MU - May 12, May 13, Dec. 13, Dec. 14, May 15, May 16, Dec. 16

Q.	Draw and explain architecture of GPRS network.	**(May 12, 5 Marks)**
Q.	Draw a neat diagram of GPRS system architecture and explain with different types of interfaces.	**(May 13, 10 Marks)**
Q.	Which components are new in GPRS as compared to GSM ? What is their purpose ?	**(Dec. 13, 10 Marks)**
Q.	What are the modifications required by an existing GSM network to be upgraded to GPRS ? Explain with the help of diagram.	**(Dec. 14, May 16, Dec. 16, 10 Marks)**
Q.	Explain GPRS architecture in detail. Compare it with GSM architecture.	**(May 15, 10 Marks)**

Fig. 2.2.1 shows simplified GPRS network architecture. As stated earlier, GPRS is an extension to traditional GSM system.

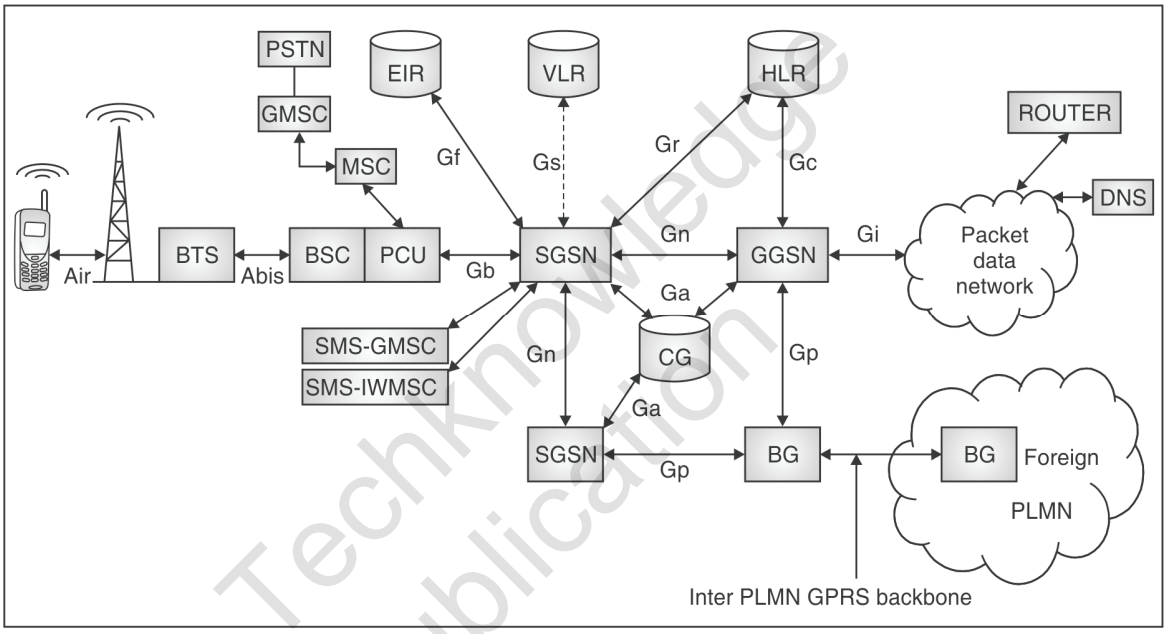


Fig. 2.2.1 : GPRS Network architecture

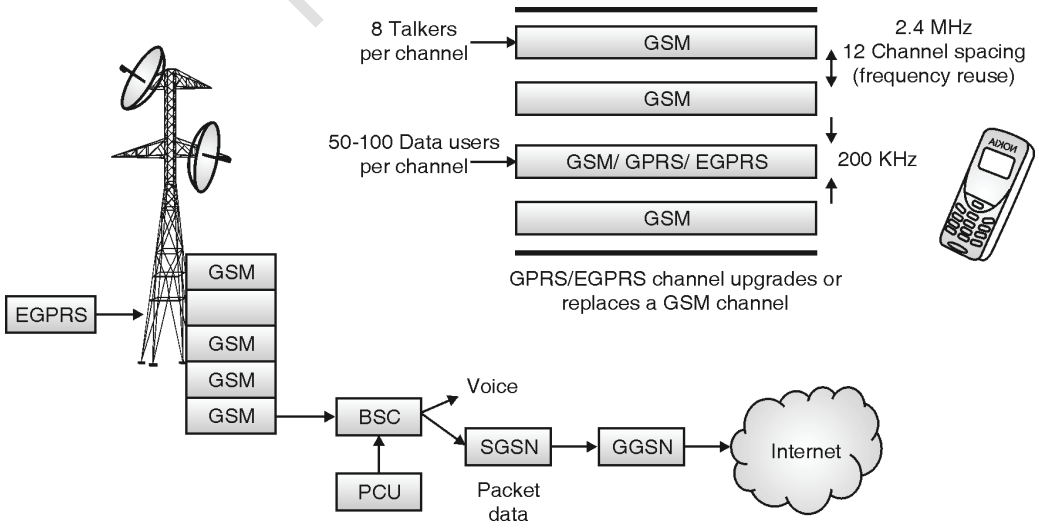


Fig. 2.2.2 : Upgrading GSM to GPRS Diagram

The following network nodes have been added to the existing GSM network to support packet switched network.

1. GPRS Support Nodes (GSNs)

- The most important network node added to the GSM network is GSN (GPRS Support Node).
- It is a network node which supports the use of GPRS in the GSM core network. All GSNs should have a *Gn* interface and support the GPRS tunneling protocol (GTP). There are two key variants of the GSN, namely serving and gateway GPRS support node.

2. Serving GPRS Support Node (SGSN)

- It is similar to MSC of GSM network. SGSN functions are listed below.
  - Performs data compression which helps to minimize the size of transmitted data units.
  - Performs authentication of GPRS subscribers and also maintains information of all the GPRS subscribers.
  - Such information contains the current cell, the current VLR and a subscriber's profile consisting IMSI number and the address used in packet network.
  - Determines the route of transmitted packets and transfer them to appropriate nodes.
  - Manages MS mobility as the subscriber moves from one PLMN area to another PLMN, and possibly one SGSN to another SGSN.
  - Maintains the statistics of traffic collections.

3. Gateway GPRS Support Node (GGSN)

- GGSN is the gateway to external networks such as PDN (Packet Data Network) or IP network. It is similar to GMSC of GSM network.
- It does two main functions.
  - Routes packet coming from external IP networks to the relevant SGSN within the GPRS network. Here it converts incoming packet to the GSM format and sends the processed packet to SGSN.
  - Routes packets originated from a GPRS user to the respective external IP network. Here it performs the conversion of the GPRS packet to the appropriate format of the Packet data protocol (PDP) depending upon the destination network.

4. Packet Control Unit (PCU)

- PCU is the core unit to segregate between GSM and GPRS traffic.
- It separates the circuit switched and packet switched traffic from the user and sends them to the GSM and GPRS networks respectively.
- In GPRS, PCU has following two paths.
  (i) PCU-MSC-GMSC-PSTN
  (ii) PCU-SGSN-GGSN-Internet (packet data network)

5. Border Gateway (BG)

- It acts as an interface between different operators of GPRS networks.
- The connection between two border gateways is called GPRS tunnel.
- It is more secure to transfer data between two operators using their own PLMN networks through a direct connection rather than via the public Internet which is less secure.
- For this both operators need to agree to provide such connectivity and terms and conditions including charging terms.

6. Charging Gateway (CG)

- Charging gateway is responsible for accounting and billing for the use of the network.
- Charging is done based on Quality of Service or plan user has opted.
- This charging data generated by all the SGSNs and GGSNs in the network is referred to as Charging Data Records (CDRs).
- The Charging Gateway (CG) collects all of these CDRs, processes the same and passes it on to the Billing System.

7. DNS server

It converts domain name to IP addresses required to establish internet connection and to deliver web pages on user's terminal screen.

8. PLMN

(i) Intra PLMN

An IP based network inter-connecting all the above mentioned GPRS network elements in one PLMN area.

(ii) Inter PLMN

Inter PLMN is a connection between two different PLMN areas.

9. HLR Register

HLR stores information and the user profile of all GPRS subscribers. The data includes the current SGSN and PDP addresses. These data are updated each time a user registers with a new SGSN.

10. SMS-GMSC and SMS-IWMSC

- The GPRS system allows SMS messages to be sent as well. For that data exchange between SMS-GMSC and
- SMS-IWMSC blocks and the appropriate SGSN takes place.

11. GPRS Interfaces

Different interfaces have been defined between different network components of the GPRS. Some new interfaces to GSM have been added in GPRS to support packet switched data mainly between GGSNs, SGSNs and other network components. The following interfaces have been defined.

(i) Um interface : Between MS and BTS there is an **Um** interface which is very similar to GSM and defines the modulation type, error correction/detection technique, power control information etc.

(ii) A interface : BTS and BSC communicates via A interface and defines the channel allocation, power measurement information etc.

(iii) Gb interface : It connects BSCs to SGSN.

(iv) Gn interface : Gn interface exist between GSNs of same PLMN. It is used to exchange user profile when the user moves from one SGSN to another.

(v) Gp interface : Two GSNs of different PLMN communicate via Gp interface**.** It is used for exchanging the user profile and other signaling information between a SGSN and GGSN of another area.

(vi) Gf interface : It is used between SGSN and EIR. It is used to query the IMEI information if an MS tries to register with the network.

(vii) Gr interface : SGSN and HLR communicate via **Gr** interface. It is used to get the user profile, the current SGSN address and the PDP address(es) for each user in PLMN.

(viii) Gc interface : Between GGSN and HLR there is **Gc** interface. It is used by GGSN to query user's location and profile to update its location register.

(ix) Gi interface : Connects GGSN to external PDN.

(x) Gs interface : Between SGSN and MSC/VLR is used to perform paging request of circuit switched GSM call for combined attachment procedure.

(xi) Gd interface : Between SMS-Gateway (SMS-GMSC) and SGSN is used to exchange short message service (SMS) messages.

(xii) GPRS Tunneling protocol (GTP) : All GSNs forming a GPRS backbone network are connected over IP. Within this backbone the GSNs encapsulate and transmit PDN packets by using GPRS Tunneling Protocol (GTP).

2.2.2 GPRS Protocol Stack

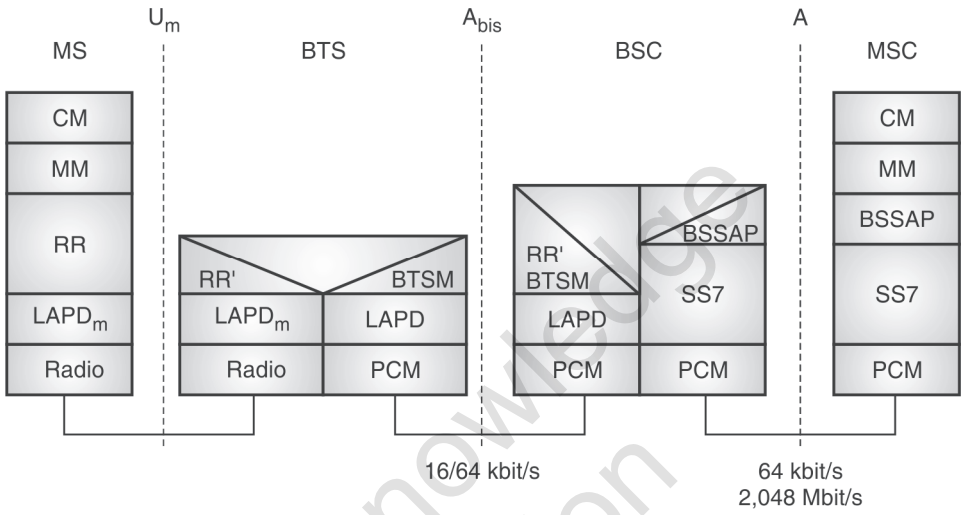


Fig. 2.2.3 : GPRS protocol architecture

The following various protocols are involved in GPRS :

1. **GPRS tunneling protocol (GTP)**

   It is responsible for all the data transfer between GSNs.

2. **TCP/UDP**

- Depending on the requirement, GTP can use either TCP or UDP as the transport layer protocol.
- UDP is used in case non-reliable data transfer is required (IP packet transfer).
- TCP is used in case reliable data transfer is required (X.25 packet transfer).

3. **Subnetwork dependent convergence protocol (SNDCP)**

- It is used between the SGSN and the MS to adapt to the characteristics of the underlying networks.
- User data packet is tunneled between the MS and the GGSN on top of SNDCP and GTP.

4. **Logical link control**

- It is used to provide reliable data transfer between the MS and the SGSN.
- It comprises ARQ and FEC mechanism for PTP (Point-To-Point) services.

5. **Base station subsystem GPRS protocol (BSSGP)**

- This protocol is used to convey routing and QoS-related information between the BSS and SGSN.
- It works on the top of a frame relay (FR).

6. **Radio link protocol (RLC)**

   It is responsible for providing a reliable link between the MS and the BSS.

7. Medium access control (MAC)

- It is responsible for controlling the medium access and the signaling procedure for the radio channel.
- Performs mapping of the LLC frames onto the GSM physical channels.

2.2.3 Comparison of GPRS Architecture with GSM Architecture

- The existing GSM nodes are upgraded with GPRS functionality.
- The GSM network only provides circuit switched services and thus two new network nodes GSN (GPRS Support Nodes) nodes were defined to support packet switched services. They are GGSN and SGSN.
- GPRS uses GSM's BSS but with enhanced functionality to support GPRS. The GSMs BSS now is used for both circuit switched and packet switched network elements to ensure backward compatibility.
- Additional PCU (Packet control Unit) unit has been added to BSC to segregate voice and data packets.
- Circuit switched data are sent to **A** interface on the MSC and packet switched data are sent to the SGSN into the GPRS backbone.
- The BSC of GSM is given new functionality for mobility management for handling GPRS paging. The new traffic and signaling interface form the SGSN is now terminated in the BSC.
- GPRS uses the MSC/VLR interface provided by GSM, between the MSC and SGSN coordinated signaling for mobile stations which have both circuit switched and packet switched capabilities.
- The HLR of GSM is modified to contain GPRS subscription data and routing information and is accessible from the SGSN. It also maps each subscriber to one or more GGSNs. The HLR may be in a different PLMN than the current SGSN for roaming terminals

Advantages of GPRS

- Very flexible.
- Suitable for bursty Internet traffic and fully packet oriented.
- Better quality of data services measured in terms of reliability, response time.
- No connection is required to be set up prior to data transfer.
- All GPRS services can be used in parallel to the conventional GSM services.
- Users of GPRS benefit from shorter access times and higher data rates.
- GPRS packet transmission offers a more user friendly billing than that offered by circuit switched services.

Disadvantages of GPRS

- The real available data rate depends on the current load of the cell as GPRS only uses idle time slots.
- Additional network elements are required to implement GPRS.
- GPRS exhibits a large jitter as compared to fixed networks.

Application of GPRS

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

7. **SMS :** It is also possible to send SMS messages over GPRS.
8. **Supplementary services :** GPRS also offers supplementary services, such as call forwarding and closed user group (CUG).

2.3 UMTS Terrestrial Radio Active Network (UTRAN)

2.3.1 UMTS (Universal Mobile Telecommunication System) Core Network

- Universal Mobile Telecommunication System (UMTS) is the European proposal for IMT-2000 prepared by ETSI.
- The UMTS specifically defines new radio interface called UMTS Terrestrial Radio Interface (UTRA).
- Two radio interfaces have been defined: UTRA-FDD and UTRA-TDD.
- UMTS does not define a complete new 3G system rather it specifies a smooth transition from second generation GSM or TDMA systems to the third generation.
- Many solutions have been proposed for 3G networks.
- One initial enhancement of GSM towards UMTS was Enhanced Data rates for Global Evolution (EDGE) which uses enhanced modulation techniques.

UMTS services

UMTS should provide following services as a 3G network :

1. Provide various bearer services.
2. Support real-time and non real-time services.
3. Support Circuit switched and packet switched transmission.
4. Handover should possible between UMTS cells, but also between other non-UMTS systems such as GSM or satellite networks.
5. The system should be compatible with GSM, ATM, IP and ISDN-based networks.
6. Should provide variable data rates for uplink and down link.

2.3.2 UMTS System Architecture

MU - May 12, May 15

Q.	Write a short note on UMTS architecture and its domain.	**(May 12, 5 Marks)**
Q.	Explain UMTS architecture.	**(May 15, 5 Marks)**

- Fig. 2.3.1 shows the simplified UMTS reference architecture.

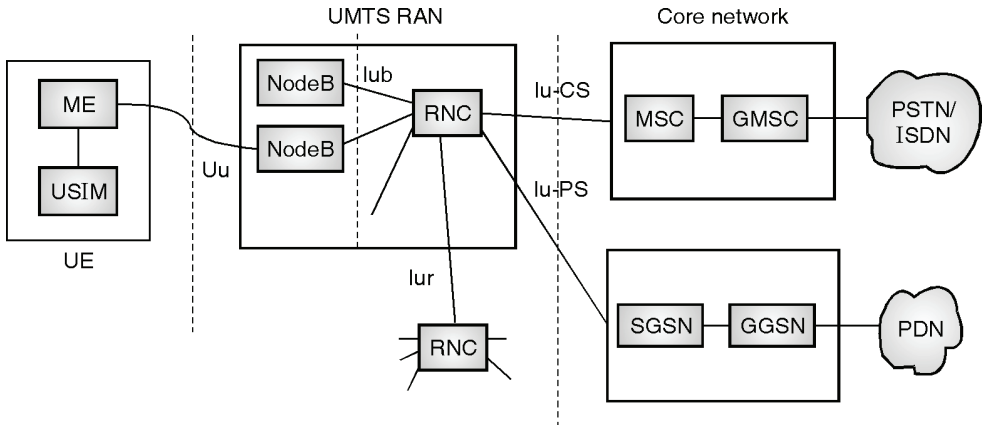


Fig. 2.3.1 : Main components of the UMTS reference architecture

Three main components of UMTS are :

1. The UTRA network (UTRAN)
2. Core Network (CN)
3. User Equipment (UE)

1. UTRAN

- The UMTS Terrestrial network (UTRAN) handles the cell level mobility and comprises several radio network subsystems (RNS).
- RNS consists of two main components: RNC(Radio Network Controller) and Node B.
- Node B is similar to the base station in GSM system, which performs physical layer processing such as channel coding, modulation, data interleaving etc.
- RNC controls one or more Node Bs. It manages radio resources assigned to them. Thus it performs data link layer processing and also participates in handover process.
- RNC is connected to MSC and SGSN to route circuit switched and packet switched data.
- In general the functions of RNS includes :
  - Radio channel ciphering and deciphering
  - Handover control
  - Radio resource management
  - Admission control
  - Congestion control
  - System information broadcasting
  - Radio network configuration etc.
- UTRAN is connected to Users Equipment via the radio interface Uu. Uu interface is comparable to Um interface in GSM.
- UTRAN communicates with the Core Network (CN) via Iu interface which is similar to the A interface in GSM.

(i) Core Network (CN)

- Core network is shared with GSM and GPRS.
- It contains components such as HLR, VLR, MSC , GMSC , SGSN and GGSN.
- Core network contains functions for inter-system handover, gateways to other networks, and performs location management.

(ii) User Equipment (UE)

- The user equipment (UE) contains two components: Mobile equipment (ME) and UMTS subscriber Identity Module (USIM).
- ME is the radio terminal connecting to the radio interface using Uu interface.
- USIM is a smart card similar to SIM in GSM system that contains the subscriber identity, authentication algorithms, encryption keys etc.
- UMTS further subdivides the above architecture into two domains as shown in Fig. 2.3.2.

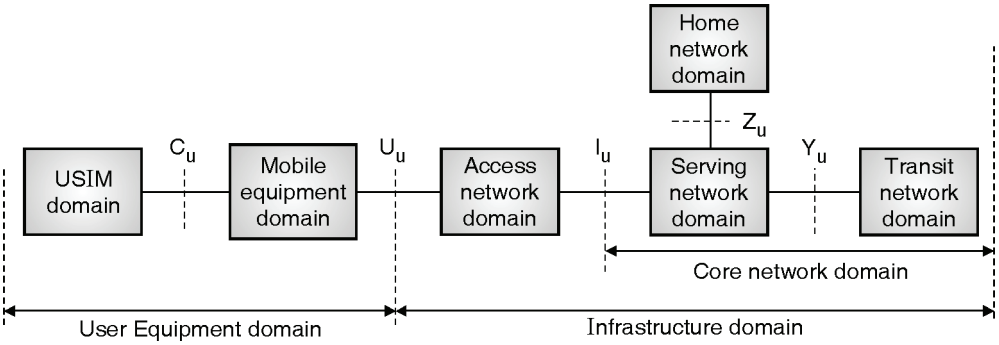


Fig. 2.3.2 : UMTS domain and interfaces

The user equipment domain

- The user equipment domain is assigned to a single user and comprises all the components needed to access UMTS services.
- The end device itself is in a mobile equipment domain. All functions for radio transmission as well as user interfaces are located here.
- This domain is further divided into two sub domains: The **USIM domain** and **mobile equipment domain**.
- The USIM domain contains the SIM for UMTS and stores all the necessary user related data. It also performs functions for encryption and authentication of users.

The infrastructure domain

- The infrastructure domain is shared among all the users.
- It offers UMTS services to all the subscribed users.
- It is further divided into two sub domains. The **access networks domain** and the **core network domain.**
- Access network domain contains the radio access networks (RAN) and provides radio access to the UMTS users.
- Core network domain contains functions that are independent of access network.
- The core network domain can be separated into three domains with specific tasks.
  - The serving network domain
  - The home network domain
  - The transit network domain
- The **serving network domain** comprises all functions currently used by a user for accessing UMTS services.
- The **Home network domain** contains all functions related to the home network of a user for example, user data look-up, user profile.
- If the serving network cannot directly contact the home network then **transit network domain** may be used.

UMTS radio interface

- The UMTS defines a new radio interface *Uu* between the user equipment and the UTRA network.
- The UMTS uses direct sequence (DS) CDMA technology.
- In DS-CDMA each user is separated using a special code called chipping sequence.
- It multiplies a stream of bits with a chipping sequence to spreads the signal.
- To separate different users the codes the codes that are used for spreading should be orthogonal.
- All signals use the same frequency band. UMTS uses the constant chipping rate of 3.84 Mchips/s.
- Different data rates can be achieved by using different spreading factors. Spreading factor is defined as the number of chips per bit.

- Fig. 2.3.3 shows basic idea of spreading and separation of user data using orthogonal spreading codes.
- The first step is spreading the user data using orthogonal spreading codes.

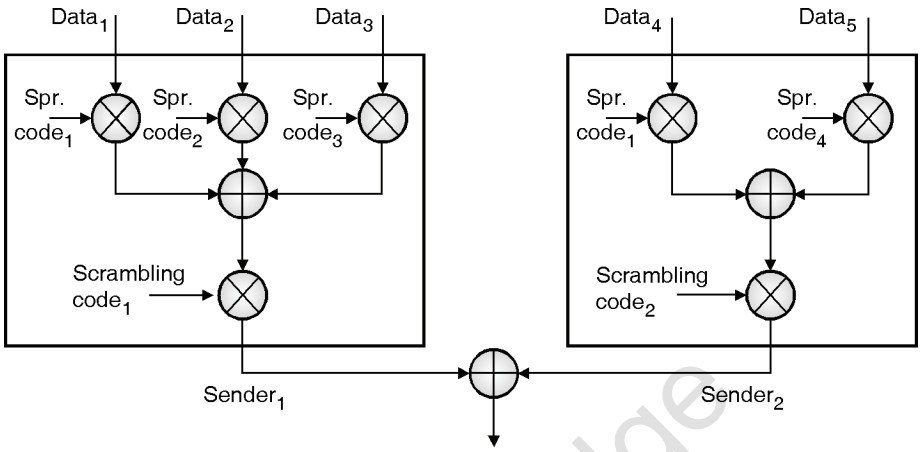


Fig. 2.3.3 : Spreading and scrambling of user data

- UMTS uses orthogonal variable spreading factor (OVSF) codes.

Working of OVSF

- Orthogonal codes are generated by doubling a chipping sequence X with and without flipping the sign of the chip.
- For example if a chipping sequence is X the next set of orthogonal codes would be (X,X) and (X,-X) as shown in Fig. 2.3.4 (a).

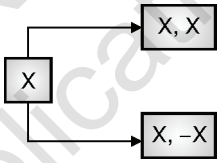


Fig. 2.3.4 (a) : Generation of orthogonal codes

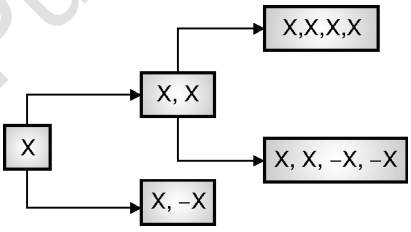


Fig. 2.3.4 (b) : Generation of orthogonal codes

- Now chipping sequence XX is doubled without flipping the signs and with flipping the signs. We get two more sets (X,X,X,X) and (X,X,-X,-X) (Fig. 2.3.4 (b)).
- The whole process of generating OVSF codes is shown in Fig. 2.3.5 assuming the starting chipping sequence as 1.

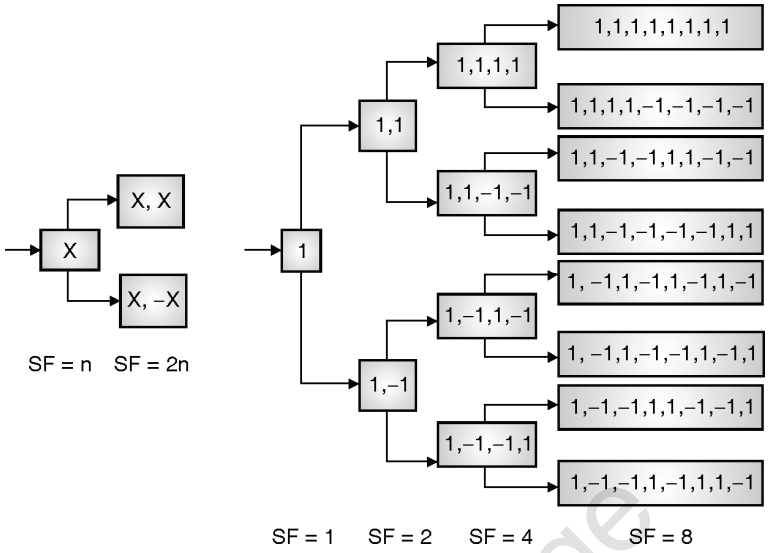


Fig. 2.3.5 : OVSF code tree used for orthogonal spreading

- Doubling the chipping sequence also results in spreading the bit twice as much as before. The spreading factor SF=n becomes SF=2n.
- Two codes are orthogonal as long as one code is not the part of another code. Thus orthogonality can be guaranteed if one code is not generated from the other code.
- Thus if a sender uses the code (1,–1) with spreading factor as 2, it is not allowed to use any of the codes located in the sub tree generated out of (1,–1).

Supporting different data rates

- UMTS uses constant chipping rate of 3.84Mchip/s.
- Different data rates are achieved by varying spreading factor.
- If the chipping rate is constant and if we double the spreading factor this will result in spreading the bit twice as much as before. Thus, it divides the data rate by two.
- Thus, by using different spreading factors we can achieve different data rates.

Spreading and scrambling of user data

- As shown in Fig. 2.3.3 each user spreads its data stream using OVSF code. After spreading, all chip streams are summed up and scrambled. Scrambling is nothing but XORing chips based on a code.
- In the FDD mode, the scrambling code is unique for each sender. Thus, here scrambling code is used to separates all senders in a cell.
- After scrambling the signals of different senders are quazi-orthogonals.
- For TDD the scrambling code is cell specific i.e. all the stations in a cell use the same scrambling code.
- The scrambled chips are then modulated using QPSK and then transmitted.

2.3.2(a) UTRA – FDD (W-CDMA)

MU - May 13, May 15

Q. Explain UTRA FDD in detail. **(May 13, May 15, 5 Marks)**

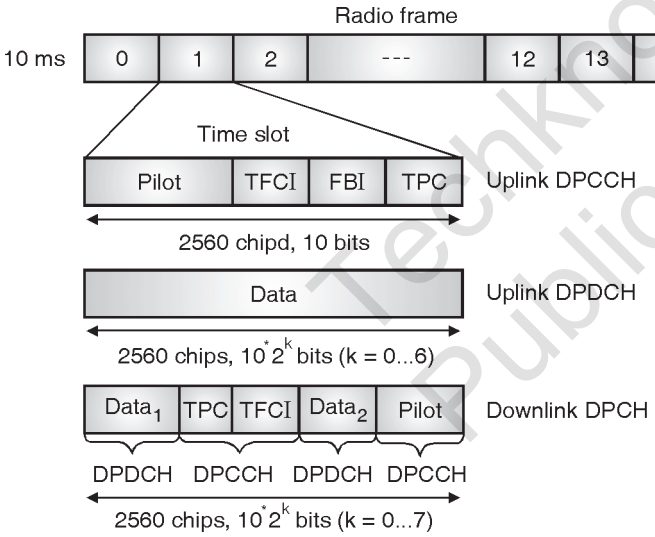
- The FDD mode for UTRA uses wideband CDMA (W-CDMA) with direct sequence spreading.
- In FDD, uplink and downlink uses different frequencies.

Features of W-CDMA

- 1920-1980 MHz uplink
- 2110-2170 MHz downlink
- Uses constant chipping rate of **3.840** Mchip/s
- Provides soft handover
- Uses QPSK for modulation
- Requires complex power control (1500 power control cycles/s)
- Spreading : Up Link : 4-256;Down Link:4-512

UTRA-FDD Frame structure

- Fig. 2.3.6 shows UTRA-FDD frame structure.
- A radio frame contains 15 time slots. The duration of each frame is 10 msec.
- A radio frame consists of 38,400 chips.
- Each time slot is of 666.6 μs and consists of 2,560 chips.
- Each W-CDMA channel occupies 4.4 to 5 MHz bandwidth.
- Time slots in W-CDMA are not used for user separation but to support periodic functions. In contrast to GSM where time slots are used to separate users.



FBI : Feedback Information
TPC : Transmit Power Control
TFCI : Transport Format Combination Indicator
DPCCH : Dedicated Physical Control Channel
DPDCH : Dedicated Physical Data Channel
DPCH : Dedicated Physical Channel

Fig. 2.3.6 : UTRA –FDD (W-CDMA) frame structure

Similar to GSM, UMTS also defines many logical and physical channels and their mapping.

Physical Channels in UMTS

- UMTS supports three physical channels which are used for data transport.
  - Dedicated Physical Data Channel (DPDCH)
  - Dedicated Physical Control Channel (DPCCH)
  - Dedicated Physical Channel (DPCH)
- And additionally a Random Access Channel (RACH) to control the media access in uplink.

1. Dedicated Physical Data Channel (DPDCH)

- This channel is used for transferring user data and signaling data.
- The spreading factor of this channel can vary between 4 and 256. This directly supports different data rates.
- Table 2.3.1 describes different spreading factors and corresponding data rate supported by DPDCH.

Table 2.3.1 : Spreading and corresponding data rates supported by DPDCH

Spreading factor	Data rate (kbits/s)
4	960
8	480
16	240
32	120
64	60
128	30
256	15

- Thus, maximum data rate supported is 960 kbit/s with spreading factor 4.
- The problem of using OSVF is that only certain multiplies of the basic data rate (i.e. 15 kbit/s) can be used. For example, 250 kbit/s data rate is required then the device has to choose 480 kbit/s, which wastes the bandwidth.
- In each connection in layer1, it can have between zero and six DPDCHs. This results in a theoretical maximum data rate of 5,740 kbit/s ($960 \times 6 = 5{,}740$).
- Table 2.3.2 shows typical user data rates together with the required data rates on the physical channel.

Table 2.3.2 : UTRA-FDD uplink data rates

User data rate [kbit/s]	12.2 (voice)	64	144	384
DPDCH	60	240	480	960
DPCCH	15	15	15	15
Spreading	64	16	8	4

2. Dedicated Physical Control Channel (DPCCH)

- In each connection, layer 1 needs exactly one DPCCH.
- This channel conveys control data for the physical layer.
- It uses constant spreading factor 256.
- The channel contains following four fields.

(i) Pilot : The pilot is used for channel estimation.

(ii) Transport format combination identifier (TFCI) : TFCI specifies the channel transported within the DPDCHs.

(iii) Feedback information field (FBI) : It supports signaling for a soft handover.

(iv) Transmit power control (TPC) : TPC is used for controlling the transmission power of a sender. Power control is performed in each slot, thus 1500 power control cycles are available per second. Tight power control is necessary to mitigate near-far-effects. Six different DPCCH bursts have been defined which differ in the size of the fields.

3. Dedicated Physical Channel (DPCH)

- This is downlink channel.
- It multiplexes control and user data.
- Spreading factors between 4 to 512 are available. The available data rates for data channels (DPDCH) within a DPCH are 6 (spreading factor = 512), 24, 51, 90, 210, 432, 912 and 1872 (spreading factor =4).

4. Physical Random Access Channel (RACH)

- It is used to control medium access on the uplink. UTRA –FDD defines 15 random access slots within 20ms.
- Within each access slot 16 different access preambles can be used for random access.
- Using slotted Aloha, User Equipment (UE) can access an access slot by sending a preamble.
- UE starts with the lowest available power to avoid interfering with other stations. If no positive response is received then UE tries for another slot with another preamble with the next higher power level. This is called power ramping.
- The number of available slots can be defined per cell and is transmitted via a broadcast channel to all Users.

Steps for searching a cell

A UE has to perform following steps during the search for a cell after a power on.

1. Primary synchronization

A UE has to synchronize with the help of a 256 chip primary synchronization code. This code is same for all the cells and helps to synchronize with the time slot structure.

2. Secondary synchronization

During this second phase, the UE receives a secondary synchronization code which defines a group of scrambling codes used in this cell. The UE is now synchronized with the frame structure.

3. Identification of the scrambling code

The UE tries all scrambling codes within the group of codes to find the right code with the help of a correlator.

2.3.2(b) UTRA - TDD (TD-CDMA)

MU - May 13, May 15

Q. Explain UTRA TDD mode in detail. **(May 13, May 15, 5 Marks)**

Features of UTRA-TDD

- UTRA-TDD separates up link and down link in time domain. The Frame structure of TDD is similar to FDD.
- 15 slots with 2,560 chips per slot form a radio frame with duration of 10ms. The chipping rate is also 3.84 Mchip/s.
- The TDD frame structure can be **symmetrical** or a**symmetrical**.
- In symmetrical frame structure number of uplink and downlink slots is same.
- In asymmetrical frame structure any arbitrary combination is used.
- The system can change spreading factor between 1 to 16 to achieve desired data rate.
- Thus using the traffic burst shown in Fig. 2.3.7 data rates of 6624, 3312, 1656, 828 and 414 kbit/s can be achieved for spreading factors 1,2,4,6,8, and 16 respectively.
- Power control is easy due to tight synchronization and use of orthogonal codes. A simple power control scheme with 100-800 power control cycles/s is sufficient.

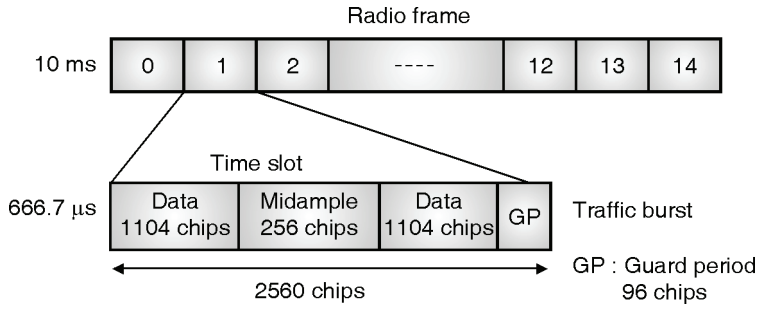


Fig. 2.3.7 : UTRA – TDD (TD- CDMA) frame structure

UTRA - TDD Frame format

- UTRA- TDD frame structure is shown in Fig. 2.3.7.
- It includes following bursts.

Data Fields

- Fig. 2.3.7 shows a burst of type2 which comprises two **data** fields each of 1,104 chips.
- Spreading is applied to these data fields only.

Midample

- Midample is used for training and channel estimation.

Guard period (GP)

- As TDD uses the same scrambling codes for all stations; the stations must be tightly synchronized and the spreading codes are available only once per slot.
- To loosen the tight synchronization little bit, a guard period has been introduced at the end of each slot.

Table 2.3.3 : Comparison of UTRA-FDD and UTRA-TDD

Parameter	UTRA-FDD	UTRA-TDD
Idea	Uses wideband CDMA (W-CDMA) with direct sequence spreading.	Uses Time domain CDMA
Separation of channels	Separates up and downlink in frequency domain	Separates up and down link in time domain.
Synchronization	Synchronization is not required in time domain	Tight synchronization is needed in time domain.
Power control	Complex power control scheme required. (1500 power control cycles/s)	Simple power control scheme is sufficient. (100-800 power control cycles/s)
Spreading	Spreading : Up Link : 4-256; Down Link :4-512	Spreading between 1-16
Maximum Data rate	960 kbit/s	6624 kbit/s
Scrambling code	Each station within a cell uses the different scrambling code.	All the stations in a cell use the same scrambling code.

2.3.3 Improvement on Core Network

- The activities of 3G developments have always focused on development of physical and MAC layers.
- The following three radio modules were selected for 3G radio access.
  (i) Direct sequence (DS) frequency division duplex(FDD)
  (ii) Multi carrier (MC) frequency division duplex (FDD)
  (iii) Time division duplex (TDD)
- The DS mode is based on the W-CDMA proposal and the MC mode is based on cdma2000 proposal. The TDD mode is basically suitable for cordless communications.
- Three major modules of core network for 3G system have been identified :
  (i) ANSI-41
  (ii) GSM MAP
  (iii) and IP-based network
- All the radio access modes of UTRAN should fully support ANSI 41 and GSM MAP.
- An operator may select one or more radio modules together with one or more core network modules to implement 3G system.
- Moreover, network related procedures are optimized to reduce signaling traffic in 3G.
- An additional improvement to the Core Network in UTRAN was addition of a new entity GLR (Gateway Location Register) between HLR and VLR.
- From the view point of VLR located in visited network, GLR is treated as roaming user's HLR in home network.
- From the view point of HLR in home network, the GLR acts as the VLR at the visited network.

Review Questions

Q. 1 Explain mobile terminated and mobile originated call in GSM.

Q. 2 Explain various security services offered by GSM.

Q. 3 Explain how the location update occurs in GSM.

❑❑❑

Mobile Networking

Syllabus

3.1 Mobile Networking : Medium Access Protocol, Internet Protocol and Transport layer

3.2 Medium Access Control : Motivation for specialized MAC, Introduction to multiple Access techniques (MACA)

3.3 Mobile IP: IP Packet Delivery, Agent Advertisement and Discovery, Registration, Tunneling and Encapsulation, Reverse Tunneling, Routing (DSDV,DSR)

3.4 Mobile TCP : Traditional TCP, Classical TCP Improvements like Indirect TCP, Snooping TCP & Mobile TCP, Fast Retransmit/ Fast Recovery, Transmission/Timeout Freezing, Selective Retransmission.

Introduction

With the rapid usage of portable devices, mobility has become an important factor in the success of mobile networks. Existing network protocols that are developed for fixed network do not work well if used directly in wireless networks. This is because the wireless networks impose various challenges like dynamic topology, asymmetric links, frequent disconnections, security, high error rate etc. To support mobility, either new protocols have to be developed or existing protocols need to be modified. This chapter discusses problems with some of the existing MAC, Internet and TCP layer protocol and required modifications to support mobility.

3.1 Mobile Networking

- Now a day, people want to access the services from anywhere, anytime irrespective of their location. This feature of moving anywhere and still be able to access the services is called mobility.
- Making such services mobile, requires modification to existing protocols and at some extent to existing architecture. The following section discusses the improvements or modifications need to be done in Media Access Control, Internet and Transport layer protocols to make a network or services mobile.

3.1.1 Medium Access Protocols

- Medium access protocols basically controls access to the shared medium.
- We know many of the MAC protocols for wired (or fixed) network such as ALOHA, Slotted ALOHA, CSMA, CSMA/CD, Token bus, token ring etc. Since wireless medium is a shared medium MAC protocols become an important design decision for wireless network.
- But all this MAC protocols from wired networks cannot be directly used for wireless networks. Here, we have introduced several **Medium Access Control (MAC)** algorithms which are specifically adapted to the wireless domain.
- Medium access control comprises all mechanisms that regulate user access to a medium using SDM, TDM, FDM, or CDM. MAC is thus similar to traffic regulations in the multiplexing.
- In this chapter we will discuss various MAC protocols specially designed for wireless networks.

3.1.2 Internet Protocols

- In traditional IP routing, IP addresses represent a topology. Routing mechanisms rely on the assumption that each network node will always have the same point of attachment to the Internet. Each node's IP address identifies the network link where it is connected.

- The Internet routers look at the IP address prefix, which identifies a device's network.
- At the network level, routers look at the next few bits to identify the appropriate subnet. Finally, at the subnet level, routers look at the bits identifying a particular device.
- In this routing scheme, if you disconnect a mobile device from the Internet and want to reconnect through a different subnet, you have to configure the device with a new IP address, and the appropriate netmask and default router. Otherwise, routing protocols have no means of delivering packets. This is because the device's IP address doesn't contain the necessary information about the current point of attachment to the Internet.
- The necessity for uninterrupted communication when the mobile device moves from one location to another calls for a new technology.
- This kind of communication can be efficiently implemented using Mobile IP. **Mobile IP** (or MIP) is an IETF standard communications protocol that is designed to allow **mobile** device users to move from one network to another while maintaining a permanent **IP** address.
- Section 3.3 discusses detail Mobile IP protocols and it's functionalities.

3.1.3 Transport Protocols

- Transmission control Protocol (TCP) is typically designed for fixed network.
- If we use the same TCP over mobile network, the performance of the TCP degrades.
- Existing TCP can be modified to support mobility.
- Section 3.5 discusses working of existing TCP, problems with existing TCP if used in mobile network and some modifications to the existing TCP that can be used for mobile networks.

3.2 Medium Access Control

3.2.1 Motivation for Specialized MAC

MU – May 18

Q. Explain the need of specialized MAC in wireless communication. **(May 18, 10 Marks)**

- CSMA/CD is the most commonly used MAC protocol for wired network. The question is, can we use the same CSMA/CD for wireless networks to control the medium access without any modifications?
- Let us consider carrier sense multiple access with collision detection, (CSMA/CD) which works as follows.
- A sender senses the medium (a wire) to see if it is free. If the medium is busy, the sender waits until it is free. If the medium is free, the sender starts transmitting data and continues to listen into the medium. If the sender detects a collision while sending, it stops at once and sends a jamming signal.
- But this scheme fails in wireless networks. This is because, CSMA/CD is not really interested in collisions at the sender, but rather in those at the receiver. The signal should reach the receiver without collisions. But the sender is the one who detects the collisions.
- This is not a problem using a wire, as the same signal strength can be assumed all over the wire if the length of the wire stays within certain standardized limits. If a collision occurs somewhere in the wire, everybody will notice it.
- The situation is different in wireless networks. Two problems hidden terminal and exposed terminal problem occur in wireless network which are discussed on following sections.
- Collision detection is very difficult in wireless scenarios as the transmission power in the area of the transmitting antenna is several magnitudes higher than the receiving power. So, this very common MAC scheme from wired network fails in a wireless scenario.
- The following sections show scenarios where CSMA/CD scheme form fixed networks fail in case of wireless network.

3.2.1(a) Hidden Station Problem and Exposed Station Problem

MU – May 12, Dec. 12, Dec. 13, May 15, May 16, May 17, Dec. 17

Q.	What is Hidden and Exposed terminal problem? Discuss solutions to these problems.	**(May 12, Dec. 13, 10 Marks)**
Q.	What do you mean by Exposed terminal problem ?	**(Dec. 12, 5 Marks)**
Q.	What do you mean by Hidden terminal problem?	**(Dec. 12, May 16, 5 Marks)**
Q.	Explain hidden station and exposed station problems in WLAN.	**(May 15, May 16, 5 Marks)**
Q.	What is hidden and exposed terminal problems? Discuss solution to these problems.	**(May 17, 5 Marks)**
Q.	Why do hidden terminal and exposed terminal problems arise? How would you propose to solve it?	**(Dec. 17, 10 Marks)**

- Wireless medium is an open, shared, and broadcast medium. Multiple nodes may access the medium at the same time.
- Traditional LANs uses CSMA/CD mechanism to control media access. This scheme works for wired network but not for wireless.
- CSMA/CD fails in case of wireless networks due to the following reason.
- In the wired network the signal strength can be assumed to be same all over the wire if the length of the wire stays within certain standardized limits. If a collision occurs somewhere in the wire, each station will notice it. But the situation is different in a wireless LAN. Here, the strength of a signal decreases proportionally to the square of the distance to the sender.
- Due to this reason, MAC schemes for wired networks may fail when used for wireless networks.
- Following two scenarios show where conventional CSMA/CD fails when used in wireless networks.

1. Hidden Station (or Terminal) Problem

Consider the scenario with three mobile phones A, B and C as shown in Fig. 3.2.1

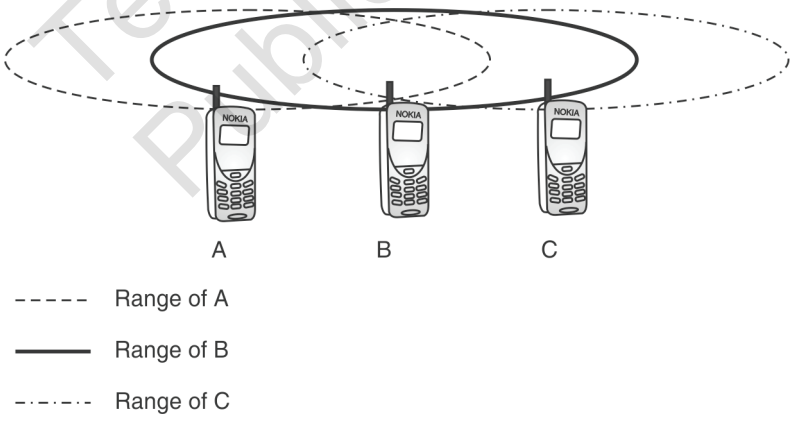


Fig. 3.2.1 : Hidden station problem

- The transmission range of A reaches B, but not C.
- The transmission range of C reaches B, but not A.
- Finally, the transmission range of A reaches both A and C. That is, A cannot detect C and vice versa.
  - (i) Initially, A senses the channel and since it finds the channel free, A transmits to B.
  - (ii) While A is transmitting, C also wants to transmit to B and hence senses the channel.
  - (iii) C does not hear A's transmission (because A is out of range of C).

(iv) C concludes that the channel is free and starts transmitting to B.

(v) Signals from A and C both collide at B.

(vi) "A" is hidden for "C".

2. Exposed Station Problem

Consider the situation shown in Fig. 3.2.2. Along with the previous situation now node D is added which is in the range of C.

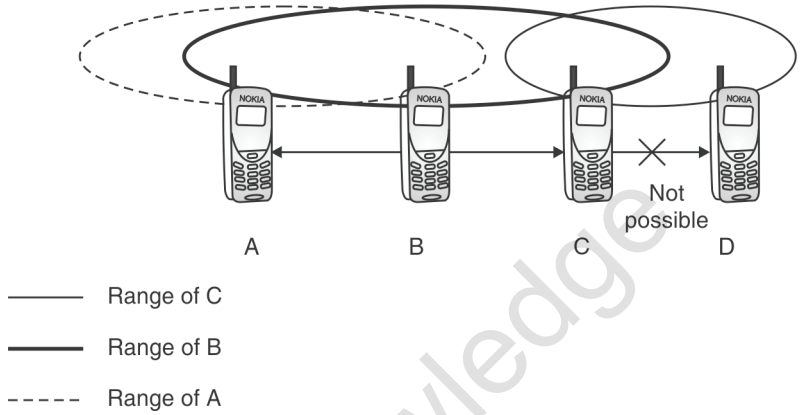


Fig. 3.2.2 : Exposed Station (or Terminal) Problem

(i) B wants to send data to A. B senses the channel and finds it free and hence transmits to A.

(ii) Now C also wants to talk to D.

(iii) C senses the channel and finds it to be busy (C can hear B's transmission since B is in C's range).

(iv) C concludes that the channel is busy and does not transmit (when it could have ideally transmitted to D because A is outside the radio range of C).

(v) "C" is exposed to "B".

The Hidden Terminal problem leads to :

(i) More collisions

(ii) Wastage of resources

On the other hand, Exposed Terminal problem leads to :

(i) Underutilization of channel

(ii) Lower effective throughput

3.2.2 Multiple Access with Collision Avoidance (MACA)

MU - May 16, May 17, Dec. 17

Q.	Explain in short how Hidden station problem is avoided in WLAN.	**(May 16, 5 Marks)**
Q.	What is hidden and exposed terminal problems? Discuss solution to these problems.	**(May 17, 5 Marks)**
Q.	Why do hidden terminal and exposed terminal problems arise? How would you propose to solve it?	**(Dec. 17, 10 Marks)**

- Hidden and exposed terminal problems can be solved by using multiple access with collision avoidance (MACA) protocol.
- We know that, "Absence of carrier does not always mean an idle medium" in the context of hidden terminal problem and "Presence of carrier does not always mean a busy medium" in the context of exposed terminal problem, MACA solves both the problems.

- MACA uses two short signaling packets called RTS and CTS for collision avoidance.
  - **(i) RTS (request to send) :** A sender requests the 'right to send' from a receiver by transmitting RTS packet before data transmission.
  - **(ii) CTS (clear to send) :** The receiver grants the 'right to send' as soon as it is ready to receive by sending back a CTS packet.
- These packets contain sender address, receiver address and length of future transmission.
- MACA solves Hidden Station Problem.

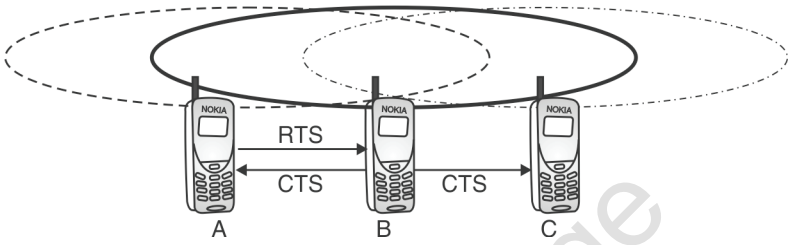


Fig. 3.2.3 : MACA solves Hidden station problem

- MACA avoids the problem of hidden stations. Consider the scenario shown in Fig. 3.2.3.
  1. A and C want to communicate to B.
  2. A sends RTS first.
  3. B receives RTS that contains name of the sender (A), receiver (B) and the length of future transmission. This RTS is not heard by C (Not in C's range).
  4. B responds to RTS by sending CTS. CTS packet contains the sender (A), the receiver (B) and the length of the future transmission. This CTS is received by both A and C (B is in range of both A and C).
  5. C waits after receiving CTS from B and is not allowed to transmit anything for the duration indicated in received CTS.
- Still there are chances of collision during the sending of an RTS. Both A and C could send an RTS at the same time that collides at B. An RTS packet is very small as compared to data packet, so the probability of a collision is much lower.

  In such cases, B resolves this contention and sends CTS to only one station.
- MACA Solves Exposed Terminal Problem
- MACA also avoids the problem of exposed terminals.

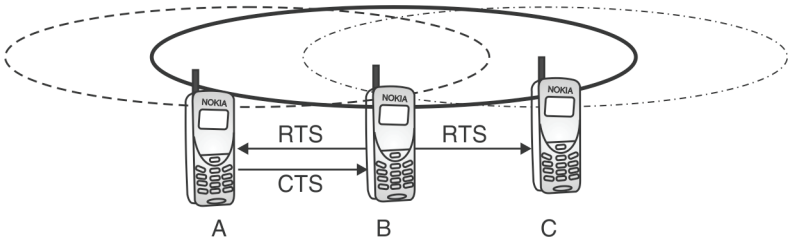


Fig. 3.2.4 : MACA solves exposed terminal problem

- Consider the scenario shown in Fig. 3.2.4.
  1. B wants to send data to A.
  2. C also wants to send data to someone else (Not to A and B)
  3. B sends RTS with sender as B, Receiver as A and length of the data packet. This RTS is received by both A and C.
  4. C does not react to this RTS as it is not the receiver.
  5. A responds to RTS by sending CTS.

6. This CTS is not received by C (A is not in C's range) and C concludes that A is outside the detection range.
7. C can now start its transmission assuming it will not cause a collision at A.

Drawbacks of MACA

1. One problem with MACA is the overheads associated with RTS and CTS transmission for short and time critical data packets.
2. MACA also assumes that the transmission links are symmetrical in both the uplink and the downlink directions. Otherwise a strong sender, directed antenna etc. could contract with the above scheme.

3.3 Mobile IP

3.3.1 Mobile IP : Basic Concept

- Mobile IP (or IP mobility) is a communication protocol developed by Internet Engineering Task Force (IETF) standard.
- In mobile IP, nodes continue to receive packets independent of their location which is achieved by modifying the standard IP in a certain way. It is designed such that mobile users can move from one network to another while maintaining a permanent IP address.

3.3.1(a) Need for Mobile IP

- To understand the need for Mobile IP, let us first understand the problem with the internet protocol (IP).
- In the standard IP, a host's IP address is made up of a network identifier and a host identifier. This network identifier specifies the network the host is attached to.
- A host sends an IP Packet with the header containing a destination address, made up of its network identifier and destination identifier.
- As long as the receiver remains connected to its original network, it can receive packets.
- Now suppose the receiver disconnects itself from its original network and joins another network, the receiver would never receive any packets. This is because, the IP address of the host is now topologically not correct in the new network.
- Hence, a host needs a so-called topologically correct address and Mobile IP standard was developed.

3.3.1(b) Goals/Requirements of Mobile IP

MU – Dec. 18

Q. What is the goal of Mobile IP? **(Dec. 18, 5 Marks)**

1. Flawless Device Mobility Using Existing Device Address

Mobile devices can continue to use their existing IP address even while changing their actual location or their original network.

2. No additional Addressing or Routing Requirements

- The same overall scheme for addressing and routing must be maintained as in regular IP. The owner of each device must assign IP addresses in the usual way.
- New routing requirements must not be placed on the internetwork, like host-specific routes.

3. Interoperability

Mobile IP devices can continue to communicate with other IP devices that have no idea about how Mobile IP works, and vice-versa.

4. Transparency of Layers

- All changes made by Mobile IP must remain confined to the network layer.
- Other layers like the transport layer and applications must be able to function in the same way as regular IPv4.

5. Restraining Hardware Changes

- A few changes are required to the routers that are used, by the mobile device and the mobile device software for Mobile IP.
- These changes must be kept to a minimum. Other devices, however, like routers between the ones on the home and visited networks, do not need changes.

6. Scalability

- Mobile IP must allow any device to change from one network to another network, and this must be supported for an arbitrary number of devices.
- The scope of the connection change must be global. For example, you can use your laptop from an office in London and also use it if you move to Mumbai.

7. Security

Mobile IP must include authentication procedures to prevent unauthorized devices from causing accessing the network and thereby causing problems.

3.3.1(c) Basic Terminology

MU – May 12, Dec. 16

Q. List the entities of mobile IP and describe data transfer from a mobile node to a fixed node and vice versa.

(May 12, Dec. 16, 10 Marks)

1. Mobile Node (MN)

An end-system or a router (node) that can change its point of connection to the network without changing its IP address.

2. Correspondent Node (CN)

It is the communication partner for the mobile node. The CN can be fixed or mobile.

3. Home Network (HN)

The home network is the subnet to which the MN belongs to with respect to its IP address.

4. Foreign Network (FN)

The foreign network is the current subnet the MN visits and which is not the home network.

5. Foreign Agent (FA)

- The FA is typically a router in the foreign network to which the mobile node is currently attached.
- The FA usually implements Mobile IP functions like providing security services to the MN during its visit to the FN and forwarding the datagrams received from the home agent to the MN.
- It also supports the sharing of mobility information so that Mobile IP operates smoothly.

6. Home Agent (HA)

- HA is a system in the home network of the MN.
- HA can be implemented on router that is responsible for the home network, or alternatively, it can be implemented on a node in a home subnet.
- HA maintains a location registry i.e. it is informed of the MN's location.
- The tunnel for packets towards the MN starts at the HA.

7. Care of Address (COA)

- The COA defines the current location of the MN.
- Packet delivery towards the MN is done using a tunnel.
- All IP Packets sent to the MN are delivered to the COA.

There are 2 different possibilities for the location of the COA.

(i) Foreign Agent COA

The COA could be the IP address of the FA. In this case, the tunnel endpoint is the FA. The FA forwards packets to the MN.

(ii) Co- located COA

If the MN acquires a temporary IP address to act as the COA, the COA is said to be co – located. This address is a topologically correct address and the MN's topologically correct IP address is now the tunnel endpoint.

- In Fig. 3.3.1, an example network is shown.
- A CN connects to the internet via a router. Another router implements the HA, thus connecting the home network and the internet.
- The foreign network's router acts as the FA. Currently, the MN is in the foreign network. The tunnel's start point is at HA and end point is at FA, for the packets directed towards the MN.

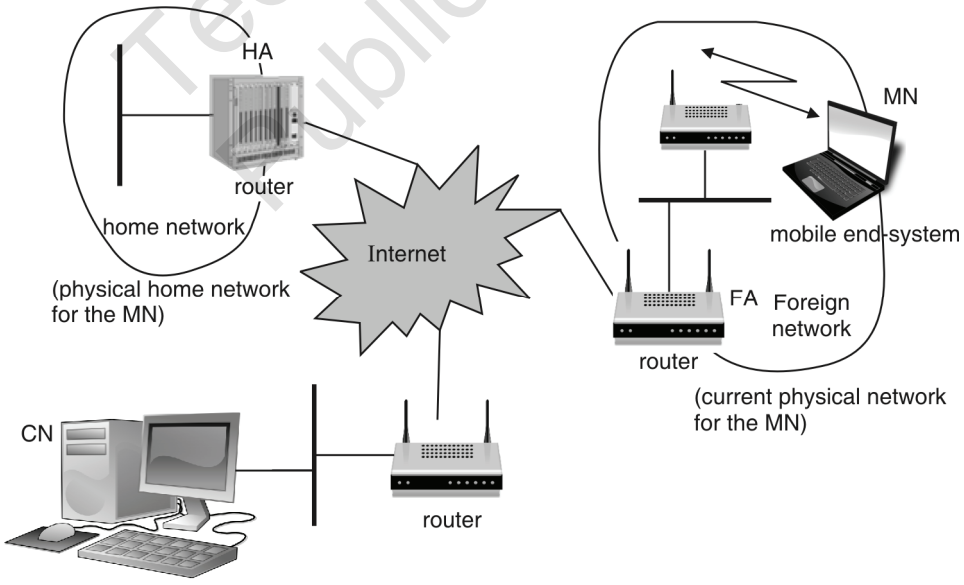


Fig. 3.3.1 : An example mobile IP network

Note : Tunnel for a packet sent to the MN always starts at HA and ends at either FA or MN depending upon the mode of COA. If the COA is foreign agent COA, then the tunnel ends at FA. If the COA is co-located, then the tunnel ends at MN.

3.3.2 IP Packet Delivery

MU – May 12, Dec. 13, Dec. 16, Dec. 18

Q.	List the entities of mobile IP and describe data transfer from a mobile node to a fixed node and vice versa.	**(May 12, Dec. 16, 10 Marks)**
Q.	Explain the IP Packet Delivery with respect to mobile IP.	**(Dec. 13, 5 Marks)**
Q.	How is packet delivery achieved to and from mobile node?	**(Dec. 18, 5 Marks)**

Consider data transmission between CN and MN. There are four scenarios.

1. CN is a fixed node and data is to be transferred from CN to MN.
2. CN is a fixed node and data is to be transferred from MN to CN.
3. CN is a mobile node and data is to be transferred from CN to MN.
4. CN is a mobile node and data is to be transferred from MN to CN.

Fig. 3.3.2 shows the packet delivery to and from MN.

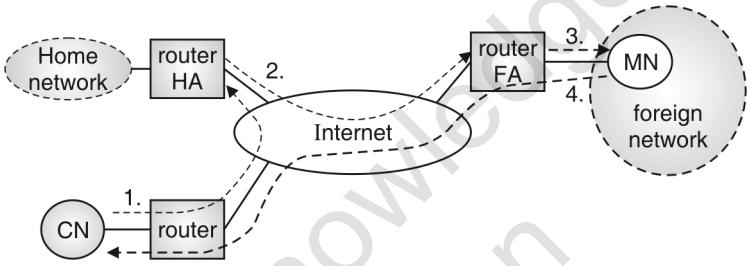


Fig. 3.3.2 : Packet delivery to and from the mobile node

(a) Data transfer from Fixed CN to MN

Step 1 : When the CN wants to send an IP packet to the MN, the CN doesn't know about the MN's current location and sends the packet to the IP address of MN. Here, the source address of the packet is CN's IP address and the destination address is MN's original IP address.

Step 2 : The packet is routed via the standard routing mechanism of the Internet to the router responsible for MN's home network. The home network's router implements the HA.

Step 3 : The HA now detects that the MN is currently not in its home network. Instead of forwarding the packet into the subnet as usual, the packet is encapsulated and is tunneled to the COA of the MN. A new header is added in front of the old IP header indicating MN's COA as the new destination and HA as the source of the encapsulated packet.

Step 4 : FA now decapsulates the packet and forwards the original packet with CN as source and MN as destination.

(b) Data transfer from MN to fixed CN

Step 1 : The packet is sent by the MN with its original IP address as the sender and the CN's IP address as the receiver.

Step 2 : The FA responsible for the foreign network acts as a default router and forwards the packet to the router responsible for the CN (The router is located in CN's home network).

Step 3 : The router responsible for CN then forwards the packet to CN.

(c) Data transfer from Mobile CN to the MN

Step 1 : The CN sends the packet with its original IP address as the source address and MN's original IP address as the destination address.

Step 2 : Since the CN is also in the visiting network, the FA responsible for the CN sends the packet to the router responsible for the home network of MN.

Step 3 : The HA of MN realizes that the MN is not in the home network. It then encapsulate the received packet and forwards it to the COA with source address as HA's IP address and the destination address as COA.

Step 4 : The foreign agent (FA) of the MN receives this packet, decapsulates it and forwards it to the MN.

(d) Data transfer from MN to a mobile CN

Step 1 : The MN sends the packet as usual with its own fixed IP address as a source address and CN's address as destination.

Step 2 : The foreign agent (FA) router responsible for MN sends this packet to the home network of the CN.

Step 3 : The HA responsible for CN receives the packet and realizes that the CN is not in the home network and hence tunnel the packet towards COA of the CN.

Step 4 : The FA responsible for CN receives the packet, decapsulates it and forwards it to the CN.

Some additional mechanisms are needed for mobile IP to work. The following section discusses about these enhancements.

3.3.3 Agent Advertisement and Discovery

MU - May 18

Q. Explain agent advertisement and discovery registration in mobile networks. **(May 18, 5 Marks)**

- When a mobile node is first turned on, it can either be in its home network or a foreign network.
- Hence, the first thing that it must do is to determine where it is, and if it is not at home, must begin the process of setting up datagram forwarding from its home network to the current location.
- This process is accomplished by communicating with a local router serving as an agent (FA), through the process called *agent discovery*.
- Agent discovery process makes it possible for an MN to determine :
  - Whether it is connected to its home network or to a foreign network.
  - Whether it has changed its position.
  - To obtain a COA when it changes to a different foreign network.

After moving to another network one initial problem is how to find a foreign agent. For this purpose, mobile IP describes two messages: ***Agent Advertisement*** and ***Agent Solicitation***.

3.3.3(a) Agent Advertisement

MU – Dec. 15, Dec. 17

Q. Explain Agent advertisement in Mobile IP. **(Dec. 15, 5 Marks)**

Q. How the agent could be discovered using Mobile IP? Give the overlay of agent advertisement packet which includes mobility extension. **(Dec. 17, 10 Marks)**

- How does a mobile node make out that it has changed network recently? This is achieved by messages from home agents and foreign agents.
- Home agents and foreign agents advertise their presence and services using messages called ***agent advertisement***.
- Agent advertisement messages are periodically broadcast and contain the following details
  - List of COAs available for the MN.
  - Special features and services provided by FA such as different types of encapsulation available. For example, minimal encapsulation or generic encapsulation.
  - Allows MN to detect the network number and congestion details of a link to the Internet.

- For agent advertisement ICMP messages with some mobility extension are used. The agent advertisement packet is shown in Fig. 3.3.3.

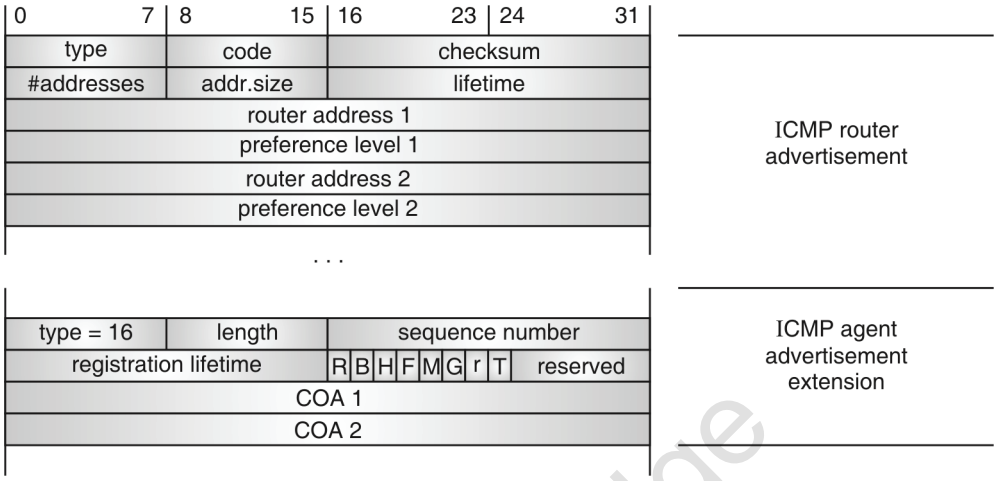


Fig. 3.3.3 : Agent advertisement message

- The various fields of ICMP part of the packet are :
  - **Type :** It is set to 9 for ICMP.
  - **Code :** Set to 0, if the agent also routes traffic from non-mobile node. And set to 16 if the agent only routes mobile traffic.
  - **#addresses :** Indicates the number of addresses advertised with this packet. The actual addresses follow as shown in Fig. 3.3.3.
  - **Lifetime :** Denotes the length of time for which the advertisement is valid
  - **Preference level :** Preference for each router address is specified. It helps a node to choose the router. The chosen router will act as an FA for the MN.
- The various fields of mobility extension part are :
  - **Type :** It is set to 16 for routing only mobile packets.
  - **Length :** Length depends on the number of COAs provided with the message and it is equal to 6 + 4 * (number of addresses).
  - **Sequence number :** It indicates the total number of advertisements set since initialization.
  - **Registration lifetime :** Specifies the maximum lifetime in seconds a node can request during registration.
- The following bits specify the characteristics of an agent :
  - **R bit :** It is the registration bit and indicates if a registration with this agent is required even when using co-located COA at the MN.
  - **B bit :** This bit is set if the agent is currently too busy to accept new registration.
  - **H bit :** This bit is set if the agent offers services as a home agent.
  - **F bit :** This bit is set if the agent offers services as foreign agent on the link where the advertisement has been sent.
  - **M and G bit :** M and G bits specify the method of encapsulation used for the tunnel. M for minimal encapsulation and G for generic routing encapsulation.
  - **r bit :** This is reserved and set to zero.
  - **T bit :** It indicates that reverse tunnelling is supported by the FA.

3.3.3(b) Agent Solicitation

MU – Dec. 15, Dec. 17

Q. Explain Agent advertisement in Mobile IP. **(Dec. 15, 5 Marks)**

Q. How the agent could be discovered using Mobile IP? Give the overlay of agent advertisement packet which includes mobility extension. **(Dec. 17, 10 Marks)**

- Agent solicitation messages are sent by MN itself to search an FA in one of the following conditions.
  - When no agent advertisements are present or
  - The inter-arrival time of advertisement message is too high or,
  - An MN has not received a COA by other means.
- To reduce the congestion on the link the MN can send out three solicitations, per second, as soon as it enters a new network.
- Any agent that receives the solicitation message, transmits a single agent advertisement in response. If a node does not receive an answer to its solicitations, it must decrease the rate of solicitations exponentially to avoid flooding the network.
- After these steps of advertisements and solicitations, the MN can now receive COA, either one for an FA or a co-located COA.
- Now the next step is, the MN has to register with the HA if the MN is in a foreign network.

3.3.4 Registration

MU – Dec. 13

Q. Explain registration with respect to mobile IP. **(Dec. 13, 5 Marks)**

- After agent discovery is done by a mobile node, it knows whether it is in its home network or in a foreign network. If it is in its home network, it communicates like a regular IP device, but if it has moved to a foreign network, it must activate Mobile IP.
- For activating Mobile IP, a process called home agent registration, or simply registration is used. For registration, the MN exchanges information and instructions with the home agent. The main purpose of registration is to get the Mobile IP working. The mobile node must inform the home that it is on a foreign network so that all datagrams must be forwarded to its foreign network.
- It also must inform the home agent about its care of address (COA) so the home agent can send the forwarded datagrams appropriately.
- When registration is performed, the home agent, in turn, needs to communicate various types of information back to the mobile node.
- Registration can be done in two different ways depending on the location of the COA.

  1. COA at the FA : In this case, registration is done as shown in Fig. 3.3.4.

  - The MN sends its registration request to the FA (containing COA).
  - The FA forwards the request to the HA.
  - The HA now setup a mobility binding containing the mobile node's home IP address, the current COA and the lifetime of the registration.
  - The registration expires automatically after the lifetime and is deleted. So the MN should reregister before expiration.
  - After mobility binding, the HA sends reply message back to the FA which forwards it to MN.

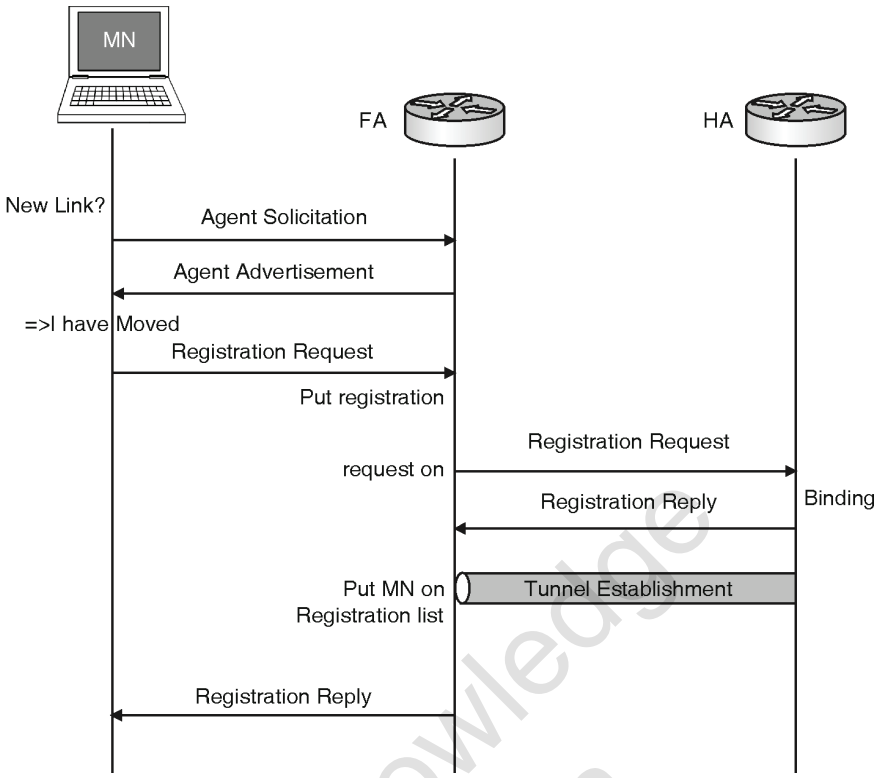


Fig. 3.3.4 : Registration procedure of mobile node via FA (COA at FA)

2. COA is co-located : In this case, the registration is very simple and shown in Fig. 3.3.5

- The MN may send registration request directly to the HA and vice versa.
- If the MN received an agent advertisement from the FA, it should register via this FA if the R bit is set in the advertisement.

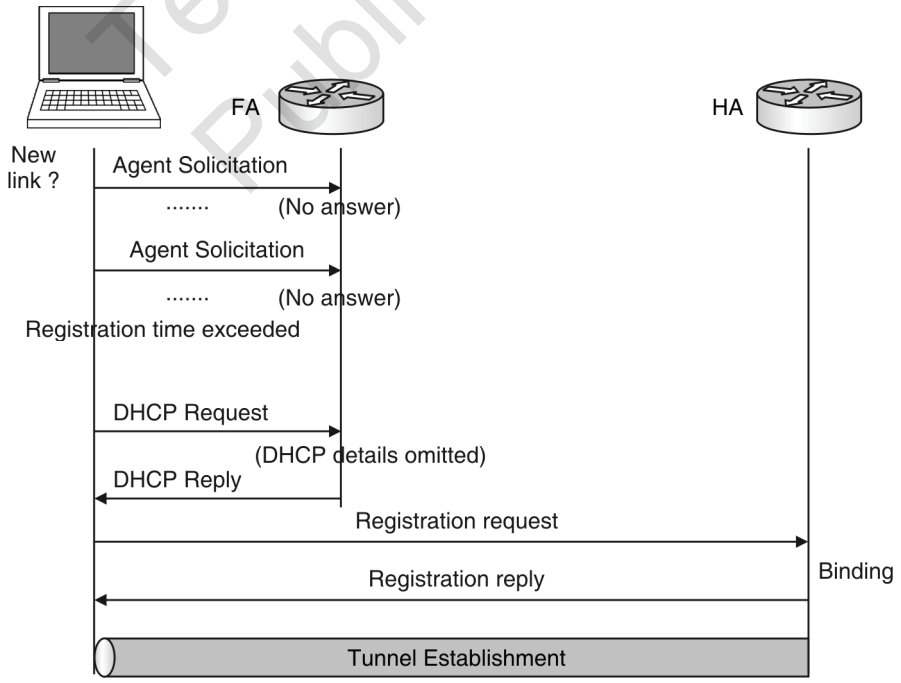


Fig. 3.3.5 : Registration procedure of mobile node via HA (Co- located COA)

1. Registration request message

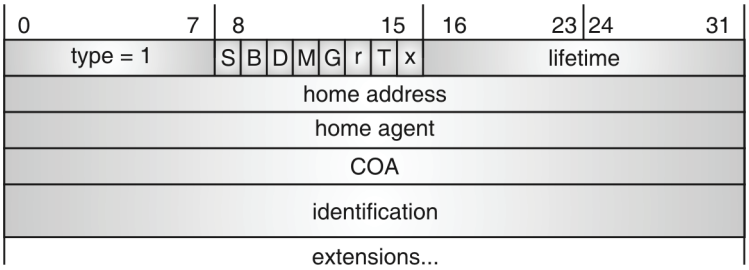


Fig. 3.3.6 : Registration request message

The registration request message is shown in Fig. 3.3.6 and various fields are described as follows :

- **Type :** It is set to 1 for registration request.
- **S bit :** If set, indicates that the MN also wants the FA to retain priority binding.
- **B bit :** If set, indicates that an MN also wants to receive the broadcast packets which have been received by the HA in home network.
- **D bit :** If set, it indicates that the de-capsulation of packets is performed by the MN.
- **Lifetime :** Denotes the validity of the registration in seconds.
- **Home address :** The home address is the fixed IP address of the MN.
- **Home agent :** It is the IP address of the home agent.
- **Identifications :** 64 bit identification is generated by MN to identify a request and match it with registration replies.

2. Registration reply message

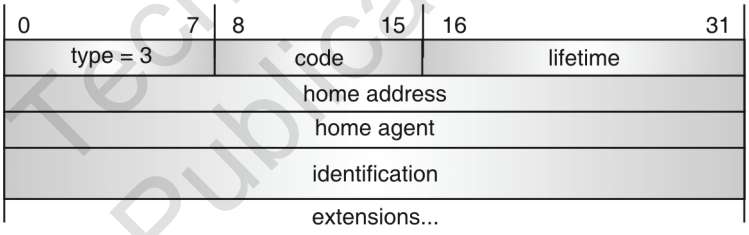


Fig. 3.3.7 : Registration reply message

The registration reply message is shown in Fig. 3.3.7 and various fields are described as follows :

- **Type :** It is set to 3.
- **Code :** Code indicates the result of the registration request. It specifies whether the registration request was successful or denied by the HA, or denied by the FA.

  Example codes are :

- Registration successful
  - Code = 0; registration is accepted
  - Code =1; registration is accepted, but simultaneous mobility bindings unsupported
- Registration denied by FA
  - Code = 65; administratively prohibited
  - Code = 66; insufficient resources
  - Code = 67; mobile node failed authentication

- Code = 68; home agent failed authentication
- Code = 69; requested lifetime too long

– Registration denied by HA
- Code = 129; administratively prohibited
- Code = 131; mobile node failed authentication
- Code = 133; registration identification mismatch
- Code = 135; too many simultaneous mobility bindings

Extensions

It contains the parameters for authentication and may also contain other information as required.

3.3.5 Tunnelling and Encapsulation

MU – May 12, Dec. 13, May 14, May 15, Dec. 15, May 16, May 17, Dec. 17

Q.	Explain how tunnelling works for mobile IP using IP-in-IP, minimal and generic routing encapsulation respectively. Discuss the advantages and disadvantages of these three methods.	**(May 12, 10 Marks)**
Q.	Explain encapsulation with respect to mobile IP.	**(Dec. 13, 5 Marks)**
Q.	Describe tunnelling and encapsulation in Mobile IP.	**(May 14, 5 Marks)**
Q.	Why is Mobile IP packet required to be forwarded through a tunnel ?	**(May 15, 5 Marks)**
Q.	Why is mobile IP packet required to be forwarded through tunnel? Explain minimal and generic technique of encapsulation of mobile IP.	**(May 15, Dec. 15, May 16, May 17, 10 Marks)**
Q.	Discuss how tunnelling work for mobile IP using IP-In-IP encapsulation.	**(Dec. 17, 5 Marks)**

What is tunneling ?

– When a mobile node moves out from home network, the HA sends packet to COA of the MN via a tunnel.

– A tunnel establishes a virtual pipe for data packet.

– In Mobile IP, the start of the tunnel is the home agent, which does the encapsulation. The end of the tunnel depends on what sort of care of address is being used which decapsulates data packet.

– If foreign agent COA is used then FA acts as the tunnel end point and if co-located COA is used then MN acts as the tunnel end point.

– If a CN wants to send data packet to MN (currently not in home network) the data packet is first encapsulated at HA and sent via a tunnel and then decapsulated at FA and finally forwarded to the MN.

– The encapsulation process is shown in the Fig. 3.3.8.

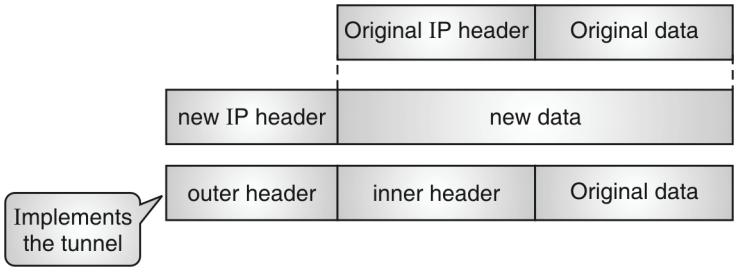


Fig. 3.3.8 : IP encapsulation

- **Encapsulation** means putting a packet made up of a packet header and data into the data field of a new packet.
- **Decapsulation** is the reverse process of encapsulation, that is removing the packet from the data part of another packet.

- The disadvantages of encapsulation are :
  - Packet size is larger than the original packet.
  - Encapsulation can be done only when there is an entity at the tunnel end that decapsulates the IP datagram.
  - After a CN's IP datagrams are captured, datagrams tunneled to the FA for delivery to the MN. The tunneling can be done by one of three encapsulation techniques. These are discussed below.

Why Tunneling is required?

Why does the Mobile IP packet required to be forwarded through a tunnel ?

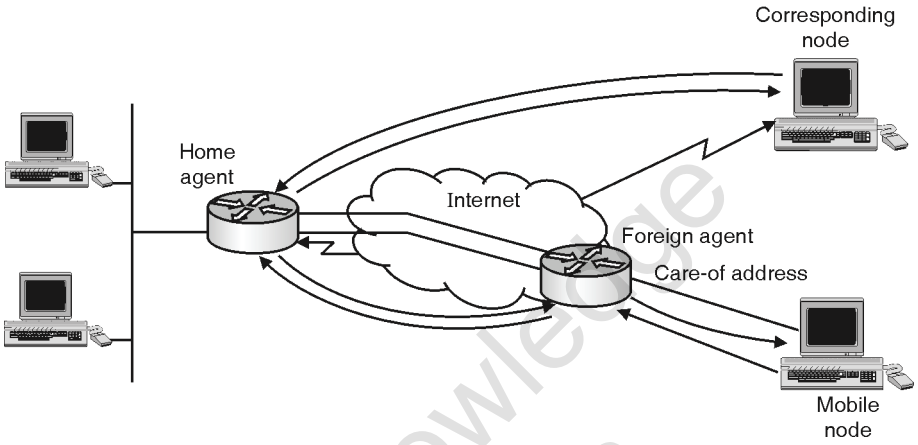


Fig. 3.3.9 : Mobile IP

- Consider a situation when a Correspondent Node (CN) wants to send an IP packet to a Mobile Node (MN). All the CN knows about this MN is, its IP address.
- The CN is totally unaware of the MN's location and so sends it as usual to MN's IP address.
- The internet, routes this packet to the Home router of the MN also called as Home Agent (HA).
- The HA now knowing that the MN is not in its home network encapsulates and tunnels the packet to the COA.
- The Care-of-address (COA) defines the current location of the MN from an IP point of view.
- Since internet routes are created based on the header contents of an IP packet, to route it from HA to COA, we need a new header for the packet to be transmitted.
- The new header on top of the original header is made (Fig. 3.3.10). Now this will enable us to set a new direct route (a tunnel) to the MN from the HA as it is roaming.

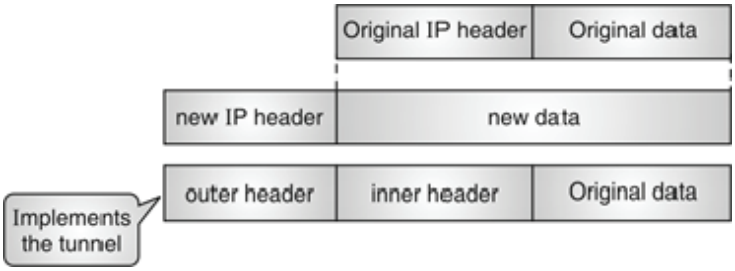


Fig. 3.3.10 : Encapsulation

Thus tunnelling is the process of creating a tunnel by the HA to the COA to route packets to the Mobile Node as it roams. It establishes a pipe (a data stream between two connected ends) wherein the data is inserted and moves in FIFO order.

3.3.5(a) IP-in-IP Encapsulation

MU - May 16, Dec. 17

Q.	Explain IP-in-IP technique of encapsulation of mobile IP.	**(May 16, 5 Marks)**
Q.	Discuss how tunneling work for mobile IP using IP-In-IP encapsulation.	**(Dec. 17, 5 Marks)**

- IP-in-IP encapsulation is defined in RFC 2003. It is the simplest approach and must always be supported.
- In this type of encapsulation, the entire IP datagram sent by the internet host is inserted in a new IP datagram as the payload.
- As shown in the Fig. 3.3.11 the HA encapsulates the received IP datagram within another IP datagram.

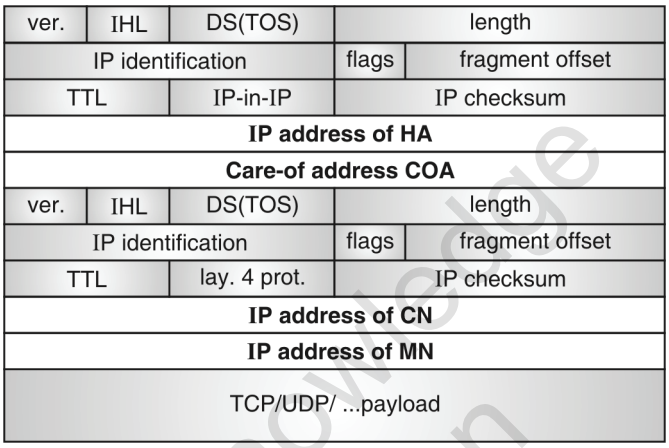


Fig. 3.3.11 : IP-in-IP encapsulation

The various fields in the outer header are :

1. **ver. (Version) :** Version field denotes the version number and set to 4 for IPv4.
2. **IHL (Internet header length) :** IHL indicates the length of the outer header.
3. **DS (TOS) :** It is just copied from the inner header.
4. **Length :** It denotes the complete length of the encapsulated packet.
5. **TTL (time to live) :** It indicates the period of validity of the packet. TTL should be high enough so the packet can reach the tunnel endpoint.
6. **IP-in-IP :** This denotes the type of protocol used in the IP payload.
7. **IP checksum :** This is used for error detection mechanism.

The fields of inner header are almost same as the outer header the only differences are :

- The address fields consist of the address of the original sender and receiver.
- The TTL value of the inner header is decremented by 1. This means that the whole tunnel considered a single hop from the original packet's point of view.

The TCP/UDP payload contains the actual user data to be transmitted.

Advantage

It is simple to implement and it is a default encapsulation mechanism.

Disadvantage

Most of the outer header fields are same as inner header so this method increases redundancy.

3.3.5(b) Minimal Encapsulation

MU – May 12, May 15, May 17

Q.	Explain minimal encapsulation. Also discuss merits and demerits.	**(May 12, 5 Marks)**
Q.	Explain minimal techniques of encapsulation of Mobile IP packet.	**(May 15, May 17, 5 Marks)**

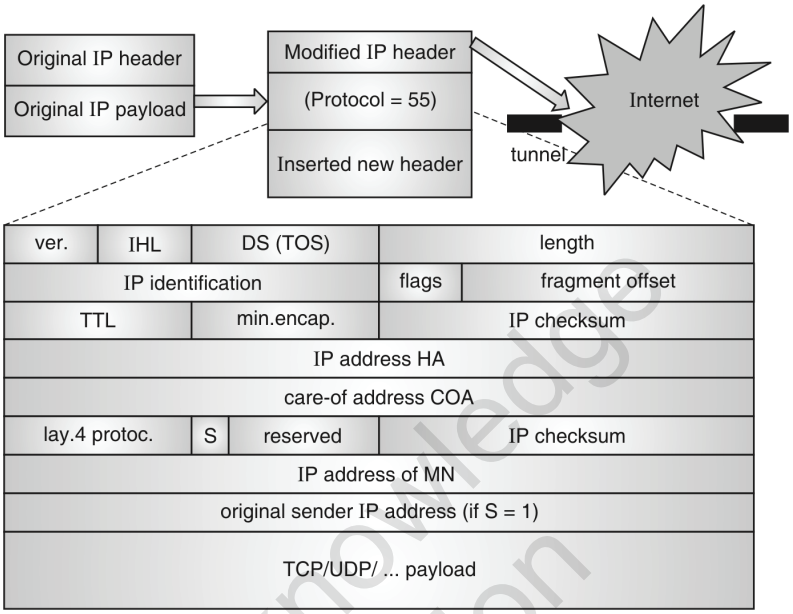


Fig. 3.3.12 : Minimal encapsulation

- Minimal encapsulation is defined in RFC 2004. It involves fewer fields in IP packet. It can be used if the HA, MN, and FA all agree to use. Fig. 3.3.12 shows the minimal encapsulation.
- The outer header fields are almost same as for IP encapsulation; the only difference is in the **Type** field. It is set to 55.
- The inner header is much smaller than IP encapsulation packet.
- The **S bit** indicates whether the original sender's IP address is included in the header or not. Value 0 indicates sender's IP address can be omitted.
- **Advantage :** Lower overhead as compared to IP-in-IP encapsulation as it avoids redundancy.
- **Disadvantage :** It does not support fragmentation to deal with tunnel with smaller path maximum transmission units (MTU).

3.3.5(c) Generic Routing Encapsulation (GRE)

MU – May 12, Dec. 15

Q.	Explain Generic encapsulation. Also discuss merits and demerits.	**(May 12, 5 Marks)**
Q.	Explain Generic technique of encapsulation of mobile IP.	**(Dec. 15, 10 Marks)**

- GRE is defined in RFC 1701.
- It is a generic encapsulation mechanism developed before the development of mobile IP.
- GRE allows the encapsulation of packets of one protocol suite into the payload portion of a packet of another protocol suite.
- Fig. 3.3.13 shows the generic routing encapsulation. The GRE header is prepended to the packet of one protocol suite with the original header and data.

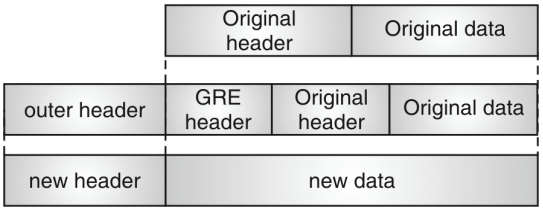


Fig. 3.3.13 : Generic routing encapsulation

Fig. 3.3.13 shows the header of the packet inside the tunnel between home agent (HA) and COA using GRE encapsulation.

The various fields of the GRE header that follow the outer header are described as follows :

1. **Protocol type :** Protocol type is set to 47 for GRE encapsulation.
2. **C bit :** If C bit is set, the checksum field contains the valid IP checksum of the GRE header and the payload.
3. **R bit :** If set, it indicates that the offset and routing fields are present and contains valid information.
4. **K bit :** If it is set, indicates the key field is present and may be used for authentication.
5. **S bit :** If set, indicates that the sequence number field is present.
6. **s bit :** If set, indicates that the strict source routing is used.
7. **rec. (recursion control) :** It represents a counter that shows the number of allowed recursive encapsulations.

ver.	IHL	DS(TOS)	length
IP identification		flags	fragment offset
TTL	GRE	IP checksum	
IP address of HA			
Care-of address COA			
C R K S s rec.	rsv.	ver.	protocol
checksum (optional)		offset (optional)	
key (optional)			
sequence number (optional)			
routing (optional)			
ver.	IHL	DS(TOS)	length
IP identification		flags	fragment offset
TTL	lay. 4 prot.	IP checksum	
IP address of CN			
IP address of MN			
TCP/UDP/ ...payload			

Fig. 3.3.14 : Generic routing encapsulation

8. **rev. (reserved) :** This field is reserved for future used and must be set to 0.
9. **ver. (version) :** It is set to **0** for the GRE version.
10. **Protocol :** Indicates the protocol used by the packet following the GRE header.
11. **Checksum :** Contains a valid IP checksum of the GRE header and the payload (present only when C bit is set).
12. **Offset :** It represents the offset in bytes for the first source routing entry (present only when R bit is set).
13. **Key :** Contains a key that can be used for authentication (present only when K bit is set).
14. **Routing :** It is a variable length field and contains the fields for source routing.

Advantage

- GRE supports other network layer protocols in addition to IP.
- It allows more than one level of encapsulation.

3.3.5(d) Optimization

MU – May 18

Q. What is triangular routing problem? How do you optimize mobile IP for avoiding triangular routing ?

Q. Why and how can optimization in Mobile IP be achieved. **(May 18, 5 Marks)**

Triangular routing

- As discussed in section 3.3.2, the IP packet from a CN destined to an MN needs to be routed to its HA first and then tunneled to the foreign agent of the MN and IP packet from the MN can be directly routed to the CN.
- If the CN and MN are very near, then also the IP packet has to travel a long way to reach the MN. This inefficient behavior of a non optimized mobile IP is called ***Triangular Routing***.
- The triangle is made of the three segments, CN to HA, HA to COA/MN, and MN back to CN. (Refer Fig. 3.3.15)

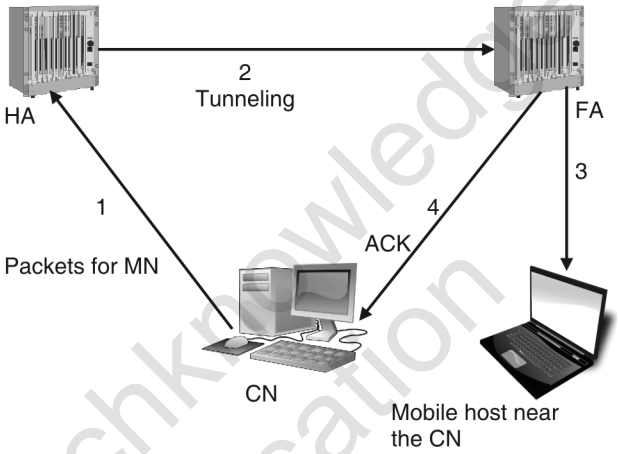


Fig. 3.3.15 : Triangular Routing

Route optimization to avoid triangular routing

To solve triangular routing problem, a route optimization protocol has been introduced. Basically this protocol defines some message so as to inform CN of an up to date location of MN. Once the current location of the MN is known, the CN itself performs tunneling and sends packet directly to MN.

The optimized mobile IP protocol needs four additional messages; these are :

1. **Binding request**

   If a node wants to know where the MN is currently located, it can send a binding request to the HA.

2. **Binding update**

   The HA sends a binding update to the CN and informs the CN the current location of an MN. The binding update can request an acknowledgement.

3. **Binding acknowledgement**

   On request, after receiving a binding update message, a node returns a binding acknowledgement.

4. **Binding warnings**

   - A binding warning message is sent by a node if it decapsulates a packet for an MN but it is not the FA for that MN currently.
   - If CN receives the binding warning, it requests the HA for a new binding update.
   - If the HA receives the warning it directly sends a binding update to the CN.

The Fig. 3.3.16 explains the four messages together with the case of an MN changing its FA and shows the exchange of messages in optimization protocol.

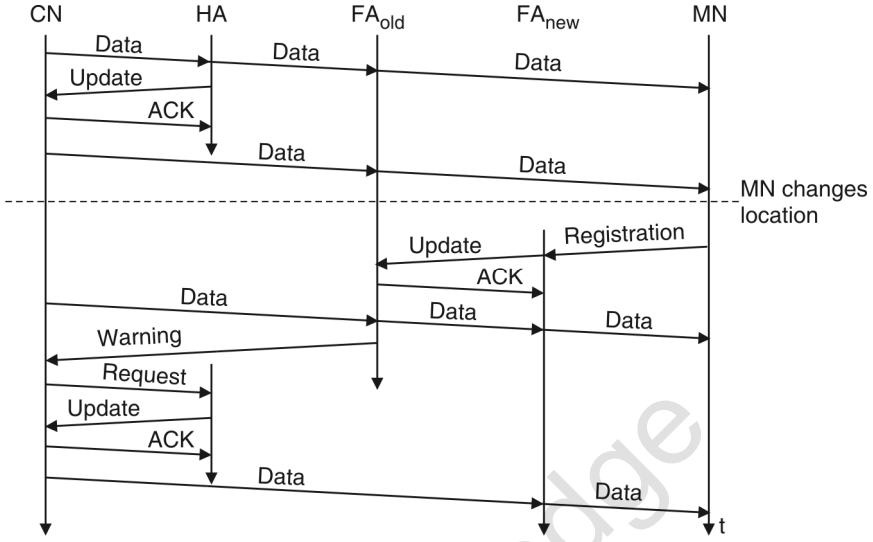


Fig. 3.3.16 : Optimized mobile IP working

- The CN requests the current location of MN from the HA.
- HA returns the COA of the MN via update message.
- CN acknowledge this updated message and stores mobility binding.
- Now CN can send data directly to the current foreign agent FA_{old}. FA_{old} now forwards these data to MN.
- The MN might now change its location and register with a new foreign agent FA_{new}.
- FA_{new} informs FA_{old} about new registration of MN via an update message and FA_{old} acknowledged this update message.
- CN doesn't know about the current location of MN, it still tunnels its packets for MN to the old foreign agent FA_{old}.
- The FA_{old} notices packets destined to MN but also knows MN currently not in current FA.
- FA_{old} might now forward these packets to the new COA of MN which is new foreign agent.
- Thus the packets that are in transit are not lost. This behavior is another optimization to basic mobile IP and provides smooth handover.
- FA_{old} sends binding warning message to CN. CN then requests a binding update.
- The HA sends an update to inform the CN about the new location, which is acknowledged. Now, CN can send data directly to FA_{new}, and avoid triangular binding.
- However, the optimization will not work if the MN does not want to reveal its current location to the CN because of security.

3.3.6 Reverse Tunnelling

- There may be a situation where it is not feasible or desired to have the mobile node (MN) send packets directly to the internetwork via FA.
- In that case, an optional feature called **reverse tunneling** is used if it is supported by mobile node, home agent and foreign agent.
- As shown in Fig. 3.3.17 , a reverse tunnel is setup between MN and HA (If COA is co-located), or between FA and HA (if FA acts as COA)
- All transmission from MN are now tunneled back to the home network where HA transmits them over the Internet.

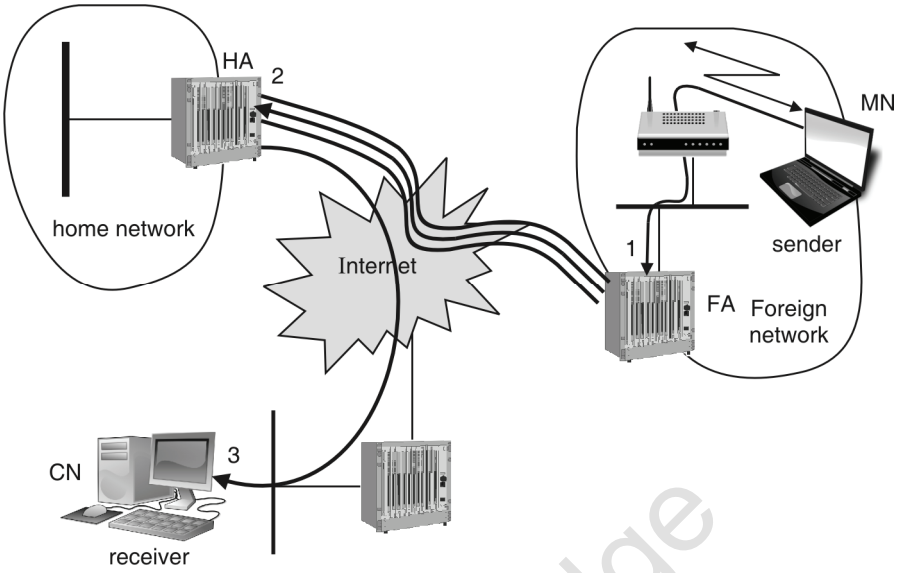


Fig. 3.3.17 : Reverse tunneling

Reverse tunneling is used in following scenario.

1. Ingress Filtering/Firewalls

- If the network where mobile node located has implemented certain security measures that prohibits the node from sending packets using its normal IP address.
- With a reverse tunnel the packet is first encapsulated by FA and sent to the HA.

2. Multi-cast

Reverse tunneling is required for multicasting where the nodes in multicast group are in the home network, as an MN in a foreign network cannot transmit multicast packets directly in this case, as the foreign network might not provide the technical infrastructure for multicast communication.

3. TTL (time to live)

- When an MN is in home network, and if MN node moves to a foreign network, its TTL might be too low for the packets to reach the same node as before.
- A reverse tunnel is needed that represents one hop transmission.

Problems with reverse tunneling

- Reverse tunneling may cause a triangular routing problem in the reverse direction. All packets from MN to CN now go through the HA. The CN might not be able to decapsulate the packet as the CN could be a non Mobile IP device, so the RFC 3024 does not offer solution to this reverse triangular routing.
- Reverse tunneling may raise some security issues. For example, a tunnel which starts in the private network of a company and reaching out into the internet could be hijacked and abused for sending packets through firewall.
- Reverse tunneling may also introduce the possibility of denial-of-service attack.

3.3.7 Limitations of Mobile IP

1. Frequent Mobility

Mobile IP was designed to handle mobility of devices, but only relatively infrequent mobility. This is due to the work involved with each change. This overhead isn't a big deal when you move a computer once a week, a day or even an hour. It can be an issue for “real-time” mobility such as roaming in a wireless network, where hand-off functions

operating at the data link layer may be more suitable. Mobile IP was designed under the specific assumption that the attachment point would not change more than once per second.

2. Issue with DHCP

Mobile IP is intended to be used with devices that maintain a static IP configuration. Since the device needs to be able to always know the identity of its home network and normal IP address, it is much more difficult to use it with a device that obtains an IP address dynamically, using something like DHCP.

3. Security Issue

Firewalls, causes difficulty for mobile IP because they block all classes of incoming packets that do not meet specified criteria. Enterprise firewalls are typically configured to block packets from entering via the internet. In many cases authentication with FA is problematic as the FA typically belongs to another organization or network.

4. QoS Issue

- The QoS solution for mobile IP should satisfy requirements such as scalability, conservation of wireless bandwidth, low processing overhead, authorization and accounting etc.
- When handover occurs in mobile IP environment, some applications such as web browser and file transfer using TCP connection will face disconnection or a degradation of the performance.
- Another problem is with the tunnel based communication. In tunnel based communications different data flows addressed to the same IP address are treated in the same manner. Thus tunneling makes it hard to give a flow of packets a special treatment needed for QoS.

3.3.8 Mobile IP and IPv6

- **Ipv4 :** The network layer protocol in the TCP/IP protocol suite is currently IPv4. IPv4 provides the host-to-host communication between systems in the Internet. IPv4 has some deficiencies that make it unsuitable for the fast growing Internet, including the following:
  - Despite all short term solutions, such as subnetting, classless addressing, and NAT, address depletion is still a long term problem in Internet.
  - The Internet must accommodate real time audio and video transmission. This type of transmission requires minimum delay strategies and reservation of resources not provided by IPv4 design.
  - The Internet must accommodate encryption and authentication of data for some applications. No encryption or authentication is provided by IPv4.
- **Ipv6 :** To overcome these problems, IPv6 also known as IPng (Internet Protocol next generation) was proposed. In IPv6, the Internet protocol was extensively modified to accommodate the growth and new demands of the Internet.
  - The format and the length of the IP addresses were changed along with the packet format
  - Related protocols such as ICMP were also modified.
  - Other protocols in the network layer, such as ARP, RARP, IGMP were either deleted or included in ICMPv6 protocol. Routing protocols such as RIP and OSPF were slightly modified to accommodate these changes.

The fast spreading use of Internet and new services such as mobile IP, IP telephony, and IP-capable mobile telephony, may require the total replacement of IPv4 by IPv6.

Advantages of IPv6

- Larger address space-An IPv6 address is 128 bit long. Compared with the 32 bit long IPv4 address, this is huge increase in address space.
- Better Header format-IPv6 uses a new header format in which options are separated from the base header and inserted when needed, between the base header and the upper layer data. This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.
- New Options-IPv6 has new options to allow for additional functionalities.
- Allowance for extension-IPv6 is designed to allow the extension of protocol if required by new technologies or applications.
- Support for resource allocation-In IPv6, the ***type-of-service*** field has been removed, but mechanism called ***Flow label*** has been added to enable the source to request special handling of packet. This mechanism can be used to support traffic such as real-time audio and video.
- Support for more security-The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

Features of Ipv6 to support mobility

- No special mechanisms are needed for securing mobile IP registration. In every Ipv6 node **address auto configuration** i.e. the mechanism for acquiring a COA is inbuilt.
- **Neighbor discovery** mechanism is also mandatory for every Ipv6 node. So special foreign agents are no longer needed to advertise services.
- Combining the features of address auto configuration and neighbor discovery enables every Ipv6 mobile node to create and obtain a topologically correct address or the current point of attachment.
- Every Ipv6 node can send binding updates to another node, so the MN can send its COA directly to the CN and HA. The FA is no longer needed. The CN processes the binding updates and makes corresponding entries in its routing cache.
- The MN is now able to :
  - Decapsulates the packets
  - To detect when it needs a new COA and
  - To determine when to send binding updates to the HA and CN
- A **soft handover** is possible with Ipv6. The MN sends its new COA to the old router serving the MN at the old COA, and the old router can encapsulate all incoming packets for the MN and forwards them to new COA.

3.4 Routing

- Routing in wireless ad-hoc networks is different and complicated than wired networks or wireless networks with infrastructure. This difference can be explained by example shown in Fig. 3.4.1.
- Fig. 3.4.1 shows the network topology at two different time t_1 and t_2.
- Seven nodes are connected depending upon the current transmission characteristics between them.
- At time t_1 node N4 can receive N1 over a good link, but N1 receives N4 via a weak link. Links may not have the same characteristics in both directions.
- The situation may change at time t_2 N1 cannot receive N4 any longer, N4 can receive N1 via a weak link. Network topology is frequently changed in ad-hoc networks.

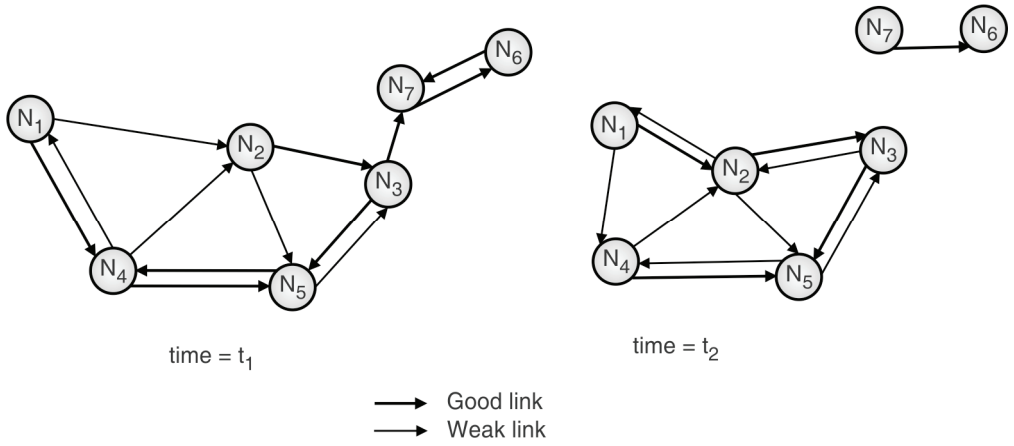


Fig. 3.4.1 : Ad-hoc network example

The main difference between ad-hoc and wired networks due to this routing in ad-hoc networks are different are as follows :

1. Asymmetric links

- Links are not symmetric in both directions as we have seen. Node N2 can receive N1 but N1 cannot receive signals from N2.
- Thus routing information collected for one direction is not useful for other direction.
- However many routing algorithms for wired networks rely on a symmetric scenario.

2. Redundant links

- Wired network have redundant link to survive link failure, but this redundancy is limited.
- In ad-hoc networks there might be many redundant links up to high complexity.
- Routing algorithms in wired network can handle up to some redundancy, but a large redundancy can cause a large computational overhead for routing table updates.

3. Interference

- In ad-hoc networks links comes and go depending on the transmission characteristics, one transmission may interfere with other, and nodes might overhear the transmissions of other nodes.
- Interference chances in wireless ad-hoc networks are very high.

4. Dynamic topology

- This is the greatest problem in routing for ad-hoc networks.
- Mobile nodes moves or medium characteristics might change frequently. This results frequent changes in topology as shown in Fig. 3.4.1 (at time=t_2). Due to change in topology, in ad-hoc networks the routing tables have to be updated frequently.

There are basically two classes of flat routing algorithms :

1. Table-Driven routing protocols (Proactive)

- These protocols are also called as proactive protocols since they maintain the routing information even before it is needed.
- Each and every node in the network maintains routing information to every other node in the network. Routes information is generally kept in the routing tables and is periodically updated as the network topology changes.
- Many of these routing protocols come from the link-state routing.

Examples of proactive routing protocols

- Destination Sequence Distance Vector (DSDV)
- Optimized Link State Routing (OLSR)
- Fisheye State Routing (FSR)
- Wireless Routing Protocol (WRP)

Advantage

- These protocols can give good real time traffic QoS.
- Route availability reduces delay (no route acquisition delay)

Disadvantage

- The proactive protocols are not suitable for larger networks, as they need to maintain node entries for each and every node in the routing table of every node. This causes more overhead in the routing table leading to consumption of more bandwidth.
- Possibly inefficient (due to unnecessary signaling message overhead)
- Redundant routes may exist
- Some computed routes may not be needed

2. On Demand routing protocols (Reactive)

- These protocols are also called reactive protocols since they don't maintain routing information or routing activity at the network nodes if there is no communication.
- If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packets.
- The route discovery usually occurs by flooding the route request packets throughout the network.

Examples of Reactive routing protocols

- Dynamic Source Routing (DSR)
- Ad-hoc On demand Distance Vector (AODV)

Advantage

- Eliminates periodic route advertisements
- May reduce power and bandwidth requirements.

Disadvantage

- Adds route-acquisition delay
- May cause more signaling if route expiration times are too short

3.4.1 Destination Sequence Distance Vector Routing (DSDV)

DSDV is a ***proactive table driven*** mobile ad-hoc network routing protocol. It is an enhancement of distance vector routing (Bellman Ford algorithm).

Problems with Distance Vector

- In Distance vector routing each node exchanges its routing table periodically with its neighbors.
- Each node uses its local information for creating its routing table.
- However, the local information may be old and invalid. This is because changes at one node in the network propagate

- However, the local information may be old and invalid. This is because changes at one node in the network propagate slowly through the network (step-by-step with every exchange). Thus the local information may not be updated promptly.
- This gives rise to loops. A message may loop around a cycle for a long time (count-to-infinity problem).
- Solutions used for this problem in wired networks such as poisoned reverse and split horizon do not work in case of ad-hoc networks due to the rapidly changing topology.

DSDV now adds two things to the distance vector algorithm.

1. Sequence numbers

- Each node advertise routing table with a sequence number.
- This sequence number used to distinguish stale route with the fresh route and help the nodes to process advertisements in correct order thus avoids loops that are likely in distance vector.

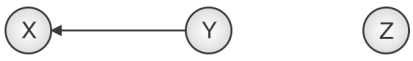
2. Damping

- It prevents temporary change in the network topology from destabilize the routing. These changes are of short duration only.
- When a node receives an advertisement containing a change in the current network topology, it waits for a certain time before forwarding the updates in routing table to other nodes.
- Waiting time depends on the time interval between the first and the best announcement of a path to a certain destination.

DSDV algorithm

- Each node maintains a routing table which stores
  - Next hop and cost metric towards each destination.
  - Also a sequence number that is created by the destination itself.
- In DSDV each node periodically forwards its own routing table to its neighbors. And each node increments and appends its sequence number when sending its local routing table.
- Each route is tagged with a sequence number, the routes with greater sequence numbers are preferred.
- Each node advertises a monotonically increasing even sequence number for itself.
- When a node finds that a route is broken, it increments the sequence number of the route and advertises it with infinite metric. Thus infinite metric indicates the route is broken.
- Destination advertises new sequence number.

Example



- Let S(X) be the destination sequence number for Z already present in X's routing table.
- Now say X receives information about route to Z with the destination sequence number S(Y) form node Y. Thus S(Y) is the destination sequence number sent from Y.
- X now compares S(X) and S(Y).
  - If S(X) > S(Y), then X ignores the routing information received from Y.
  - If S(X) = S(Y), and cost of going through Y is smaller than the route known to X, then X sets Y as the next hop to Z.
  - If S(X) < S(Y), then X sets Y as the next hop to Z, and S(X) is updated to equal S(Y).

Advantages of DSDV

- DSDV is an efficient protocol for route discovery. Whenever a route to a new destination is required, it already exists at the source.
- Hence, latency for route discovery is very low.
- DSDV also guarantees loop-free paths.

Disadvantages of DSDV

- However, DSDV needs to send a lot of control messages. These messages are important for maintaining the network topology at each node.
- This may generate high volume of traffic for high-density and highly mobile networks.
- Special care should be taken to reduce the number of control messages.

3.4.2 Dynamic Source Routing (DSR)

- DSR is a **reactive routing** protocol which is able to manage a MANET.
- DSR was specifically designed for use in **multi-hop wireless ad hoc networks** of mobile nodes.
- It uses an **on-demand** approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. This approach saves the bandwidth
- It uses **Source routing** for route discovery that is the source node determines the whole path from the source to the destination node and deposits the addresses of the intermediate nodes of the route in the packets.

DSR contains 2 phases

1. Route Discovery (find a path)
2. Route Maintenance (maintain a path)

1. Route Discovery

- A node only tries to discover a route to a destination if it has to send something to this destination and there is no known route.

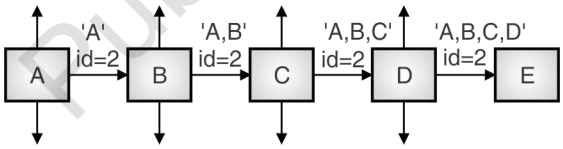


Fig. 3.4.2 : Route Discovery example

- If node A has in his Route Cache a route to the destination E, this route is immediately used. If not, the Route Discovery protocol is started :
  1. Node A (initiator) sends a Route Request packet by flooding the network
  2. If node B has recently seen another Route Request from the same target or if the address of node B is already listed in the Route Record, Then node B discards the request!
  3. If node B is the target of the Route Discovery, it returns a Route Reply to the initiator. The Route Reply contains a list of the “best” path from the initiator to the target. When the initiator receives this Route Reply, it caches this route in its Route Cache for use in sending subsequent packets to this destination.
  4. Otherwise node B isn’t the target and it forwards the Route Request to his neighbors (except to the initiator).

2. Route Maintenance

- In DSR every node is responsible for confirming that the next hop in the Source Route receives the packet. Also each packet is only forwarded once by a node (hop-by-hop routing).
- If a packet can't be received by a node, it is retransmitted up to some maximum number of times until a confirmation is received from the next hop. Only if retransmission results then in a failure, a Route Error message is sent to the initiator that can remove that Source Route from its Route Cache. So the initiator can check his Route Cache for another route to the target.
- If there is no route in the cache, a Route Request packet is broadcasted.

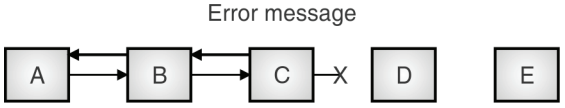


Fig. 3.4.3 : Route maintenance example

Example :

1. If node C does not receive an acknowledgement from node D after some number of requests, it returns a Route Error to the initiator A.
2. As soon as node receives the Route Error message, it deletes the broken-link-route from its cache. If A has another route to E, it sends the packet immediately using this new route.
3. Otherwise the initiator A is starting the Route Discovery process again.

Optimization to route discovery

To avoid too many broadcasts, that causes flooding of the network; every node has an counter and it is decremented each time the packet is broadcasted. Nodes can drop a request if the counter reaches zero.

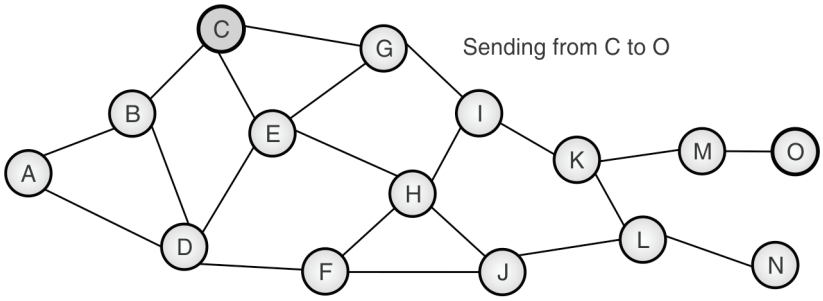
DSR Advantages

- Routes maintained only between nodes who need to communicate
- Reduces overhead of route maintenance
- Route caching can further reduce route discovery overhead.
- A single route discovery may yield many routes to the destination, due to intermediate nodes replying from local caches.

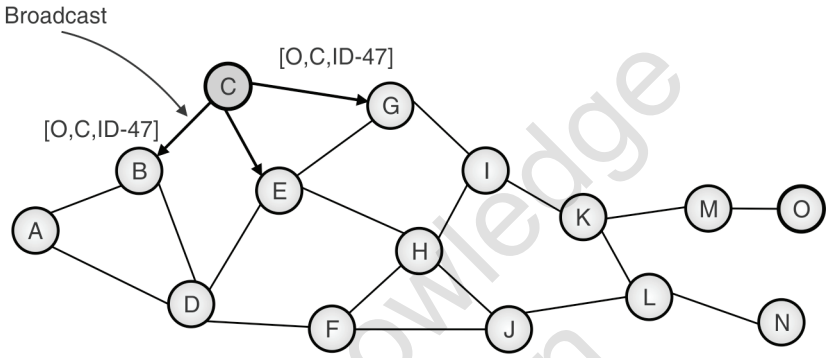
DSR Disadvantages

- Packet header size grows with route length due to source routing
- Flood of route requests may potentially reach all nodes in the network.
- Potential collisions between route requests propagated by neighboring nodes
  - Insertion of random delays before forwarding RREQ
  - Increased contention if too many route replies come back due to nodes replying using their local cache
  - Route Reply *Storm* problem
- Stale caches will lead to increased overhead

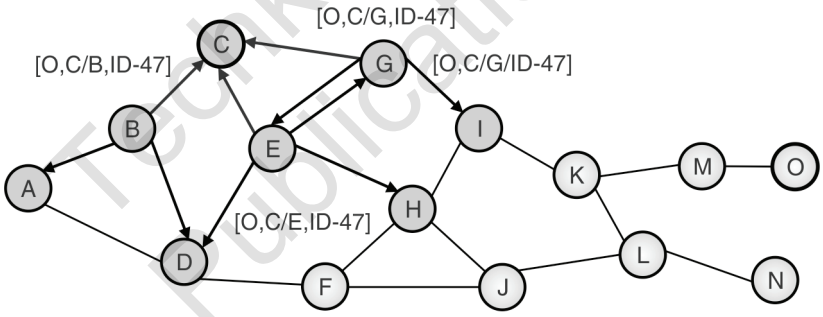
Example of DSR



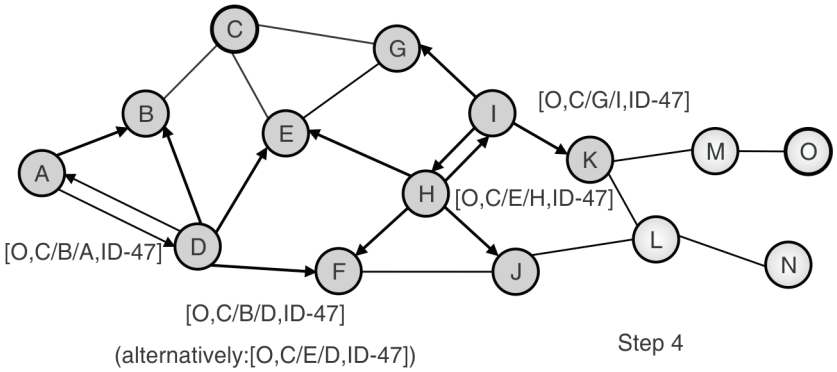
Step 1



Step 2



Step 3



Step 4

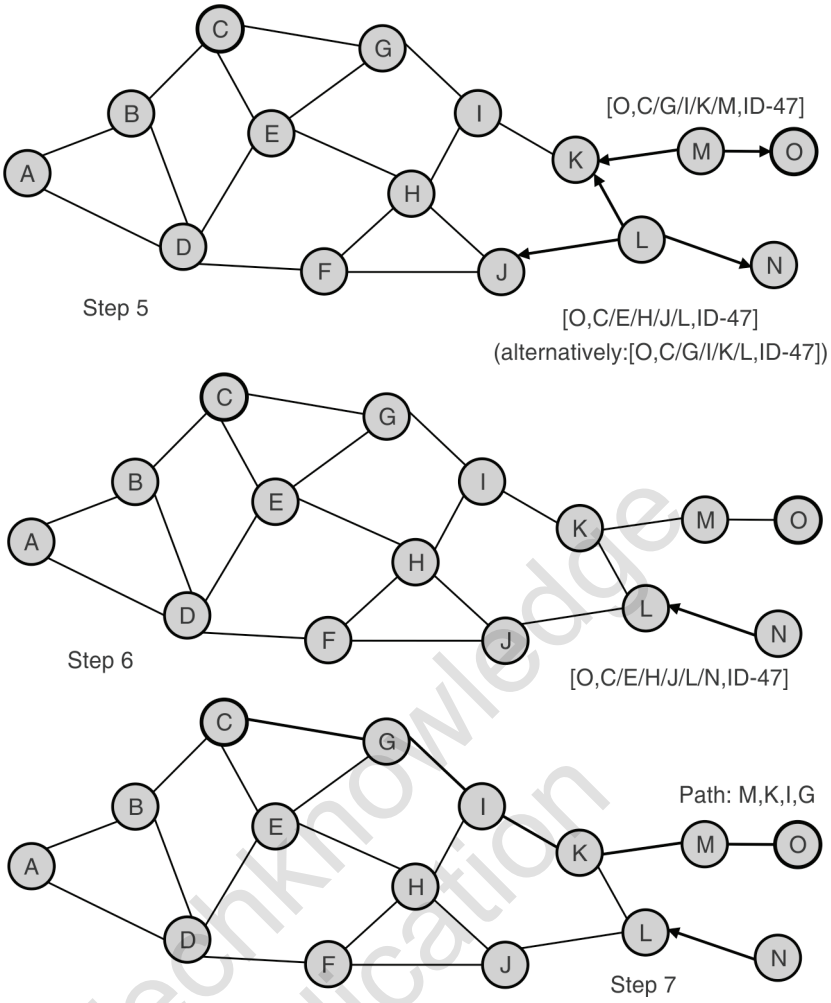


Fig. 3.4.4 : DSR route discovery, Step1 to Step7

3.5 Mobile TCP

MU – May 12, Dec. 12, Dec. 13, May 14, May 15

Q.	Explain snooping TCP and mobile TCP with their merits and demerits.	**(May 12, Dec. 13, 10 Marks)**
Q.	Discuss Mobile Transport Layer.	**(Dec. 12, 5 Marks)**
Q.	Explain merits and demerits of snooping TCP and indirect TCP?	**(May 14, 5 Marks)**
Q.	Explain the functioning of I-TCP and SNOOP -TCP, giving advantages and disadvantages of both.	**(May 15, 10 Marks)**

3.5.1 Traditional TCP

- Traditional TCP's performance is deteriorated in wireless networks causing many errors and disconnections as it was designed to perform well in wired networks and stationary node environments, and not in wireless networks.
- The traditional TCP does not consider properties of wireless network such as limited bandwidth, long latency, high bit error rate, and frequent disconnections and hence, does not guarantee reliable and efficient data transmission in wireless environment.
- TCP assumes that most of the packet losses in wired network are due to congestion. But in wireless environment, there could be many reasons for packet losses those need to be considered.

- The following section describes the traditional TCP designed for a wired network and also discusses the need for modification to the traditional TCP in order to use it efficiently in wireless networks.

1. Congestion Control

- TCP was originally designed for fixed networks with fixed end systems.
- Routers are responsible to transfer packets from source to destination.
- If a packet is lost in the wired network, the probable reason of that is congestion. Congestion is nothing but a temporary overload at some point in the transmission path, i.e. a state of congestion at a node.
- Each router maintains buffers for packets. If the sum of the packets' input rate destined for one output link exceeds the capacity of the output link, then the buffer becomes full and it cannot forward the packets fast enough, so the packets are dropped by the router.
- A dropped packet is lost and a gap is noticed by the receiver in the packet stream.
- The receiver continues to acknowledge all in-sequence packets up to the missing one.
- The receiver notices the missing acknowledgement of the lost packet and assumes a packet is lost due to congestion.
- Retransmitting the lost packet and continuing to send packets at full sending rate would only increase congestion.
- To reduce congestion, the transmission rate is slowed down considerably by TCP.
- All other TCP connections with the same problem follow the same process. By doing this, the congestion is resolved soon.
- This behavior of TCP during congestion is called **slow-start**.
- TCP ensures that even under heavy load the available bandwidth will be shared equally.

2. Slow start

- The behavior of TCP after detection of congestion is called slow start.
- It is used to resolve congestion quickly.

Slow-start working

- Sender calculates a congestion window for the receiver. The start size of window is one segment (TCP packet).
- The sender sends one packet and waits for an acknowledgement. If this acknowledgement arrives, the sender increases the congestion window by one. And now sends two packets (congestion window = 2).
- After arrival of two corresponding acknowledgements, the sender adds 2 in the congestion window, one for each acknowledgement.
- This scheme doubles the congestion window every time the acknowledgement arrives. This is called as an **exponential increase,** and it continues till a certain value called as **congestion threshold**.
- Once congestion window crosses the congestion threshold, further increase in transmission rate is linear i.e. congestion window is increased by one each time the acknowledgement is received.
- This linear increase continues till the sender detects the packet loss.
- Once the packet loss is detected; the sender sets the congestion threshold to half of its current congestion window and congestion window is set to one. The above steps are repeated again.

3. Fast retransmit/fast recovery

- The sender detects the loss of packets in two ways.
  (i) If a time-out occurs at the receiver, in that case the sender activates normal slow start.
  (ii) If the sender receives continuous acknowledgements for the same packet (Duplicate acknowledgements).

- If this is the case, then the sender can deduce two things - one is that the receiver got all packets up to the acknowledgement in sequence and second is that the receiver is continuously receiving something from the sender. Therefore, the packets must have been lost due to simple transmission error and not due to network congestion.
- The sender can now retransmit the missing packet(s) before the timer expires. This behavior is called as a **fast retransmit**.
- The receipt of an acknowledgements show that there is no congestion to justify a slow start. The sender can continue with the current congestion window. The sender performs a fast recovery from the packet loss.
- This mechanism improves the efficiency of TCP dramatically.

4. Implication on mobility

There are many problems that degrade the performance of TCP.

Transmission errors

TCP assumes congestion if packets are dropped. This is not always true for wireless networks, where often, packet loss is due to transmission errors.

Mobility (i.e. handoff)

Mobility (i.e. handoff) itself can cause packet loss, if e.g. a mobile node roams from one access point (e.g. foreign agent in Mobile IP) to another while there are still packets in transit to the wrong access point and forwarding is not possible.

High delay

Wireless networks have a considerably longer latency (delay) than wired network.

Battery powered devices

Mobile devices are battery powered and hence power is a scarce source. Protocol designed for mobile or wireless networks should be power efficient.

Limited Bandwidth

- Available bandwidth within a cell may change dramatically. This leads to difficulties in guaranteeing QoS parameters such as delay bounds and bandwidth guarantees.
- **Slow start** is the mechanism of traditional TCP for wired network to deal congestion. In that, TCP assumes packet losses due to congestion. However, in wireless network there could be some other reasons that cause packet loss such as BER, and frequent disconnections by handoff.
- If we use traditional TCP in wireless environment, it drastically reduces the congestion window size and doubles the transmission timeout value. This unnecessary congestion control reduces the utilization rate of the bandwidth, reduces the network performance severely.
- Serial time-out at TCP sender degrades overall throughput more than losses due to bit errors or small congestion window do.
- Hence we required to change TCP for mobile environment. There are large number of devices and applications that are using current TCP; it is not possible to change TCP completely just to support mobile users or wireless links.
- Therefore any enhancement to TCP has to be compatible with the standard TCP.

3.5.2 Classical TCP improvements

- In modified TCP, following characteristics are desired :
  1. Improve the TCP performance for mobile entities.

2. Maintenance of end-to-end TCP semantics.
3. Minimize the problem caused by lengthy disconnections or by frequent disconnections.
4. Adjust with dynamically changing bandwidth over the already starved wireless link.
5. Make sure that the handoff management is efficient.

- The following sections present some classical solutions that can be used to modify standard TCP to improve the performance of wireless environment.

3.5.2(a) Indirect TCP (I-TCP)

MU - May 13, May 14, May 15, Dec. 15, May 17, May 18

Q.	Explain I-TCP in detail.	**(May 13, 10 Marks)**
Q.	Explain merits and demerits of indirect TCP ?	**(May 14, 5 Marks)**
Q.	Explain functioning of I-TCP and Snooping TCP. Giving advantages and disadvantages of both.	**(May 15, May 17, 10 Marks)**
Q.	Explain the functioning of Mobile TCP.	**(Dec. 15, 5 Marks)**
Q.	Explain any two TCP for Mobile communication.	**(May 18, 5 Marks)**

- There are two facts: one is that TCP performs poorly together with wireless links and second is that TCP within the fixed network cannot be changed.
- Fig. 3.5.1 shows an example with a mobile host connected via a wireless link and an access point to the wired internet where the correspondent node resides. The correspondent node could also use wireless access.
- I-TCP separates a TCP connection into two parts : a fixed and a wireless part.
  - **Fixed part is** between the mobile support router (access point) and the fixed host over the fixed network.
  - **Wireless part** is between the MH (Mobile host) and its access point over the wireless medium.
- Standard TCP is used between the fixed computer and the access point.
- A good point for segmenting the connection between mobile host and correspondent host is at the foreign agent of mobile IP.
- The foreign agent is responsible for controlling the user mobility. And during handover, foreign agent transfers the connection to the new foreign agent.
- The foreign agent acts as a proxy and relays all data in both directions.

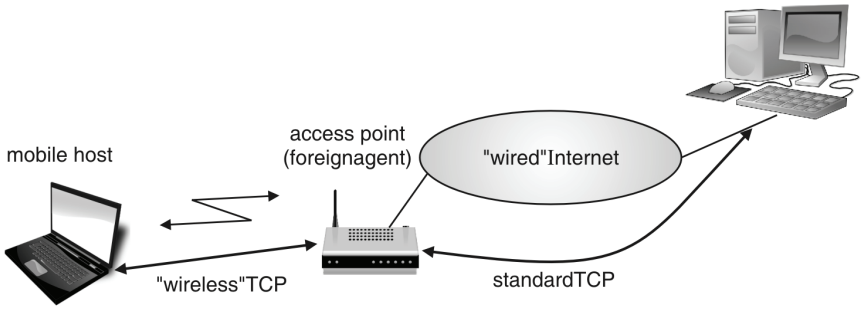


Fig. 3.5.1 : Indirect TCP

There may be following scenarios.

1. Correspondent host sends a packet to mobile host

- Since the correspondent node is a fixed node, it sends a TCP packet via a standard TCP.

- An access point receives that packet and sends an acknowledgement to a fixed host for the received packet.
- The access point buffers the packet and forwards this packet to a mobile host using wireless TCP.
- If there is any transmission error on wireless link then access point retransmits that packet instead of fixed host retransmitting it. (This is also called local retransmission).
- Once the acknowledgement is received for the packet form the mobile host; the access point then removes that packet from its buffer.
- Thus the access point acts as a proxy.

2. Mobile host transmits a packet to a fixed host

- Mobile host sends a TCP packet and access point receives that packet and sends an acknowledgement to mobile host.
- If a packet is lost at wireless link then the mobile host notices this event much faster and retransmits the packet.
- The access point then transmits that packet to the fixed host via standard TCP connection.
- If a packet is lost in wired network then FA handles the retransmissions.
- After receiving the acknowledgement the packet is removed from the buffer.

3. The mobile host moves to a new location and handover takes place

- When mobile host moves to a new location, it registers with new foreign agent. After registration the new foreign agent informs the old foreign agent about its current location.
- The old foreign agent forwards all the buffered packets to new foreign agent as the packet in the buffer have already been acknowledged.
- With the buffered data the sockets of the access point must also migrate to the new foreign agent. This is shown in Fig. 3.5.2.

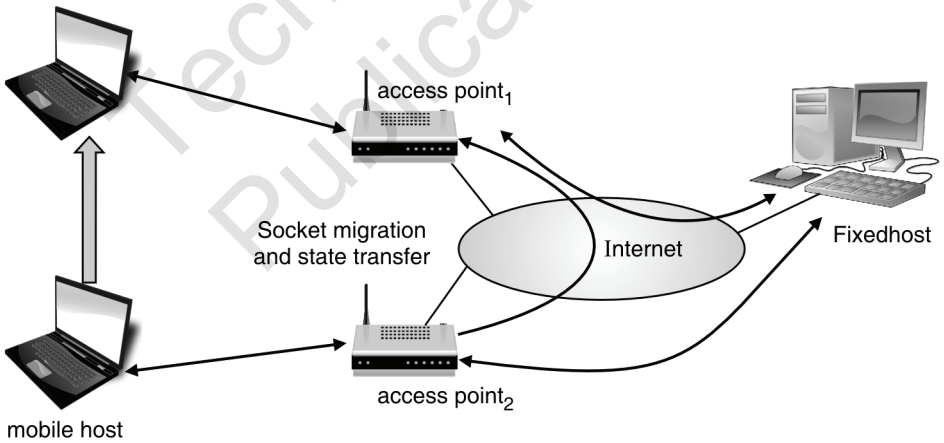


Fig. 3.5.2 : Socket migration after handover of a mobile host

- The socket reflects the current state of the TCP connection i.e. sequence number, addresses, port numbers etc.
- The handover is transparent to the correspondent host and no new connection is established for the mobile host.

Advantages of I-TCP

- I-TCP does not require any changes in the standard TCP used for wired networks.
- Due to the partitioning transmission errors on the wireless link cannot propagate into the fixed network.
- It is simple to control, mobile TCP is used only for one hop between, e.g., a foreign agent and mobile host.
- A very fast retransmission of packets is possible, the short delay on the mobile hop is known.

- Due to the segmentation of the TCP connection, the mobile host and correspondent host can use different transport layer protocols.
- Different solutions to optimize the transfer over the wireless link can be tested or carried out without putting of the Internet at risk.

Disadvantages of I-TCP

- It losses end-to-end semantics; an acknowledgement sent by access point to a sender does now no longer mean that a receiver really got a packet. If a foreign agent crashes before sending acknowledged packet to a mobile host; the sender has no way to find out whether packets have been received or not.
- Higher handover latency is more problematic. All packets sent by correspondent host are buffered by the foreign agent. If a mobile host changes its location, old foreign agent has to forward the buffered packets to the new foreign agent as they have already been acknowledged by the old access point.
- The foreign agent must be a trusted entity because TCP connection ends at this point.

3.5.2(b) Snooping TCP (S-TCP)

MU – May 12, Dec. 13, May 14, May 15, May 17, May 18

Q.	Explain snooping TCP with its merits and demerits.	**(May 12, Dec. 13, May 14, 5 Marks)**
Q.	Explain the functioning of SNOOP -TCP, give advantages and disadvantages.	**(May 15, 10 Marks)**
Q.	Explain functioning of I-TCP and Snooping TCP. Giving advantages and disadvantages of both.	**(May 15, May 17, 10 Marks)**
Q.	Explain any two TCP for Mobile communication.	**(May 18, 5 Marks)**

- Snooping TCP works completely transparently and leaves the TCP end-to-end connection intact.
- It overcomes the some drawbacks of the I-TCP.

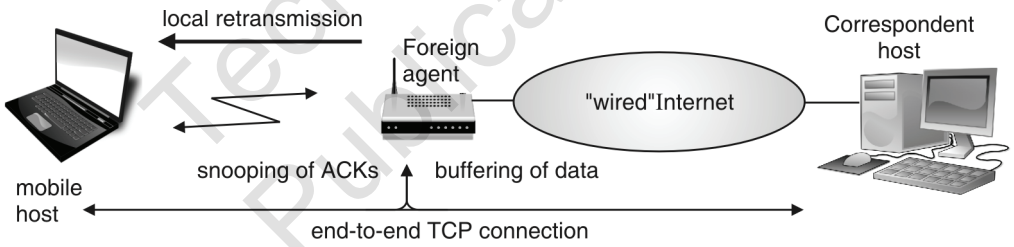


Fig. 3.5.3 : Snooping TCP

Snooping TCP works as follows :

1. Correspondent host sends a packet to mobile host

- Correspondent host sends a packet to mobile host via wired TCP connection. The access point buffers the packet sent by correspondent host.
  - Access point also snoops on the packet in both directions to reorganize acknowledgements.
  - Once the mobile host receives the packet, it sends an acknowledgement and this acknowledgement also passes through the access point.
  - If the access point doesn't receive any acknowledgement from a mobile host within certain amount of time, then it retransmits the packet from its buffer, performing a much faster retransmission compared to the fixed host.
  - The time-out for acknowledgements can be much shorter, because it reflects only the delay of one hop plus processing time.

- It is also possible that mobile host sends duplicate acknowledgements for the same packet to indicate a packet loss; the foreign agent can filter these duplicate acknowledgements so, that unnecessary retransmissions from the correspondent host can be avoided.

2. Mobile host transmits a packet to a correspondent host

- When a mobile host sends a packet to correspondent host, the foreign agent keeps track of the sequence numbers of these packets.
- When a foreign agent detects a gap in the sequence numbers, i.e. packet loss, it sends a negative acknowledgement (NACK) to the mobile host.
- Once the mobile host receives the NACK, it can retransmit the missing packet immediately.
- Reordering of the packets is done automatically at the correspondent node by TCP.

Note that to maintain end-to-end semantics of TCP, foreign agent must not acknowledge data itself to the correspondent host (instead FA forwards the ACK received from the MH). This ensures the correspondent host that the mobile host has actually received the data. Now if foreign agent crashes, the time-out mechanism of correspondent host still works and triggers a retransmission of a lost packet.

Advantages of Snooping-TCP

- The end-to-end semantics are preserved.
- Correspondent host need not to be changed; most of the enhancements are done in the foreign agent.
- It doesn't need handover of the state as soon as the mobile host moves to another foreign agent. Assume there might still be data in the buffer not transferred to the new foreign agent. All that happens is a time-out at the correspondent host and the retransmission of the packets to the new foreign agent.
- It doesn't matter if the new foreign agent uses the enhancement or not. If not, snooping TCP automatically falls back to the standard solution.

Disadvantages of snooping TCP

- Using NACK between foreign agent and the mobile host assumes additional mechanisms on mobile host. This approach is no longer transparent for arbitrary mobile hosts.
- Snooping TCP does not isolate the behavior of the wireless link from wired link as in case of I-TCP. If the delay in wireless link is very high as compared to wired link, the timers of the access point and the correspondent host would almost be same. Thus, the delay on wireless link automatically triggers time-out in correspondent host and causes retransmissions. Thus the effectiveness of S-TCP completely depends on the quality of wireless link.
- If user applies end-to-end encryption, S-TCP fails. Because TCP header would be encrypted and hence snooping on the sequence numbers is meaningless.

3.5.2(c) Mobile TCP (M-TCP)

MU – May 12, Dec. 13, May 13, Dec. 17, May 18

Q.	Explain M-TCP in detail.	**(May 13, 5 Marks)**
Q.	Explain mobile TCP with its merits and demerits.	**(May 12, Dec. 13, 5 Marks)**
Q.	Write a short note on M-TCP.	**(Dec. 17, 5 Marks)**
Q.	Explain any two TCP for Mobile communication.	**(May 18, 5 Marks)**

- The occurrence of lengthy and/or frequent disconnection is the major problem in wireless networks. M-ICP deals with the lengthy and/or frequent disconnections.

- M-TCP aims :
  - To improve overall throughput
  - To lower the delay
  - To maintain end-to-end semantics of TCP
  - To provide a more efficient handover
- The connection is split up into 2 parts by M-TCP similar to I-TCP.
- The correspondent host and supervisory host communicate via the unmodified standard TCP.
- The communication between supervisory host (SH) and mobile host (MH) is done by the modified special TCP.
- For transferring data between both parts, the supervisory host is used.
- SH does not perform caching or retransmission of data as a relatively low bit error rate is assumed by M-TCP on the wireless link. Whenever a packet is lost on the wireless link, the original sender must retransmit it. TCP end-to-end semantics are thus maintained. For fair sharing over the wireless link, M-TCP needs a bandwidth manager.

Working of M-TCP

- Packets are sent to the mobile host by a correspondent host.
- If any packet is lost on the wireless link, then the original sender retransmits the packet. Thus, end-to-end semantics are maintained.
- All the packets sent to MH are monitored by the SH and are acknowledged by the MH via ACK packets.
- After a set amount of time, if the SH still does not receive any ACK, it assumes that the MH is disconnected.
- SH sets sender's window size to zero and thus chokes the sender. Once the window size is set to zero, the sender is forced to go into a persistent mode. In the persistent mode, independent of the receiver's period of disconnected state, the state of the sender will not change.
- Once the SH detects the connectivity again, the sender's window size is again set to the old value, enabling the sender to send at full speed.

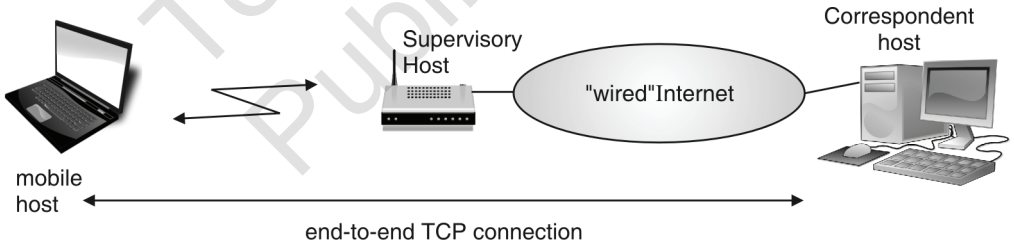


Fig. 3.5.4 : Mobile TCP (M-TCP)

Advantages of M-TCP

- End-to-end semantics are maintained. SH itself doesn't send any ACK, it only forwards ACKs that were received from the MH.
- It avoids unnecessary retransmissions, if the MH is disconnected.
- It is not necessary to forward all data to a new SH because SH does not buffer any data.

Disadvantages of M-TCP

- Losses on wireless link are propagated to the wired link. This is because SH does not act as a proxy and does not buffer the packets and is not responsible for local retransmission.
- It requires new network elements like bandwidth manager.

3.5.3 Fast Retransmit/Fast Recovery

- This scheme improves the performance during handover.
- Moving to a new FA can cause packet loss or time out at mobile host or correspondent host. In such case standard TCP assumes congestion and goes into slow start mode although there is no congestion (Here packet loss is caused due to handover).
- A host can use fast retransmit/fast recovery after it receives duplicate acknowledgements. The idea here is to automatically force the fast retransmit behavior on the mobile host and correspondent host.

Correspondent host enters in fast retransmit mode

- As soon as mobile host registers at a new foreign agent, it starts sending duplicate acknowledgements (three duplicate ACKs) to the correspondent host.
- On receiving these duplicates the correspondent host continues to send with the same rate it did before the mobile host moved to new foreign agent.
- Thus the correspondent host goes into fast transmit mode and not to the slow start.

Mobile host enters in fast retransmit mode

- Mobile host may also enter in slow start after moving to a new foreign agent.
- To avoid this, after handover a mobile host automatically activates fast retransmit mode.
- The mobile host retransmits all unacknowledged packet using the current congestion window size without going into slow start.

Advantages of fast retransmit/fast recovery

- Foreign agent or correspondent host need not to be changed.
- Minor changes are required in mobile host's software.
- Very Simple.

Disadvantages of fast retransmit/fast recovery

- Insufficient isolation of packet losses. If the handover from one FA to another takes a longer time, the correspondent node will have already started retransmissions.
- This approach focuses on the packet loss due to handover. Packet loss due to problems on the wireless link is not considered.
- This approach requires cooperation between Mobile IP and TCP. It is therefore harder to change one without affecting the other.

3.5.4 Transmission/ Time-out Freezing

- This approach can handle long disconnections of MH.
- Quite regularly, it happens that the MAC layer predict the connection problems, before the connection is actually interrupted from TCP point of view.
- Additionally, the MAC layer knows the actual reason of the disconnection and does not assume congestion as TCP does.
- MAC layer can now inform the TCP layer for the upcoming loss in connection.
- TCP can now stop packet sending and freeze the current state of congestion window and all timers of TCP.
- If the disconnections occur frequently then additional mechanism in the access point must be included to inform the correspondent host about the reason of interruption.

- As soon as the MAC layer detects connectivity again, it informs the TCP to resume operation with the same congestion window and the timers.

Advantages of transmission/time-out freezing

- It offers a way to resume TCP connection even after a longer interruption of the connection.
- This scheme is independent of any other TCP mechanisms such as acknowledgements or sequence numbers. So it can be used together with encrypted data.

Disadvantages of transmission/time-out freezing

- Mobile host as well as correspondent host needs to be changed.
- All mechanisms are based on the capability of MAC layer to detect future interruption.
- If the encryption is used that depends on time-dependent random numbers, then this scheme required resynchronization after interruption.

3.5.5 Selective Retransmission

- In the standard TCP acknowledgments are in sequence.
- If a packet is lost, the sender has to retransmit all the packets starting from the lost packet. (GO-BACK N retransmission). This wastes the bandwidth.
- The selective retransmission approach allows a retransmission of a selective packet i.e. the sender can now determine which packet is to be retransmitted.

Advantages of Selective retransmission

- Sender need to retransmit lost packet only. Thus, bandwidth requirement is much lower and it is advantageous in slow wireless links.
- Improves the performance of TCP in wireless as well as in wire networks.

Disadvantages of Selective retransmission

- Complexity of receiver side increases.
- More buffer space is required at the receiver side to store all the packets following the missing packet and wait for the gap to be filled.

3.5.6 Transaction oriented TCP (T/TCP)

- If a mobile host wants to send a packet via TCP, it requires three steps: connection setup, data transmission, and connection release.
- Both connection setup and connection release require three way handshaking.
- If a mobile host has to send one packet, TCP requires seven packets. Three for connection set up, one for data and again three for connection release (Fig. 3.5.5).
- For the large transmission this overhead is negligible but for small amount of data it is not negligible.
- The transaction oriented TCP provides a solution. It combines the connection setup and connection release with the user data packet.
- This can reduce the number of packets to two from seven.

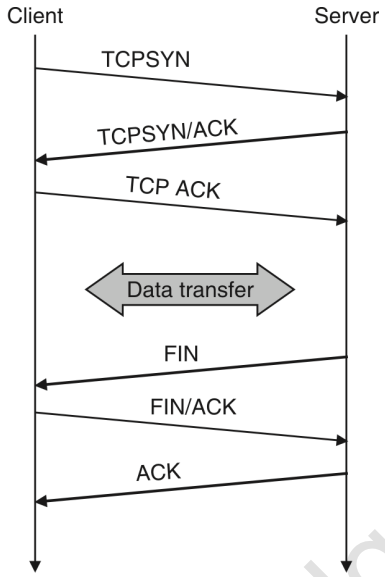


Fig. 3.5.5 : Example of TCP connection setup and release

Advantage of transaction-oriented TCP

Reduce overhead.

Disadvantage of transaction-oriented TCP

- It requires change in mobile host and all correspondent hosts.
- The mobility is no longer transparent.
- It poses many security risks.

3.5.7 Comparison of TCP Variants

Table 3.5.1 : Comparison of the TCP enhancements

Sr. No.	Approach	Mechanism	Advantages	Disadvantages
1.	**Indirect TCP**	Splits TCP connection into two connections	Isolation of wireless link, simple	Loss of TCP semantics, higher latency at handover
2.	**Snooping TCP**	"Snoops" data and acknowledgements, local retransmission	Transparent for end-to-end connection, MAC integration possible	Problematic with encryption, bad isolation of wireless link
3.	**M-TCP**	Splits TCP connection, chokes sender via window size	Maintains end-to-end semantics, handles long term and frequent disconnections	Bad isolation of wireless link, processing overhead due to bandwidth management
4.	**Fast retransmit/ fast recovery**	Avoids slow-start after roaming	Simple and efficient	Mixed layers, not transparent
5.	**Transmission/ time-out freezing**	Freezes TCP state at disconnect, resumes after reconnection	Independent of content or encryption, works for longer interrupts	Changes in TCP required, MAC dependant

Sr. No.	Approach	Mechanism	Advantages	Disadvantages
6.	**Selective retransmission**	Retransmit only lost data	Very efficient	Slightly more complex receiver software, more buffer needed
7.	**Transaction oriented TCP**	Combine connection setup/release and data transmission	Efficient for certain applications	Changes in TCP required, not transparent

3.6 IPv4 and IPv6

MU - May 12

Q. What advantages does the use of IPV6 offer for mobility? **(May 12, 5 Marks)**

Ipv4

The network layer protocol in the TCP/IP protocol suite is currently IPv4. IPv4 provides the host-to-host communication between systems in the Internet. IPv4 has some deficiencies that make it unsuitable for the fast growing Internet, including the following:

- Despite all short term solutions, such as subnetting, classless addressing, and NAT, address depletion is still a long term problem in the Internet.
- The Internet must accommodate real time audio and video transmission. This type of transmission requires minimum delay strategies and reservation of resources not provided by IPv4 design.
- The Internet must accommodate encryption and authentication of data for some applications. No encryption or authentication is provided by IPv4.

Ipv6

- To overcome these problems, IPv6 also known as IPng (Internet Protocol next generation) was proposed.
- In IPv6, the Internet protocol was extensively modified to accommodate the growth and new demands of the Internet.
- The format and the length of the IP addresses were changed along with the packet format.
- Related protocols such as ICMP were also modified.
- Other protocols in the network layer, such as ARP, RARP, and IGMP were either deleted or included in ICMPv6 protocol. Routing protocols such as RIP and OSPF were slightly modified to accommodate these changes.
- The fast spreading use of Internet and new services such as mobile IP, IP telephony, and IP-capable mobile telephony, may require the total replacement of IPv4 by IPv6.

Advantages of IPv6

(i) Larger address space : An IPv6 address is 128 bit long. Compared with the 32 bit long IPv4 address; this is huge increase in address space.

(ii) Better Header format : IPv6 uses a new header format in which options are separated from the base header and inserted when needed, between the base header and the upper layer data. This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.

(iii) New Options : IPv6 has new options to allow for additional functionalities.

(iv) Allowance for extension : IPv6 is designed to allow the extension of protocol if required by new technologies or applications.

(v) Support for resource allocation : In IPv6, the ***type-of-service*** field has been removed, but mechanism called ***Flow label*** has been added to enable the source to request special handling of packet. This mechanism can be used to support traffic such as real-time audio and video.

(vi) Support for more security : The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

Features of Ipv6 to support mobility

- No special mechanisms are needed for securing mobile IP registration. In every Ipv6 node **address auto-configuration** i.e. the mechanism for acquiring a COA is inbuilt.
- **Neighbor discovery** mechanism is also mandatory for every Ipv6 node. So special foreign agents are no longer needed to advertise services.
- Combining the features of address auto-configuration and neighbor discovery enable every Ipv6 mobile node to create and obtain a topologically correct address or the current point of attachment.
- Every Ipv6 node can send binding updates to another node, so the MN can send its COA directly to the CN and HA. The FA is no longer needed. The CN processes the binding updates and makes corresponding entries in its routing cache.

  The MN is now able to :
  - Decapsulate the packets
  - Detect when it needs a new COA and
  - Determine when to send binding updates to the HA and CN
- A **soft handover** is possible with Ipv6. The MN sends its new COA to the old router serving the MN at the old COA, and the old router can encapsulate all incoming packets for the MN and forwards them to new COA.

Ipv6 Header

Fig. 3.6.1 shows both Ipv4 and Ipv6 header format.

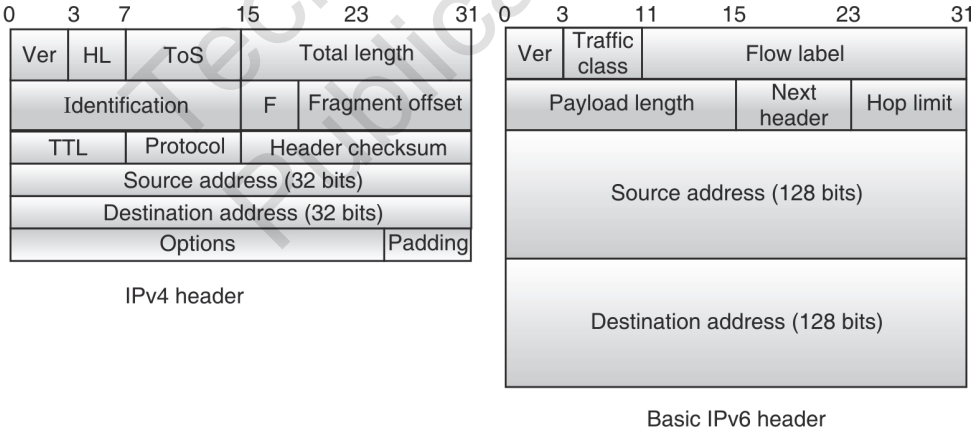


Fig. 3.6.1 : Comparison of Ipv4 and Ipv6 Header format

Fields of Ipv6 header

(i) Version : 4 bits. IPv6 version number.

(ii) Traffic Class : 8 bits. Used to specify different classes or priorities of IPv6 packets.

(iii) Flow Label : 20 bits. Used for specifying special router handling from source to destination(s) for a sequence of packets. It distinguishes the different types of packets such as audio, video, txt etc. and accordingly provides Quality of services to them.

(iv) Payload Length : 16 bits unsigned. Specifies the length of the data in the packet.

(v) Next Header : 8 bits. Specifies the next encapsulated protocol. The values are compatible with those specified for the IPv4 protocol field.

(vi) Hop Limit : 8 bits unsigned. For each router that forwards the packet, the hop limit is decremented by 1. When the hop limit field reaches zero, the packet is discarded. This replaces the TTL field in the IPv4 header that was originally intended to be used as a time based hop limit.

(vii) Source address : 16 bytes. The IPv6 address of the sending node.

(viii) Destination address : 16 bytes. The IPv6 address of the destination node.

Review Questions

Q. 1 Explain working of DRS with a suitable example.

Q. 2 Explain DSDV routing protocol.

Q. 3 Compare M-TCP and Snooping TCP.

Q. 4 Write a short note on DSR.

Q. 5 Explain any two routing algorithms used for MANET.

Q. 6 Explain the errors in wireless networks that degrade the performance of TCP.

Q. 7 Explain various types of transmission errors in wired and wireless networks.

Q. 8 Explain the errors in wireless networks that degrade the performance of TCP and how TCP snooping can improve the performance.

Q. 9 Discuss the problems of using traditional TCP in wireless networks? Explain I-TCP.

Q. 10 What are the problems with IPv4 protocol? What advantages does IPv6 provide over IPv4?

Q. 11 What are the features of IPv6? Explain IPv6 packet format.

❑❑❑

Wireless Local Area Networks

Syllabus

4.1 Wireless Local Area Networks : Introduction, Infrastructure and ad-hoc network

4.2 IEEE 802.11:System architecture, Protocol architecture, Physical layer, Medium access control layer, MAC management, 802.11a, 802.11b

4.3 Wi-Fi security : WEP, WPA, Wireless LAN Threats, Securing Wireless Networks

4.4 HIPERLAN 1 and HIPERLAN 2

4.5 Bluetooth : Introduction, User Scenario, Architecture, protocol stack

Introduction

This chapter introduces another class of wireless network technologies called Wireless Local Area Networks (WLANs). In contrast to the technologies described in the previous chapters such as GSM, GPRS, UMTS etc. WLANs are typically restricted in their diameter to buildings, a campus or a single room and are operated by individuals and not by large scale network providers. The main goal of WLAN is to replace office cabling, to enable tetherless access to the Internet and to allow ad hoc communication. The chapter discusses various WLAN technologies such as IEEE 802.11, HIPERLAN/1 and HIPERLAN/2. For each WLAN system, the details of architecture, the physical layer and MAC layer have been discussed.

Remainder of the chapter focuses on Bluetooth technology and comparison of all of the above mentioned WLAN technologies.

4.1 Wireless Local Area Networks

4.1.1 Introduction

- A wireless LAN (or WLAN, for wireless local area network) is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection.
- The IEEE 802.11, group of standards specify the technologies for wireless LANs.
- Home users can create a wireless network out of an existing wired network and wirelessly extend the reach of the Internet throughout the home on multiple computers.
- By using wireless LAN, it is now not required that every workstation and conference room be wired up to hubs and switches with cables.

Advantages of Wireless LAN

1. **Flexibility :** Within radio coverage, a user can easily communicate without any restriction.
2. **Simplified planning :** Wireless ad-hoc networks do not require any planning for configuring a network.
3. **(Almost) no wiring difficulties :** Because no wiring is required, it can be easily installed where wiring is difficult (e.g. historic buildings, firewalls).
4. **Robust :** Wireless LAN is more robust against disasters like, e.g., earthquakes, fire, or users pulling a plug.
5. **Cost effective :** Once a wireless network is installed, adding new additional user will not increase further cost.

Disadvantages of wireless LAN

1. **Lower bandwidth and transmission quality :** Wireless LAN offers **very low bandwidth** (1-10 Mbit/s) compared to wired networks due to shared medium. Also it has high error rates due to interference. Hence it offers **low QoS** as compared to wired network.
2. **Many proprietary solutions** exist, due to slow standardization procedure.
3. **Local regulatory restrictions :** Several countries impose different spectral restrictions. Due to this it is difficult to establish global WLAN solutions.
4. **Lower safety and security :** Security concerns are high in wireless networks. The open radio interface makes eavesdropping much easier in WLANs than wired network.

4.1.2 Types of WLAN

Based on the network configuration, wireless LANs can be classified into two categories.

1. Infrastructure based wireless networks
2. Ad hoc wireless networks

1. Infrastructure based wireless network

- An important element of this type of network is Access point (AP).
- AP provides an interface between the wireless terminals and wired network infrastructure.
- Here wireless nodes communicate with each other via an access point.
- All the network control procedures like medium access control, synchronization, power management has been done by the AP.
- Fig. 4.1.1 shows three access points with three wireless networks and a wired network.
- The design of infrastructure based wireless network is very simpler than ad-hoc networks. Since AP performs most of the transmission control procedures, the complexity of individual node is less.
- Infrastructure based wireless network is less flexible. For example, in the case of disaster they cannot be used when no infrastructure is left.
- For Example, Cellular phone network.

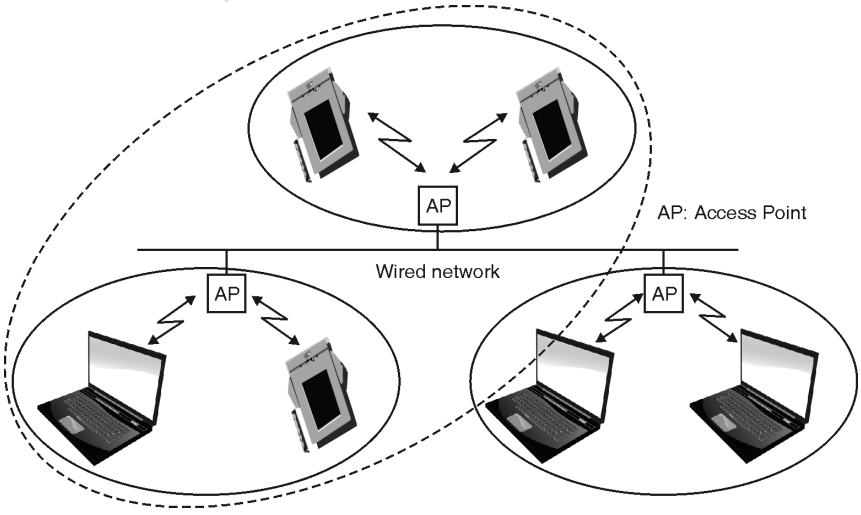


Fig. 4.1.1 : Infrastructure based wireless networks

2. Ad-hoc wireless networks

- Ad hoc wireless networks do not have any wired infrastructure.
- All nodes can communicate directly without need of access point.
- The complexity of nodes in an ad-hoc network is higher because all network functionalities like medium access mechanisms, which hidden and exposed terminal problems have to be implemented within the node itself.
- Fig. 4.1.2 shows two ad-hoc networks with three nodes each.

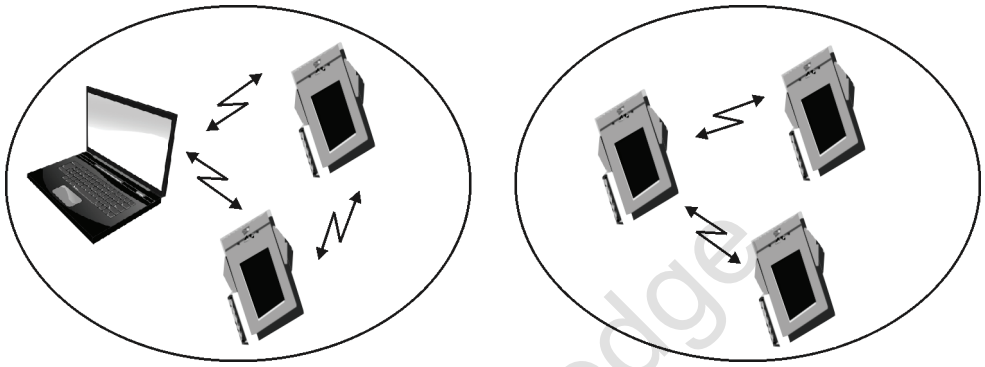


Fig. 4.1.2 : Ad-hoc wireless networks

- In ad hoc networks, nodes can only communicate when they are within each other's radio range or if other nodes can forward the message.
- It offers higher flexibility as these networks can be installed instantly without need of any infrastructure.

4.1.3 Difference between Ad-hoc Network and Infrastructure based Wireless Networks

MU – Dec. 15

Q. Explain Difference between Ad-hoc Network and Infrastructure based Wireless Networks. **(Dec. 15, 5 Marks)**

Sr. No.	Infrastructure based Network	Ad-hoc networks
1.	Devices on this type of network all communicate through a single access point, which is generally the wireless router.	Ad-hoc networks don't require a centralized access point. Instead, devices on the wireless network connect directly to each other.
2.	Infrastructure mode is ideal if setting up a more permanent network.	Ad-hoc mode can be easier to set up if you just want to connect few devices to each other without requiring a centralized access point.
3.	Wireless routers that function as access points generally have higher-power wireless radios and antennas so they can cover a wider area.	Range of Ad-hoc networks are limited by the power of wireless devices connected in the network. Ad-hoc networks don't scale well.
4.	If a device is out of range of another device it wants to connect to, then forwarding of packets is done via access point.	If a device is out of range of another device it wants to connect to, it will pass the data through other devices on the way. Passing the data through several computers is just slower than passing it through a single access point.
5.	The design of infrastructure based network is simpler than ad hoc networks, since an access point	Complexity of individual node in ad hoc networks is higher because all network functionality such as

Sr. No.	Infrastructure based Network	Ad-hoc networks
	performs most of the transmission control procedures, thus reducing the complexity of individual node.	medium access mechanism, power management, synchronization etc. have to be implemented within the node itself.
6.	Infrastructure based wireless network is less flexible. For example, in case of disaster, they cannot be used when no infrastructure is left.	It offers higher flexibility as these networks can be installed instantly without need of any infrastructure.
7.	Requires more planning and takes time to set up.	No planning is needed and Easy to set up.
8.	Architecture of Infrastructure based network is shown in Fig. 4.1.1.	Architecture of ad- hoc network is shown in Fig. 4.1.2.

4.2 IEEE 802.11

- **IEEE 802.11** is a set of standards for implementing wireless local area network (WLAN) in 2.4, 3.6 and 5 GHz frequency bands.
- They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802).
- IEEE 802.11 introduced various versions of 802.11 - 802.11a, 802.11b, 802.11g, etc.
- To maintain interoperability, this standard uses the same interface as the others to higher layers, but specifies the **physical layer** and **medium access layer** adapted to the special requirement of wireless LANs.

4.2.1 IEEE 802.11 System Architecture

IEEE 802.11 LANs can be configured as infrastructure based network or as ad hoc networks.

1. Architecture of Infrastructure based network

Fig. 4.2.1 shows the architecture of IEEE 802.11 infrastructure based network.

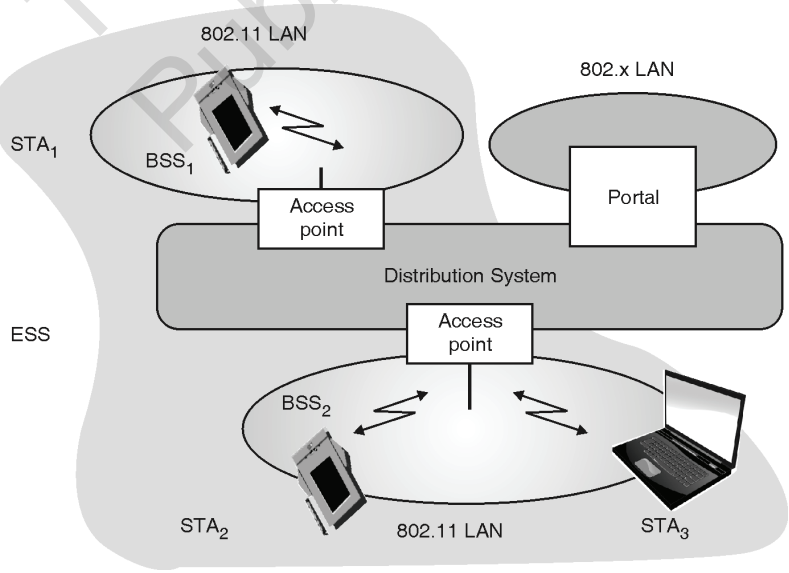


Fig. 4.2.1 : Architecture of an infrastructure based IEEE 802.11

Basic Service Set (BSS)

- The basic building block of IEEE 802.11 architecture is the Basic Service Set (BSS).
- The stations and access point which are within the same radio coverage form a Basic Service Set (BSS).
- All stations within a BSS communicate with the same access point and compete for shared medium.
- Access point can be connected to other access points via distribution system.

Station (STA)

- The station is a wireless node and it is connected to an access point.
- All stations are equipped with wireless network interface cards (WNICs) and contain the functionalities of the 802.11 protocol.
- Wireless station can be mobile devices such as laptops, personal digital assistants, IP phones and other smart phones, or fixed devices such as desktops and workstations that are equipped with a wireless network interface.

Access Point (AP)

- Access points (APs) are base stations for the wireless network.
- Two terminals in the same BSS communicate via AP.
- AP's functions are :
  1. Supports roaming (i.e. changing access points)
  2. Provides synchronization within a BSS
  3. Supports power management
  4. Can control medium access to support time bounded services

Extended Service Set (ESS)

- A set of connected BSSs together form ESS (An Extended Service Set (ESS))
- Access points in an ESS are connected by a distribution system.
- Each ESS has an ID called the ESSID which is a 32-byte (maximum) character string.

Portal

It acts as an internet working unit to connect other LANs.

Distribution System (DS)

- A distribution system works as a backbone network and handles data transfer between different AP's. It connects several BSS's via AP's to portal thus forming a single network.
- The DS is not really the part of IEEE802.11 standard.
- The DS could consist of bridged IEEE LAN wireless links or any other network.

2. Architecture of ad hoc network

In ad-hoc wireless networks, there are one or more independent BSSs (IBSS) as shown in Fig. 4.2.2.

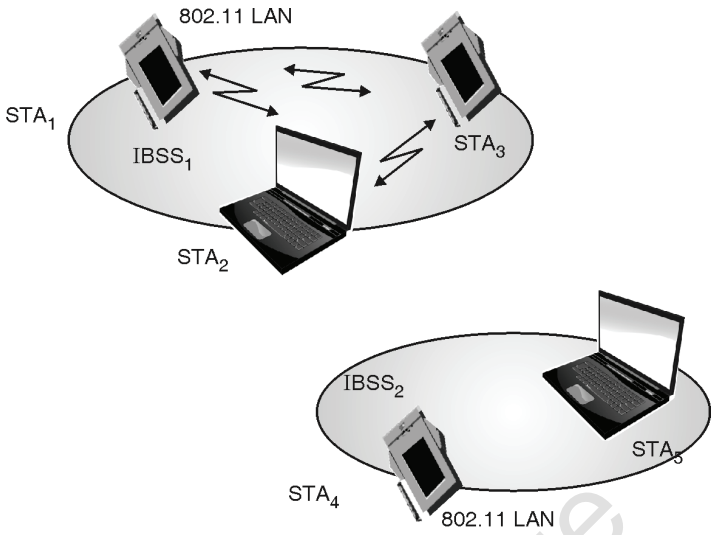


Fig. 4.2.2 : Architecture of IEEE 802.11 ad-hoc wireless LAN

IBSS comprises a group of stations using the same radio frequency. For example, as shown in Fig. 4.2.2 STA_1, STA_2, and STA_3 are in $IBSS_1$, where as STA_4 and STA_5 in $IBSS_2$. This mean, STA_2 can communicate directly with STA_3 but not with STA_4.

4.2.2 IEEE 802.11 Protocol Architecture

MU – May 13

Q. Explain protocol architecture of 802.11. **(May 13, 10 Marks)**

- As shown in Fig. 4.2.3 an 802.11 wireless LAN connected to a switched IEEE 802.3 Ethernet via a bridge (Access point).
- The higher layers (Application, TCP, IP) of wireless node works same as wired node.
- The upper part of data link control layer i.e. logical link control (LLC) covers the differences of the medium access control layers needed for different media.
- IEEE 802.11 standard only covers the specification of **physical layer and MAC layer.**

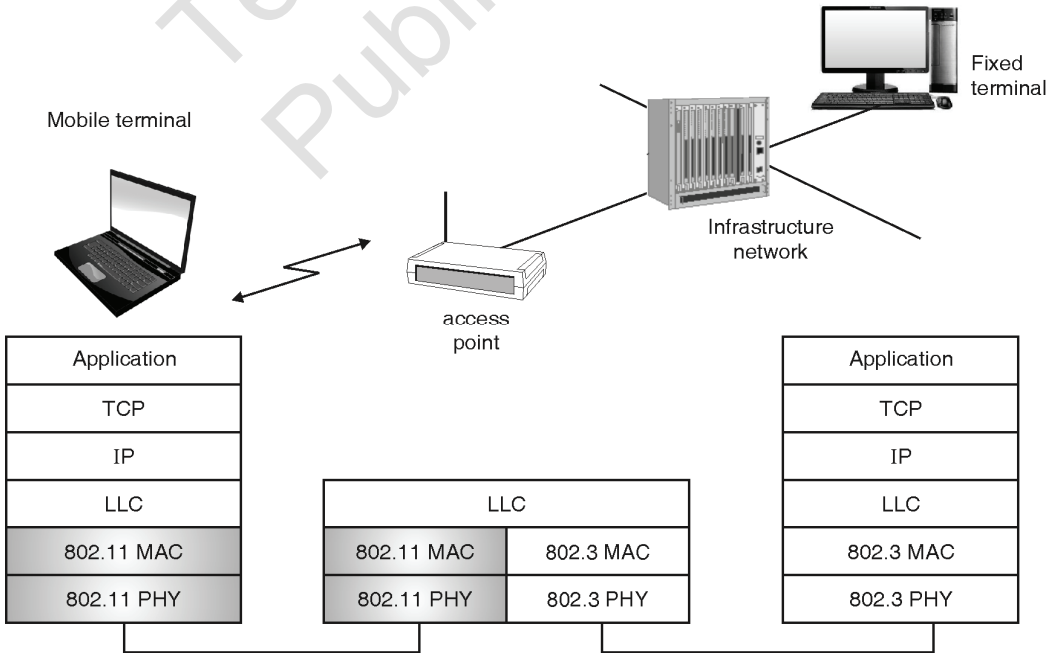


Fig. 4.2.3 : IEEE 802.11 protocol architecture and bridging

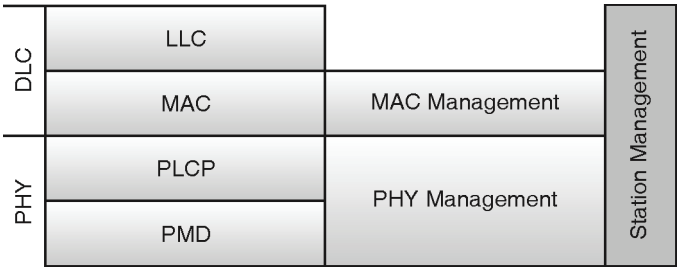


Fig. 4.2.4 : IEEE protocol architecture and management

Physical Layer

- The Physical layer (**PHY**) is subdivided into 2 parts :
  - Physical layer convergence protocol (PLCP) and
  - Physical medium dependent (PMD) sub layer.
- Protocol architecture is shown in Fig. 4.2.4 :
  - The **PLCP** sub layer provides
  - (a) A carrier sense signal, called clear channel assessment (CCA)
  - (b) A common PHY service access point (SAP)
  - The **PMD** sub layer handles
  - (a) Modulation
  - (b) Encoding/decoding of signals

MAC layer

The basic tasks of **MAC** layer :

(a) Medium access

(b) Fragmentation of user data

(c) Encryption of user data

MAC management

Tasks of MAC Management :

(a) Supports the association and re-association of a station to an access point

(b) Roaming between different access points

(c) Controls authentication mechanisms

(d) Encryption

(e) Synchronization of a station with regard to an access point

PHY management

Tasks of PHY management :

(a) Channel tuning

(b) Physical MIB maintenance

(c) Station management

4.2.3 IEEE 802.11 Physical Layer

In basic IEEE802.11 version three different physical layers have been standardized.

(a) DSSS Physical layer (DSSS-PHY)

(b) FHSS Physical layer (FHSS – PHY)

(c) Infra red Physical Layer

4.2.3(a) Direct Sequence Spread Spectrum Physical Layer (DSSS-PHY)

MU – Dec. 14

Q. Discuss the PHY frame format of an IEEE 802.11 using the spread spectrum technique, which separates by code. **(Dec. 14, 10 Marks)**

- This type of physical layer uses radio wave for transmission.
- As the name suggests, it uses direct sequence spread spectrum technique.
- IEEE 802.11 DSSS spreads the signal by using 11 bit barker code (+ 1, – 1, + 1, + 1, – 1, + 1, + 1, + 1, – 1, – 1, – 1).
- It also uses **2.4 GHz** ISM band (same as FHSS) and offers both 1 Mbit/s and 2 Mbit/s data rate.
- It uses Differential Binary Phase Shift Keying (DBPSK) for 1 Mbit/s transmission and Differential Quadrature Phase Shift Keying (DQPSK) for 2 Mbit/s.
- Maximum transmit power is 1W (in the US), 100mW EIRP in the Europe and 10mW/MHz in Japan.
- The symbol rate is 1 MHz and chipping rate is 11 MHz.
- Implementation is difficult.
- Provides a better coverage and a more stable signal (less interference and less multipath propagation).

Frame structure of DS-SS physical layer

- General packet sent over the channel consists of three parts : The PLCP preamble, The PLCP header and the Payload shown in Fig. 4.2.5.

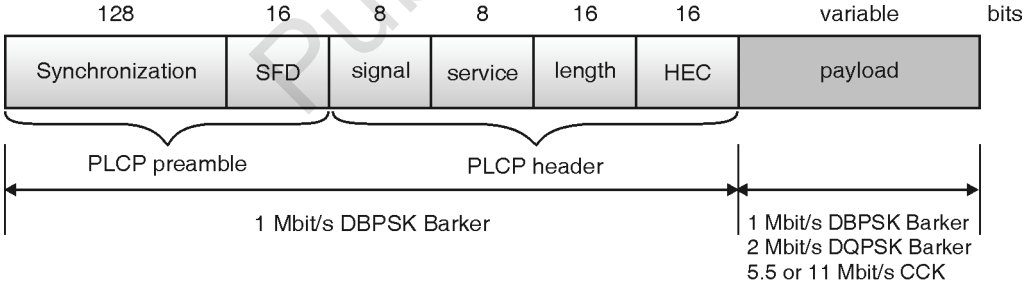


Fig. 4.2.5 : IEEE 802.11 DS-SS PLCP Physical layer packet format

- The DS-SS Physical layer PLCP packet format of IEEE 802.11 is shown in Fig. 4.2.5.
- The PLCP part is always transmitted at the rate of 1 Mbit/s.
- Payload can be transmitted at either 1 or 2 Mbit/s depending upon the modulation technique used.

The fields of a frame have the following functions.

- **Synchronization :** It is a 128 bit field (alternating 0 and 1) used for synchronization, gain setting, energy detection, and for frequency offset compensation.

- **Start frame delimiter (SDF) :** This field indicates the starting of a frame and consist the pattern 1111001110100000.
- **Signal :** This field indicates the data rate of the payload. The value 0x0A is for 1 Mbit/s and 0x14 is for 2 Mbits/s, other values are reserved for future use.
- **Service :** This field is reserved for future use.
- **Length :** This 16 bit field is used to indicate the length of a payload in microseconds.
- **Header Error Check (HEC) :** HEC is used to protect PLCP header.

– The PLCP part of the packet is followed by the payload carrying MAC packet data unit (MPDU) of the length between 1 to 2048 octets.

– Instead of 11–bit Barker code applied with DBPSK or DQPSK modulation, the Complementary Code Keying (CCK) can be used to achieve higher data rates of 5.5 or 11 Mbit/s.

– The DS-SS version of the physical layer ensures high data rate and high range, but is costlier than FH-SS technique due to the high cost of DS-RF components. More over DS-RF components also use more power.

4.2.3(b) Frequency Hopping Spread Spectrum Physical Layer (FHSS – PHY)

– This type of physical layer uses radio wave for transmission.

– As the name suggests, it uses frequency hopping spread spectrum.

– Compared to DS-SS physical layer, FH-SS physical layer provides high distortion immunity, high system capacity, low power use and uses low cost RF components.

– It also uses the **2.4 GHz** ISM band.

– Provides bandwidth of **1MHz**.

– It uses Gaussian Frequency Shift Keying (GFSK) for modulation.

– 2-level GFSK is used for 1 Mbit/s (1 bit is mapped on one frequency). 4-level GFSK is used for 2 Mbit/s (2 bits are mapped on one frequency).

– Operation at 1 Mbit/s is mandatory while at 2 Mbit/s is optional.

– 79 Hopping channels for North America and Europe and 23 hopping channels for Japan.

– Maximum transmit power is 1 W/MHz in US, 100 mW EIRP in Europe and 10mW/MHz in Japan.

– FHSS is easier to implement.

Frame structure of FH-SS Physical layer

– Fig. 4.2.6 shows the frame structure of the physical layer with FH-SS PHY.

– The frame consists of three basic parts : the PLCP preamble, PLCP header and the payload part.

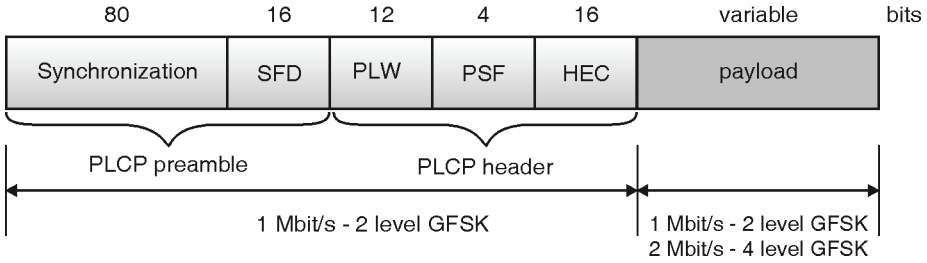


Fig. 4.2.6 : IEEE 802.11 FH-SS PLCP Physical layer packet format

The fields of a frame are as follows :

1. **Synchronization :** This pattern is used for the synchronization of the receivers and signal detection by the CCA (Clear Channel assessment). It is 80 bit field which is a 010101010…. Bit pattern.
2. **Start frame delimiter (SFD) :** This is a 16 bit field indicates the start of frame and provides frame synchronization. The pattern of SFD is 000011001011101.
3. **Packet length word (PLW) :** The 12 bit packet length width shows the length of the payload. The length of a packet could be up to 4k bytes.
4. **PLCP signaling field (PSF) :** 4 bit PSF field specifies the data rate of the payload following. If all bits are set to zero (0000) it means the lowest data rate (1 Mbit/s). 2 Mbit/s data rate is represented by 0010 bit sequence. Maximum data rate 8.5 Mbits/s is represented by 1111.
5. **Header error check (HEC) :** 16 bit HFC is added to protect the PLCP header. It can recover errors of up to 2 bits, otherwise identify whether PLCP bits are corrupted.

4.2.3(c) Infra Red Physical Layer

- The physical layer uses ***infra red*** for transmission.
- Digital signals are sent using infra red rays of the wave length 850-950nm range and Pulse Position Modulation (PPM).
- Two data rates, 1 and 2 Mbit/s have been standardized.
  - For 1 Mbit/s data rate, transmitted bits are grouped in 4-bit blocks and 16-PPM is applied.
  - For 2 Mbit/s, the data stream is divided into 2-bit blocks and 4-PPM is applied.

Frame structure of Infra red physical layer

The PLCP packet format of Infra red physical layer has been shown in Fig. 4.2.7.

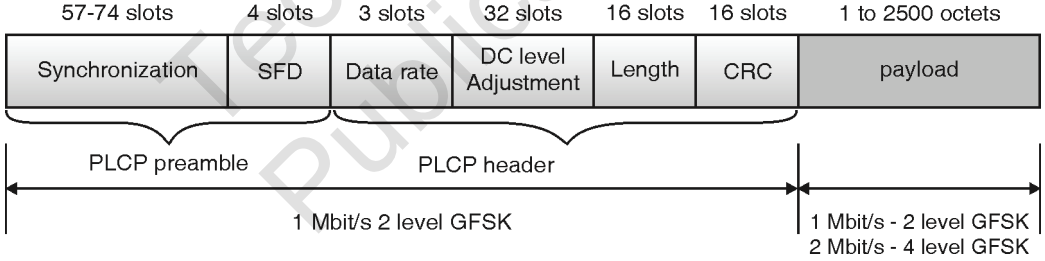


Fig. 4.2.7 : IEEE 802.11 Infrared PLCP Physical layer packet format

- Here the field **DC level adjustment** contains pattern which enables the receiving station to set the DC level of the signal.
- The IR interface is the cheapest of all 802.11 physical interfaces.
- It does not need any frequency regulations.
- It is resistant to eavesdropping. But it has lower coverage.
- As Infra red light interferes with other resources like sunlight or heat sources etc. such networks can only be used within buildings, e.g. classrooms, meeting hall, conference hall etc.
- Frequency reuse is very simple. The same frequency can be used in different classrooms.

4.2.4 IEEE 802.11 MAC Sublayer

MU – Dec. 16

Q.	Explain in Detail IEEE 802.11 MAC sublayer.	**(Dec. 16, 10 Marks)**

The MAC layer responsibilities are divided between MAC sub layer and MAC layer management sub layer.

- Responsibilities of MAC sub layer :
  - To handle access mechanism
  - Define addressing and frame format
- Responsibilities of MAC layer management sub layer :
  - Roaming in the DSS
  - Power management
  - Authentication
  - Security

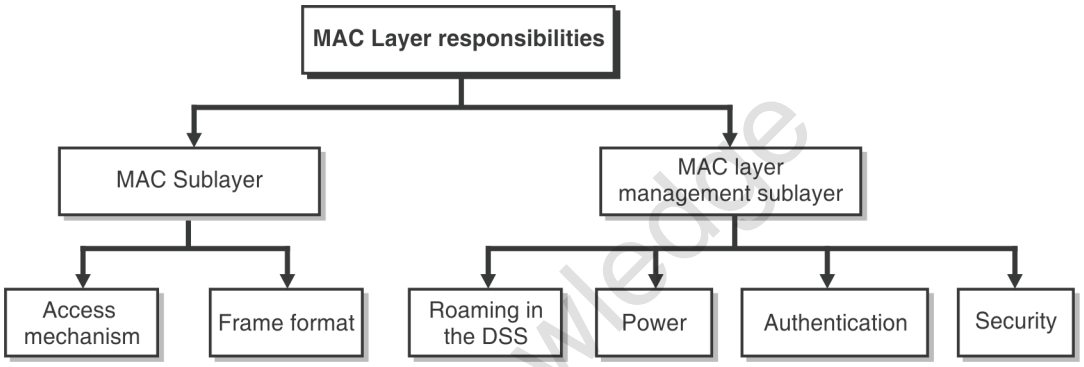


Fig. 4.2.8 : IEEE 802.11 MAC Layer Responsibilities

4.2.4(a) MAC Frame Format

MU – May 14

Q. Explain IEEE 802.11 MAC frame format in detail. **(May 14, 10 Marks)**

Fig. 4.2.9 shows the general MAC frame format of IEEE 802.11.

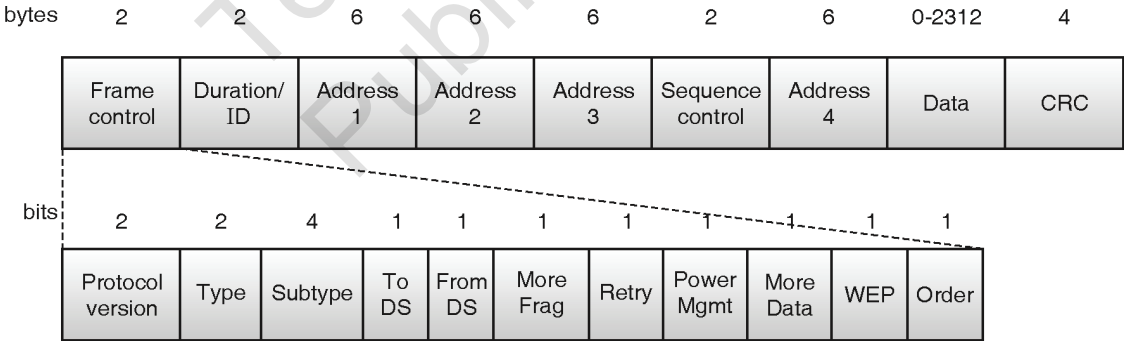


Fig. 4.2.9 : IEEE 802.11 MAC frame format

1. **Frame control :** This field carries the instructions on the nature of the packet. It distinguishes data from control and management frames. Frame control contains several sub-fields.
2. **Protocol version :** Shows the current protocol version and is fixed by 0.
3. **Type :** Determines the functions of a frame: management (00), control (01) and data (10). The value 11 is reserved.
4. **Subtype :** Values 0000 for association request, 1000 for beacon, 1011 for RTS control frame, 1100 is for CTS frame. User data transmits with 0000 subtype.
5. **To DS/From DS :** Used to control meaning of the address field in the MAC frame.

6. **More fragments :** Value 1 represents that there are more data or management fragments of the current MSDU to follow.
7. **Retry :** This field is set to 1 if the frame is the retransmission of previous frame.
8. **Power management :** Value 1 indicates the station goes in power save mode, 0 represents the station remains active.
9. **More data :** This field indicates a receiver that sender has more data to send than the current frame.
10. **Wired Equivalent Privacy (WEP) :** Indicates that the standard security mechanism of IEEE 802.11 is used.
11. **Order :** Value 1 indicates the received frames must be processed in strict order.
12. **Duration/ID :** This field is used to define the period of time in which the medium is occupied. This field is used to set NAV in RTS/CTS mechanism.
13. **Address 1 to 4 :** Four address fields (48 bits each) are used to identify the source, destination and access point to which they are connected.
14. **Sequence control :** Used for fragmentation numbering to control sequence numbering.
15. **Checksum :** Used to protect frame.

- MAC frames can be transmitted :
  - Between mobile stations
  - Between mobile station and access point
  - Between access points using DS
- The two bits within Frame Control field **To DS** and **From DS** differentiate these cases and define the four address fields.

  (i) **Address 1** identifies the physical receiver. Every station, access point or wireless node filters on address 1.

  (ii) **Address 2** represents the transmitter of a frame.

  (iii) **Address 3** and **Address 4** are mainly necessary for the logical assignment of frames.

Table 4.2.1: MAC addresses in IEEE 802.11

Scenario	To DS	from DS	address 1	address 2	address 3	address 4
Ad hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

Note : DS : Distribution System , AP : Access Point, DA : Destination Address, SA : Source Address BSSID : Basic Service Set Identifier, RA : Receiver Address, TA : Transmitter Address

MAC Control packets

Fig. 4.2.10 shows three different types of control packets : Acknowledgement packet, RTS, and CTS packet.

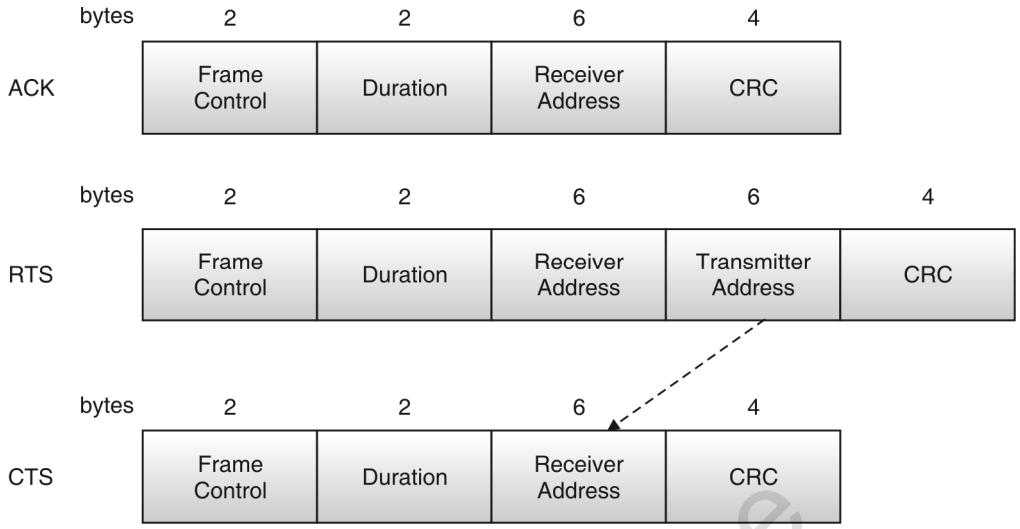


Fig. 4.2.10 : IEEE 802.11 special control packets ACK, RTS and CTS

- RTS packet contains the receiver address of the intended recipient and the transmitter address of the station transmitting the RTS.
- The duration specifies the time required to send CTS, data and its ACK plus three SIFS.
- The immediately following CTS frame copies the transmitter address from the RTS packet in to the receiver address field.

4.2.4(b) Access Mechanisms in IEEE 802.11

IEEE 802.11 offers two types of MAC services,

1. **DCF (Distributed Coordination Function) :** DCF offers only asynchronous data service and it includes two mechanisms.
   - **Contention** mechanism supported by CSMA/CA protocol.
   - **Contention free** mechanism by using RTS/CTS.

   It is mandatory service.
2. **PCF (Point Coordination Function) :** PCF offers asynchronous data service as well as time bounded service. It includes :
   - **Contention free** polling method. It is an optional service.
   - Ad hoc networks can offer only **asynchronous data services** (can only use DCF).
   - Infrastructure based networks can offer both **asynchronous (DCF)** as well as **time bounded services (PCF)**.
   - The MAC mechanisms collectively are also called Distributed Foundation Wireless Medium Access Control **(DFWMAC)**.

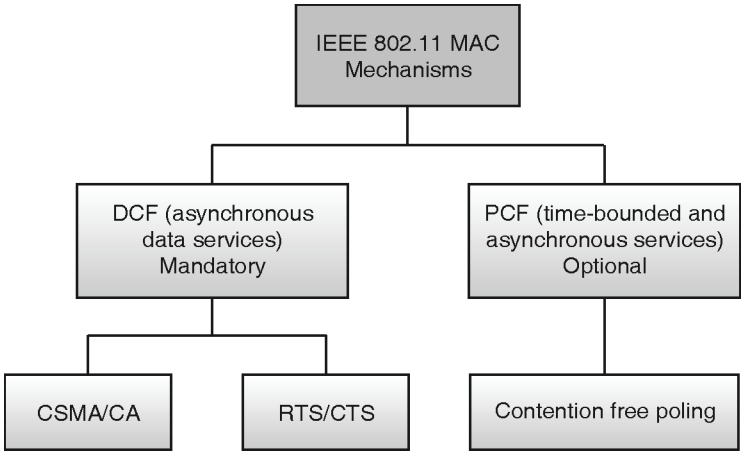


Fig. 4.2.11 : MAC mechanisms

Inter-Frame Spacing

- IEEE 802.11 offers three inter-frame spacing (IFS) between transmissions of frame.
- After completion of transmission, each station having a packet waits for one of the three IFS periods depending on the type of the packet.

(i) Short Inter-Frame Spacing (SIFS)

- This is the shortest waiting time for medium access.
- The higher priority packets such as short control messages, acknowledgement of data packets or polling responses have to wait for SIFS before medium access.

(ii) Distributed Coordinating Function IFS (DIFS)

- This denotes the longest waiting time and has the lowest priority for medium access.
- Lowest priority packets such as payload packets (packets containing data) have to wait for DIFS before the medium access.
- DIFS is a SIFS plus two slot times.

(iii) Point Coordinating Function IFS (PIFS)

- This is the waiting time between DIFS and SIFS.
- It is used by the access point.
- Before polling other nodes, the access point has to wait for PIFS time for medium access.

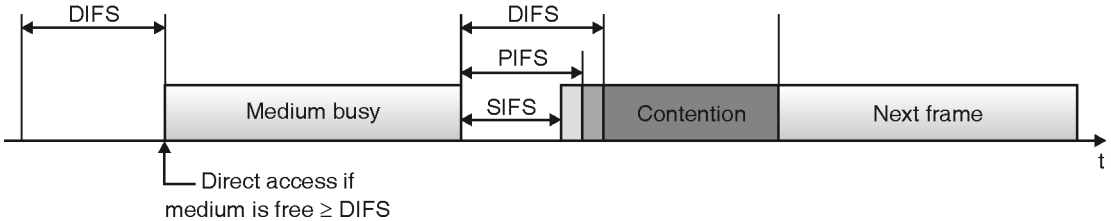


Fig. 4.2.12 : Medium access and inter-frame spacing

Basic DFWMAC-DCF using CSMA/CA

- It is a mandatory method and is used for only asynchronous data services.
- It is based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

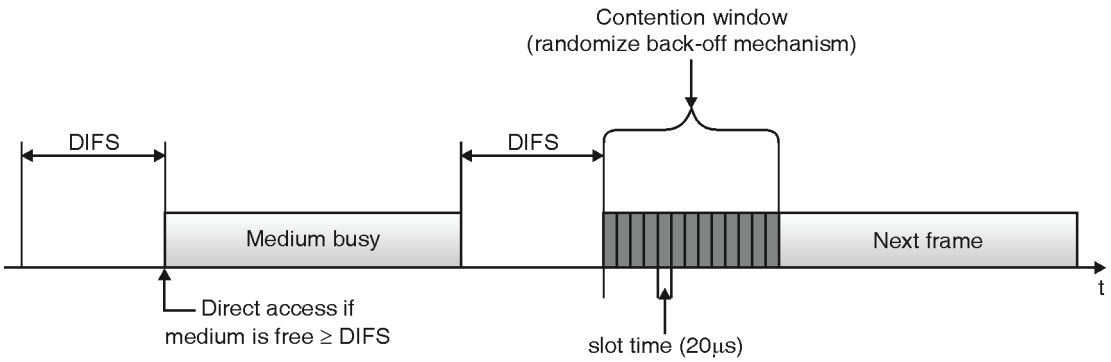


Fig. 4.2.13 : Contention window and waiting time

It works as follows

- If the medium is idle for at least DIFS time duration a node can access the medium.
- Node checks whether the medium is free or not with the help of the CCA (Clear Channel Assessment signal) in the PHY layer.
- If the medium is busy, then all the nodes wanting to access the medium wait until the medium becomes free.
- Once the medium is free, all the competing nodes wait for DIFS time period. After waiting for a DIFS time, competing nodes enter in **contention phase**.
- Now each node chooses a random back-off time within the contention window and does not try to access the medium for this random amount of time.
- Once the randomized waiting time for a node is over, the node continues to sense the medium. As soon as the node senses the channel is busy, it has lost this cycle and has to wait for a next chance i.e. until the medium becomes idle for at least DIFS time.
- But if the randomized additional waiting time for a node is over and the medium is still idle, the node can access the medium immediately and can start transferring data.
- To provide fair access mechanism, IEEE 802.11 adds a **back off timer.**
- Each station now chooses a back-off timer in the range of contention window.
- If a station does not get access to the medium in the first cycle, the back-off timer **is not cleared, instead it is just paused**.
- In the next contention cycle, the node does not choose a new random back-off time, the timer continues from where it was paused.
- Thus the stations that have waited for a longer time access the medium first.
- Fig. 4.2.14 shows unicast data transfer using DFWMAC-DCF.

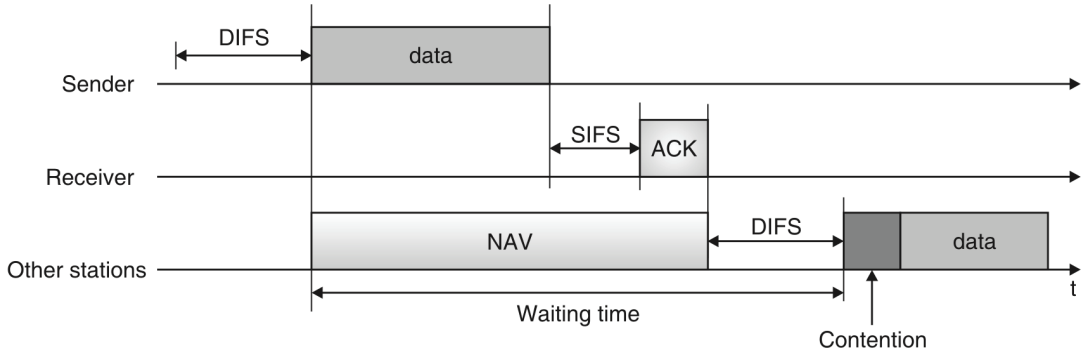


Fig. 4.2.14 : IEEE 802.11 unicast data transfer

- As shown in Fig. 4.2.14, the sender accesses the medium after waiting for DIFS time and transmits data.
- The other stations read the MAC frame and detect from the ***duration field*** how long the channel will be busy. Therefore they can set their NAV (Net allocation vector) for the appropriate time period.
- After waiting for SIFS the receiver acknowledges if the packet was received correctly.
- If no ACK is returned by the sender, after the timer expires, the sender retransmits that packet.
- The contention window starts after NAV + DIFS period. All other stations competing for the channel now choose a randomized back off timer after which they sense a channel.
- The station with the shortest back off time finds the channel idle and starts to transmit data.

DFWMAC-DCF with RTS/CTS extension

- To avoid hidden terminal problem, IEEE 802.11 defines RTS/CTS protocols. It works as follows.
- The process of unicast data transfer using RTS/CTS is illustrated in Fig. 4.2.15.
- If a terminal is willing to send data, after waiting for DIFS (plus a random backoff time if the medium was busy), it sends a short RTS control packet.
- The RTS packet contains the source address, destination address and the duration of the whole data transmission including the acknowledgement.
- All other nodes receiving RTS packets set their net allocation vector (NAV). NAV is set in accordance with the duration field specified in the RTS packet. These stations will not try to access the medium for this duration.
- The destination station responds to this packet by sending CTS control packet after an SIFS period.
- This CTS packet contains the duration field again and all stations receiving the CTS from the receiver of the data transmission set their NAV

Note : This is needed because the set of stations receiving RTS can be different from the set of stations receiving CTS, thus separate NAV has to be set by the receivers of RTS and the receivers of CTS).

- The source terminal receives the CTS and sends data after waiting for SIFS.
- The destination terminal sends ACK after another SIFS.
- After completion of transmission, NAV of each station terminated and channel is available for other users.

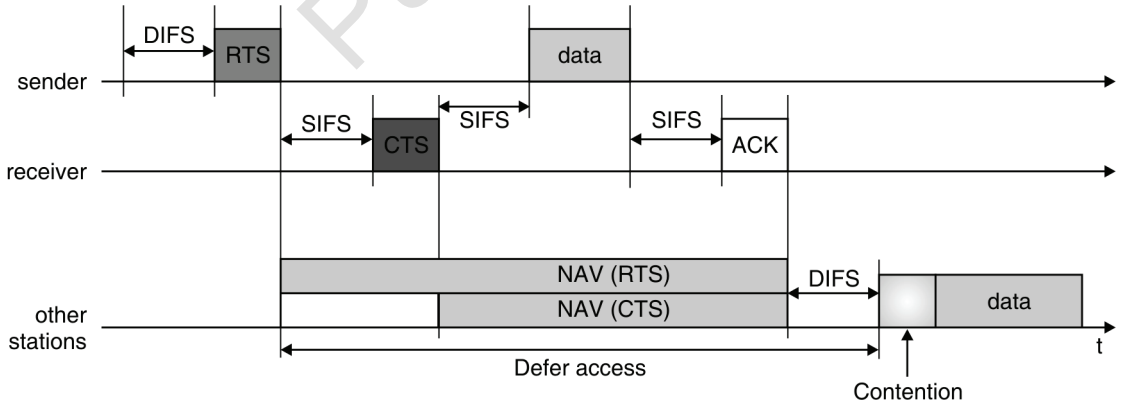


Fig. 4.2.15 : Implementation of RTS/CTS mechanisms in the IEEE 802.11

Fragmented mode of DFWMAC-DCF with RTS/CTS

- If we fragment the large frames (packets) into shorter frames then the **bit error rate** will remain the same but now short frames are destroyed and hence the **frame error rate** (rate of error per frame) decreases. Fig. 4.2.16 shows the fragmentation mode of RTS/CTS.

- Here the data frame is fragmented into smaller frames.
- Sender sends an RTS after waiting DIFS time. This RTS includes the duration for the transmission of the first fragment and the corresponding ack.
- Other stations receiving this RTS sets their NAV (for RTS) according to the duration specified in RTS.

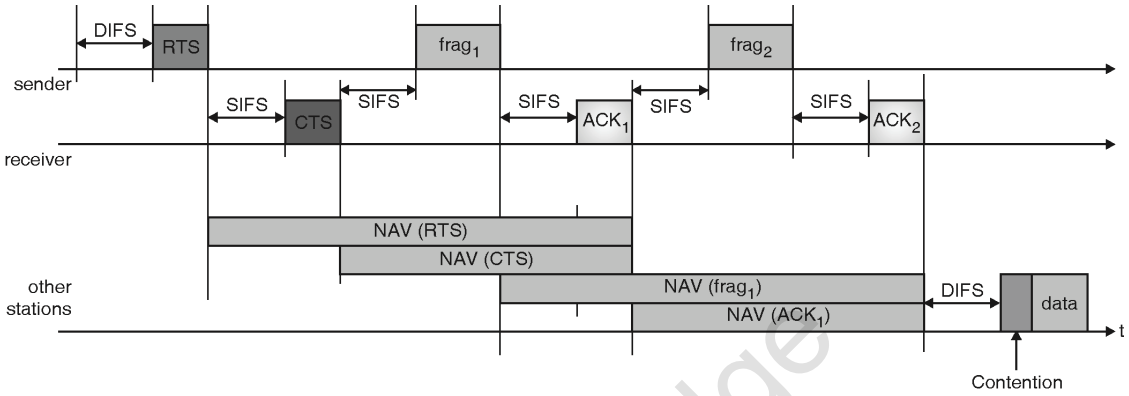


Fig. 4.2.16 : IEEE 802.11 fragmentations of data

- The receiver now answers with CTS, again including duration field.
- Receivers of CTS set their NAV (for CTS) according to the duration field.
- The sender can now send the first fragment (frag1) after waiting for SIFS time.
- The fragment 1 includes duration value. This duration field reserves the medium for the transmission of the following fragments (that is for second fragment and its ack).
- Again, all other stations receive this reservation and adjust their NAV (for frag1) accordingly.
- The receiver of frag1 sends ack for frag1 after waiting for SIFS time. This ack includes reservation for the next fragment.
- Other stations receiving this ack set their NAV for (ack1) accordingly.
- If the fragment is the last fragment then it does not reserve the medium (Duration field is empty) and the medium is now free for other stations.

DFWMAC-PCF with polling

- Point coordinating function (PCF) is used to provide time-bounded services.
- PCF requires an access point that controls the medium access and polls a single node.
- PCF operation is available only for infrastructure networks.

The PCF polling method works as follows

- Point coordinator in the access point splits the entire access time into super frame periods.
- A super frame contains a ***contention free period*** and a ***contention period***.
- Fig. 4.2.17 shows several wireless stations and their NAV.
- At time t_0 the contention-free period of a superframe should theoretically start but because the medium is busy it is postponed till t_1.
- After waiting for a PIFS time, the point coordinator (AP) sends D_1 data to poll first station. This station can reply once after SIFS.
- After waiting for SIFS time, the point coordinator sends D_2 data to poll second station. This station may answer by sending U_2 data after SIFS.

- The point coordinator now sends D_3 to poll third station. This time third station has nothing to send. The point coordinator will not receive anything after SIFS time.
- Now, the point coordinator can poll other stations after waiting PIFS time.
- The point coordinator can send end marker (CF_{end}) that indicates the end of contention-free period and the start of contention period.
- The contention period can be used for BASIC- DFWMAC or DWFMAC with RTS/CTS.
- Once the contention period is over (after t_3) the next superframe starts and the above process starts again.

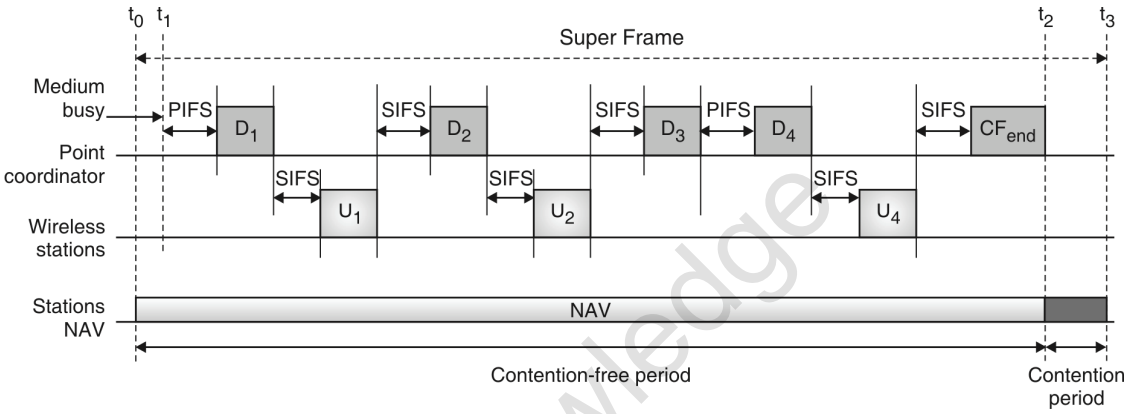


Fig. 4.2.17 : DFWMAC-PCF with polling

4.2.5 MAC Management

Following are the responsibilities of **MAC Management sub layer :**

(a) Synchronization

(b) Power Management

(c) Association/Reassociation

(d) MAC Management Information Base(MAC MIB)

4.2.5(a) Synchronization in IEEE 802.11

MU – May 15

Q. Explain synchronization in 802.11 MAC management layer for both infrastructure as well Ad-hoc WLANs. **(May 15, 10 Marks)**

- Each node of an IEEE 802.11 network maintains an internal clock.
- To synchronize the clocks of all nodes, IEEE 802.11 specifies a timing synchronization function (TSF).
- These synchronized clocks are needed for :
  - Power management
  - Coordination of the PCF
  - Synchronization in FHSS hopping sequence.

Synchronization process for infrastructure based networks

- In infrastructure based networks, an access point coordinates the synchronization process.

- The AP transmits a special frame called **beacon** periodically.
- A beacon frame consists of a time stamp and other management information used for power management and roaming.
- Other wireless nodes adjust their local clocks with beacon time stamp.
- The node is not required to hear every beacon to stay synchronized, however from time to time its clock should be adjusted.
- The transmission of the beacon is not always periodic. If the medium is busy, the access point postponed the transmission of the beacon frame.

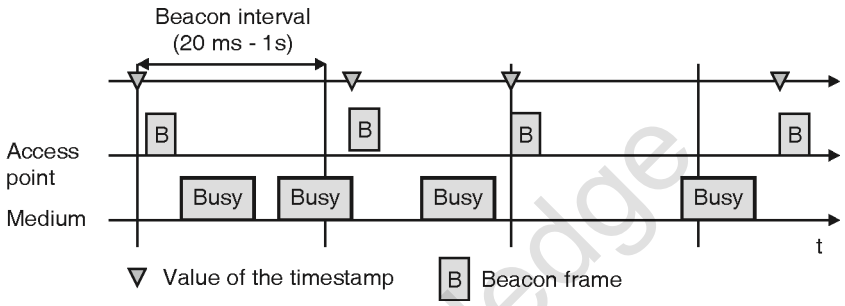


Fig. 4.2.18 : Beacon transmission in 802.11 infrastructure network

Synchronization process for ad-hoc networks

- As there is no access point in ad hoc network, each node within the network is responsible for the synchronization process.
- After each beacon interval, all stations choose random back-off time.
- Only one station whose random delay time is less becomes the winner and can send the beacon frame. All other stations adjust their local clock accordingly.

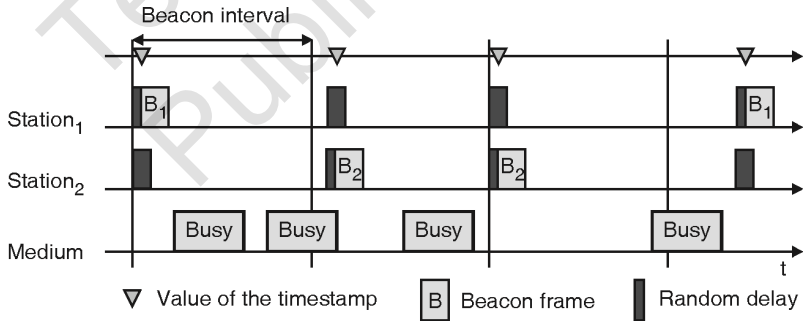


Fig. 4.2.19 : Beacon transmission in 802.11 ad-hoc networks

4.2.5(b) Power Management in IEEE 802.11

MU – May 12, Dec. 13, Dec.17

Q. Explain how the power management is done in IEEE 802.11 infrastructure based and ad-hoc networks. **(May 12, Dec. 13, Dec. 17, 10 Marks)**

- Since wireless devices are powered by battery; power saving is a big challenge in IEEE 802.11.
- The basic idea to save power in WLAN is to switch off the transceiver whenever it is not needed.
- Each station can be in one of the two states **(1) sleep (2) awake.**

- If a sender is willing to communicate with a power saving station (station in sleep mode) then the sender has to buffer data.
- The sleeping station awakes periodically and remains awaken for a certain period of time.
- During this time all stations announce destinations of their buffered data.
- If a station sees that it is a destination of a buffered data, then it stays awake until the transmission takes place.
- All stations should wakeup or be awake at the same time. For this, Time Synchronization Function (TSF) is used.

Power management in infrastructure based networks

- In infrastructure networks, an access point is responsible for the power management function.
- Access point buffers data packets for all sleeping stations.
- The access point transmits a Traffic Indication Map (TIM) with a beacon frame. TIM consists of a list of destinations of buffered data.
- Additionally, the access point also maintains a Delivery Traffic Indication Map (DTIM) interval. DTIM is used for sending broadcast/multicast frames.
- The DTIM interval is always a multiple of TIM intervals.

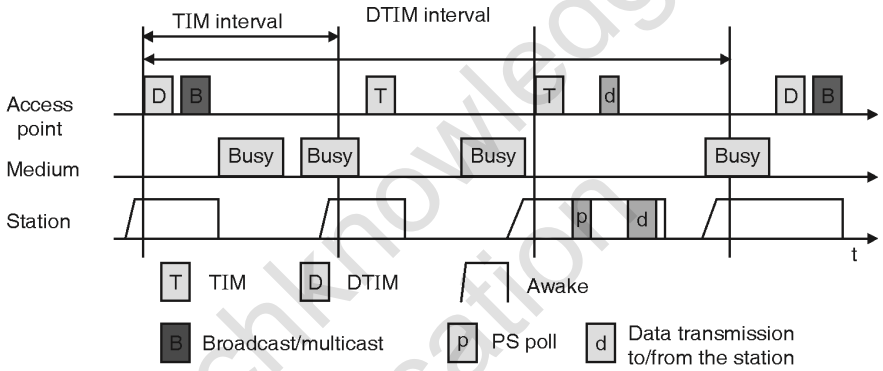


Fig. 4.2.20 : Power management in IEEE 802.11 infrastructure networks

- All stations wake up prior to an expected TIM and DTIM.
- As shown in Fig. 4.2.20, at the start of the DTIM interval, the access point has to transmit a broadcast frame. Therefore, the station stays awake until it receives that a broadcast frame.
- After receiving the broadcast frame, a station goes back to the sleep mode.
- The station wakes up again before the next TIM transmission. But the access point delays the transmission of the next TIM due to the busy medium, so the station stays awake.
- This time, the access point has nothing to send. Hence the station goes back to sleep after some time.
- At the next TIM, the access point indicates that the station is the destination of buffered data.
- The destination station replies by sending **PS** (power saving) **Poll.** And the station stays awake to receive that data.
- After receiving data, the station sends an acknowledgement or may send some data and goes back to sleep.
- In the next DTIM, the access point has more broadcast data to send and the station has to awake to receive that data.

Power management in ad-hoc networks

- In ad-hoc networks, power management is more difficult than in infrastructure networks because there is no access point to buffer data for power saving stations.
- Here, each station buffers data that it wants to send to power saving stations.
- In ad-hoc networks, all stations announce a list of buffered frame during a period when they are all awake.

- All stations announce destinations for which packets are buffered using ATIM (Ad-hoc traffic indication map) during the ATIM interval.
- As shown in Fig. 4.2.21 all stations awake at the same time and stay awake for ATIM interval.

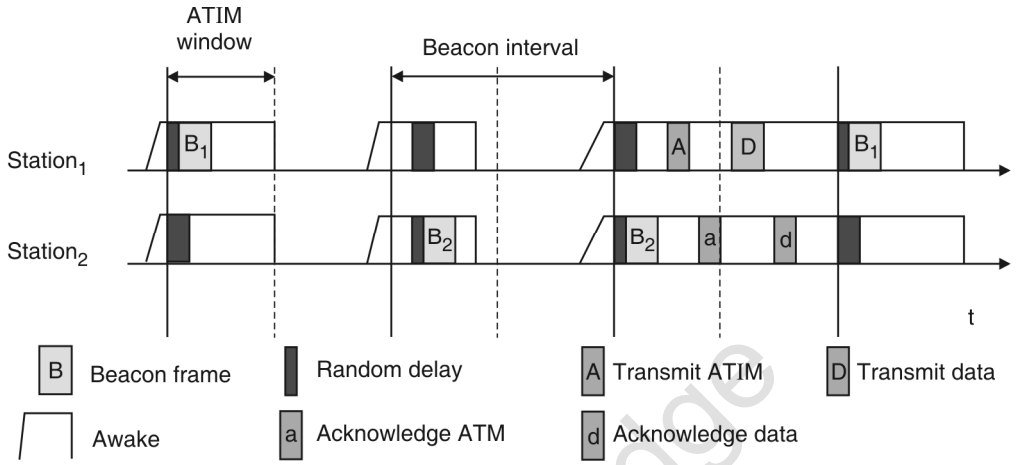


Fig. 4.2.21 : Power management in IEEE 802.11 ad-hoc networks

- In the first two ATIM intervals, stations have nothing to send, hence, stations stay awake for ATIM interval and later go back to sleep.

  In the third ATIM interval, station$_1$ has buffered data for station$_2$ hence station$_1$ sends ATIM (Shown as **A** in Fig. 4.2.21).
- Station$_2$ acknowledges this ATIM (Shown as **d** in Fig. 4.2.21) and stays awake for transmission. After the ATIM window, Station$_1$ can transmit buffered data (Shown as **D** in Fig. 4.2.21) and station$_2$ sends acknowledgement (shown as **d** in Fig. 4.2.21) or data (if it has) in reply.

4.2.5(c) Association/ Reassociation

1. Association

- Once authentication is completed, stations can associate with an access point (or reassociate with a new access point) to gain full access to the network.
- Association allows the distribution system to track the location of each mobile station.
- The basic procedure of association is shown in Fig 4.2.22.

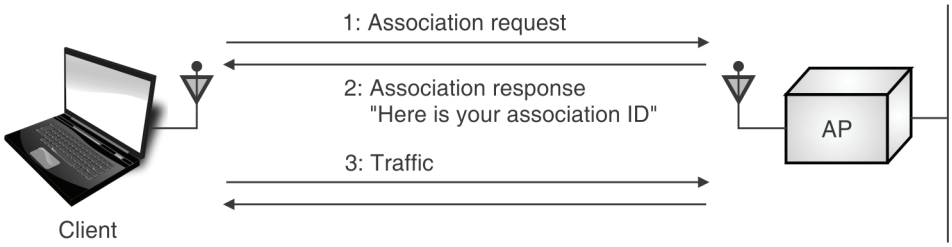


Fig. 4.2.22 : Association

Association Procedure :

(i) Once a mobile station has authenticated to an access point, it can issue an Association Request frame.

(ii) The access point then processes the association request.

(a) When the association request is granted, the access point responds with a status code of 0 (successful) and the Association ID (AID). The AID is a numerical identifier used to logically identify the mobile station to which buffered frames need to be delivered.

(b) Unsuccessful association requests include only a status code, and the procedure ends.

2. Reassociation

Reassociation is the process of moving an association from an old access point to a new one.

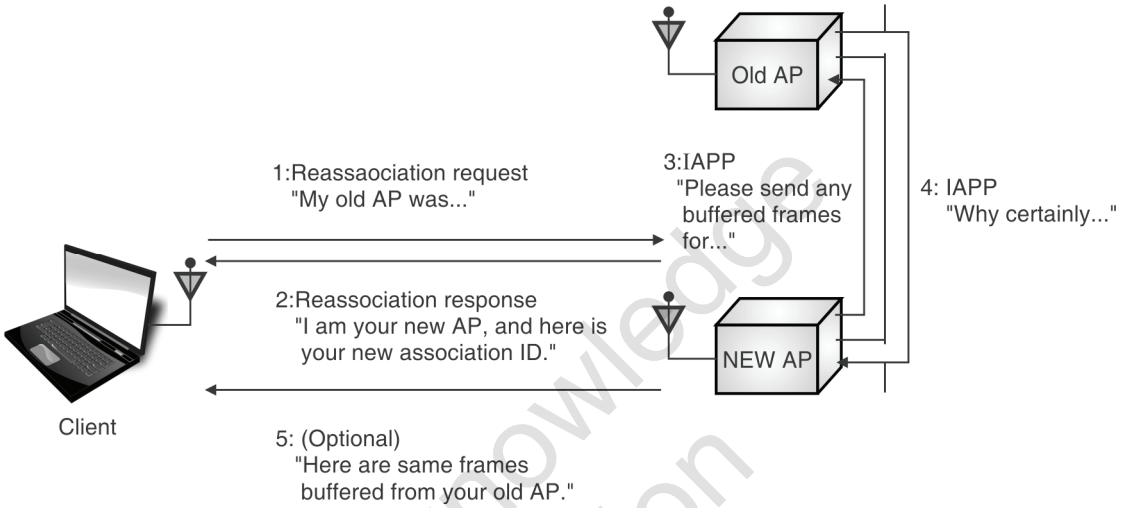


Fig. 4.2.23 : Reassociation procedure

Reassociation Procedure :

- The station monitors the quality of the signal it receives from that access point, as well as the signal quality from other access points in the same ESS.
- When the mobile station detects that it's receiving better signal from other access point, it initiates the reassociation procedure.

Fig. 4.2.23 depicts the following steps :

1. The mobile station issues a Reassociation Request to the new access point.
2. The new access point must communicate with the old access point to verify that the old access point authenticated the station. If the verification fails then the new access point responds with a Deauthentication frame and ends the procedure.
3. The access point processes the Reassociation Request. Processing Reassociation Requests is similar to processing Association Requests :
   (a) If the Reassociation Request is granted, the access point responds with a Status Code of 0 (successful) and the AID.
   (b) Unsuccessful Reassociation Requests include just a Status Code, and the procedure ends.
4. The new access point contacts the old access point to finish the reassociation procedure. This communication is part of the IAPP.
5. The old access point sends any buffered frames for the mobile station to the new access point.

6. The old access point terminates its association with the mobile station.

7. The new access point begins processing frames for the mobile station. When it receives a frame destined for the mobile station.

Roaming/ Scanning

When a mobile station moves from one access point to another access point then it has to associate with new access point for uninterrupted service, this moving between access points called roaming (Handoff). The steps for roaming handoff between access points are as follows (Refer Fig. 4.2.24) :

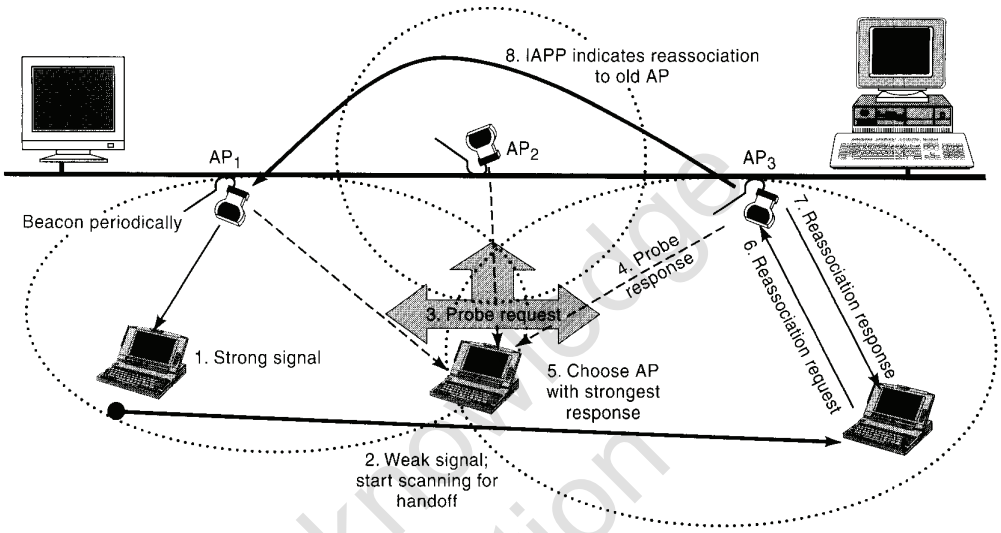


Fig. 4.2.24 : Roaming in IEEE 802.11 WLAN

- When station moves from one BSS to another its link quality from the access point AP_1 becomes poor. The station then starts scanning for another access point.
- Scanning involves search for another BSS or setting up new BSS in the case of ad-hoc networks. Scanning may be active or passive. In **Active scanning** station sends a **probe** on each channel and wait for a response. In **Passive scanning** the station listen to the medium i.e. station receives beacon signal of another network. Probe and beacon contains the necessary information to join the new access point.
- The station then select the best access point AP_3 with the strongest probe/ beacon signal strength, and send **reassociation request** to the selected access point.
- The new access point answers with **reassociation response.** If the response is successful, the station has roamed to the new access point.
- The new access point used IAPP (Inter Access Point Protocol) to inform to the old access point AP_1 about the change of access point.

4.2.5(d) MAC Management Information Base (MAC-MIB)

IEEE 802.11 Management Information Base (MIB) is a database used for managing the entities in a Wireless LAN. It can be construed as an SNMP Managed object with several configuration controls, option selectors, counters, and status indicators. These different attributes permit an external management agent to determine the status and configuration of an IEEE 802.11 station. The MIB in a station comprises separate sections for MAC and PHY.

4.2.6 IEEE 802.11a

- It operates at **5 GHz** frequency band.
- It offers maximum data rate of **54 Mbits/s**.
- Uses **OFDM** (Orthogonal FDM) modulation scheme for achieving such a high data rate.
- Transmission range is 100m outdoor, 10m indoor.
- Here too, all the MAC schemes and management procedures are same as that of the original IEEE 802.11.
- The heart of the system is its modulation schemes and coding schemes.
- To offer high data rate, the system uses **52 sub carriers** that are modulated using various modulation schemes like BPSK, QPSK, 16-QAM and 64-QAM.
- To mitigate transmission errors, it uses **FEC** (Forward Error Correction coding) using coding rate of 1/2, 2/3 or 3/4.
- Using various combination of modulation (BPSK, QPSK etc.) and coding schemes it achieves various data rates such as 6, 9, 12, 18, 24, 36, 48 and 54 Mbits/s.

Usage of OFDM in IEEE802.11a

- The basic idea of OFDM is the reduction of the symbol rate by distributing bits over numerous subcarriers.
- IEEE 802.11a uses fixed symbol rate of 250,000 symbols per second independent of the data rate.

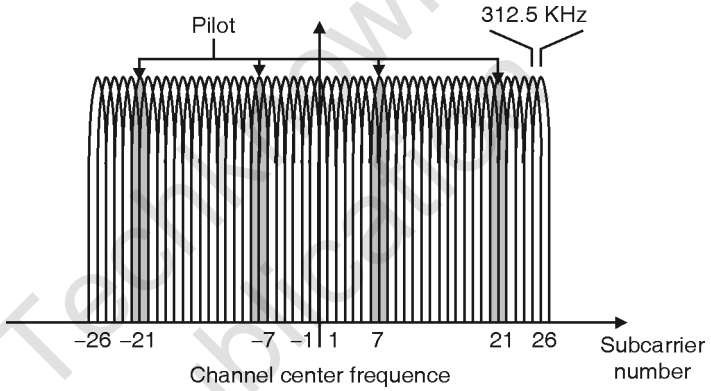


Fig. 4.2.25 : Usage of OFDM in IEEE 802.11a

- Fig. 4.2.25 shows 52 subcarriers equally spaced around a centre frequency. The spacing between the subcarriers is 312.5 KHz.
- The center frequency itself is not used as a sub carrier. Subcarriers numbered -21,-7, 7, 21 are used for pilot signals to make the signal selection robust against frequency offset.
- Compared to IEEE 802.11b that operates in 2.4 GHz the IEEE802.11a offers higher data rate and more coverage, however shading at 5GHz is much more severe compared to 2.4 GHz.

4.2.7 802.11b

- Unlike IEEE 802.11a, IEEE 802.11b operates at 2.4 GHz.
- It provides raw data rates up to 11 Mbps.
- It provides a wireless range of roughly 35 meters indoors and 140 meters outdoors.
- It uses the CSMA/CA technique.
- The RF signal format used for 802.11b is CCK or complementary Code Keying.

– IEEE 802.11b supports Adaptive Rate selection. The system monitors the signal quality. If the signal falls or interference levels rise, then system adopt a slower data rate with more error correction. The system will first fall back to a rate of 5.5 Mbps, then 2, and finally 1 Mbps. This scheme is known as Adaptive Rate Selection (ARS).

4.2.8 Comparison of Various IEEE 802.11x Standards

MU – Dec. 15

Q. Compare various IEEE 802.11x standards. **(Dec. 15, 10 Marks)**

Parameters	IEEE 802.11	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
Operates at	2.4GHz	5GHz	2.4GHz	2.4 GHz	5 GHz or 2.4 GHz
Maximum data rate	2 Mbps	54 Mbps	11 Mbps	54 Mbps	300 Mbps
Modulation	DSSS, FHSS	OFDM	DSSS or CCK	DSSS or CCK or OFDM	DSSS or CCK or OFDM
Channel width	20 MHz	20 MHz	20 MHz	20 MHz	20 MHz or 40 MHz
Typical range	66 feet	75 feet	100 feet	150 feet	150 feet
Antenna configuration	1x1 SISO	1x1 SISO	1x1 SISO	1x1 SISO(Single Input-Single Output)	4x4 MIMO (Multiple Input-Multiple Output)

IEEE 802.11 is mainly designed for enhanced security purposes. It addresses two main weaknesses of wireless security networks which are encryption and authentication. Encryption is accomplished by replacing WEP's original PRNG RC4 algorithm by stronger cipher that performs three steps on every block of data. The authentication and key management is accomplished by the IEEE 802.1x standard.

4.3 Wi-Fi Security Standards

– Since wireless networks transmit data over radio waves, it is easy to intercept data or "eavesdrop" on wireless data transmissions.

– Several Wi-Fi security algorithms have been developed since the inception of Wi-Fi.

– The wireless security protocols prevent unwanted parties from connecting to your wireless network and also encrypt your private data sent over the airwaves.

– Different types of wireless security protocols have been discussed below.

4.3.1 WEP – Wired Equivalent Privacy

– WEP stands for 'Wired Equivalent Privacy'.

– WEP is specified by IEEE 802.11 for encryption and authentication of Wi-Fi networks.

– It operates at physical and data link layer.

– The goal of WEP is to make wireless networks as secure as wired networks.

– WEP is having two main parts. Authentication and Encryption.

(i) WEP Authentication

– Fig. 4.3.1 shows an example of WEP authentication:

Fig. 4.3.1 : WEP authentication

- First a requesting station sends an Authentication Request to the access point (AP).
- On receiving the request, the AP, replies with a 128 byte random challenge text generated by WEP algorithm.
- The requesting node then copies the text into the authentication frame and encrypts it with a shared key , and then sends the frame back to the AP.
- The AP then will decrypt the value of the challenging text using the same shared key and compare it to the challenging text sent earlier.
- If match occurs, the AP will reply with a positive authentication indicating a successful authentication.
- If there is not a match, the AP will send back a negative authentication.

(ii) WEP Encryption

Encryption process

- WEP uses RC4 encryption which is a symmetric stream cipher to provide confidentiality.
- The 40-bit secret key is connected with a 24-bit Initialization vector (IV) resulting in a total 64 –bit key(shown as a seed in Fig. 4.3.2).
- The resulting key (seed) is the input for the Pseudo Random Number Generator (PRNG). The PRNG (RC4) outputs a pseudo random key sequence based on the input key.
- The resulting sequence is used to encrypt the data by doing a bitwise XOR.

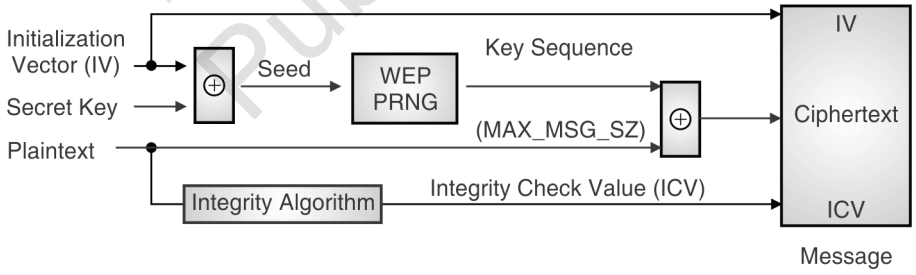


Fig. 4.3.2 : WEP Encryption

- The result is encrypted bytes equal in length to the number of data bytes that are to be transmitted in the expanded data plus four bytes. This is because the key sequence is used to protect the 32-bit Integrity Check Value(ICV) as well as the data.
- Fig. 4.3.2 shows the encryption algorithm and Fig. 4.3.3 shows the decryption algorithm.
- To prevent unauthorized data modification an integrity algorithm, CRC-32 operates on the plain text to produce ICV.
- The output of the whole process is a message containing three parts: the resulting ciphertext, the IV, and the ICV.

Decryption process

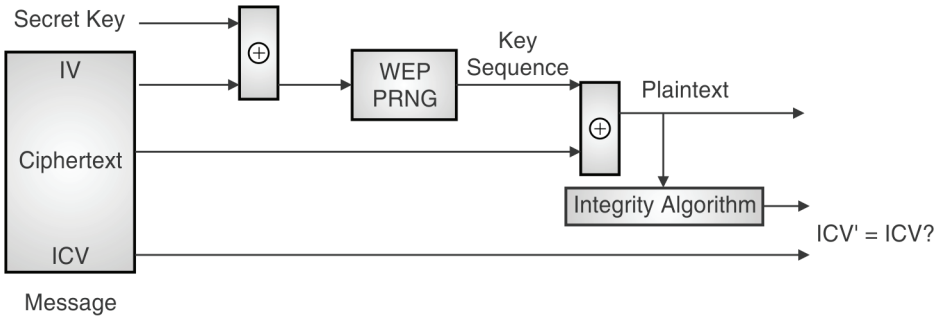


Fig. 4.3.3 : WEP Decryption

- The incoming message has three parts: Ciphertext, IV and ICV.
- The IV of the incoming message is used to generate the key sequence to decrypt the incoming message.
- Combining the ciphertext with the proper key sequence will give the original plaintext and ICV.
- The decryption is verified by performing integrity check algorithm on the recovered plain text and comparing the output of the ICV' (Calculated ICV) to the ICV submitted with the message. If calculated ICV (ICV') is not same as ICV , the received message is in error.

WEP vulnerabilities

Although WEP attempts to achieve wired equivalent security, there are still many weaknesses in WEP which may be used by the malicious user to compromise the security of WLAN.

(i) The IV is too small and in clear text.

Initial Vector used in WEP is 24-bit field sent in the clear text portion of a message. This 24-bit string, used to initialize the key stream generated by the RC4 algorithm, is a relatively small field when used for cryptographic purposes.

(ii) The IV is static.

The same IV is used to produce the key every time. Reuse of the same IV may produce identical key streams and since IV is short, it guarantees that those streams will repeat after a relatively short time.

(iii) The IV makes the key stream vulnerable.

The 802.11 standard does not specify how the IVs are set or changed, and individual wireless adapters from the same vendor may all generate the same IV sequences, or some wireless adapters may possibly use a constant IV. As a result, hackers can record network traffic, determine the key stream, and use it to decrypt the cipher text.

(iv) WEP provides no cryptographic integrity protection.

The combination of non-cryptographic checksums with stream ciphers is dangerous - and often introduces vulnerabilities. T

(v) WEP Uses Stream Cipher.

The basic problem with WEP is that it uses a stream-cipher known as RC4 in synchronous mode for encrypting data packets. Using the synchronous stream ciphers, the loss of a single bit of a data stream causes the loss of all data following the lost bit. Thus the stream cipher is not suitable for wireless medium where placket loss is widespread.

4.3.2 WPA

- WPA stands for "Wi-Fi Protected Access".
- WPA was developed by the Wi-Fi Alliance to provide better user authentication than Wired Equivalent Privacy (WEP),
- One major improvement in WPA over WEP is the Temporal Key Integrity Protocol (TKIP), which dynamically changes keys as the system is used.

- It uses RC4 stream cipher with a 128 bit key and a 48 bit IV. The longer key and IV together defeat the key recovery attacks on WEP.
- In addition to authentication and encryption, WPA also provides vastly improved payload integrity.
- The cyclic redundancy check (CRC) used in WEP is insecure; it is possible to alter the payload and update the message CRC without knowing the WEP key.
- WPA uses a solution called Michael, which is a Message Integrity Check (MIC), to the checksum being corrupted issue. WPA uses a 32 bit Integrity Check Value (ICV). This is inserted after payload and before IV. The MIC includes a frame counter, which helps to prevent replay attacks.

WPA Modes

WPA supports two modes of operation.

1. Pre-Shared Key Mode or Personal Mode

This mode is used for personal use. The preshared mode does not require authentication server. It utilizes a shared key that is communicated to both sides (AP and client) before establishing a wireless connection; this key is then used to secure the traffic.

2. Enterprise Mode

Enterprise Mode requires an authentication server. It uses more stringent 802.1x authentication with the Extensible Authentication Protocol (EAP). It Uses RADIUS protocols for authentication and key distribution. In this mode, the user credentials are managed centrally.

WPA2 vs. WPA and WEP

- Among all three wireless LAN security protocols, WEP is the least secure which provides security equal to that of a wired connection.
- WEP broadcasts messages using radio waves and is much easier to crack. This is because it uses the same encryption for every data packet. If enough data is analyzed by an eavesdropper, the key can be easily found with automated software.
- WPA improves on WEP by using the TKIP encryption scheme to scramble the encryption key and verify that it hasn't been altered during the data transfer.
- Further, WPA2 improves the security of a network by using stronger encryption method called AES.

4.3.3 Wireless LAN threats

There are a number of threats that exist to wireless LANS, these include:

- Rogue Access Points/Ad-Hoc Networks
- Evil Twin APs
- Denial of Service
- Configuration Problems also called Mis-Configurations or Incomplete Configurations
- Passive Capturing
- Misbehaving Clients

1. Rogue Access Points/Ad-Hoc Networks

- One way that is the attackers target wireless LANs is by setting up a rogue access point.
- A rogue access point (AP) is a wireless AP that has been installed on a secured network without any authorization from the network administrator.
- The idea is to 'fool' some of the legitimate devices and to make them connect to the rogue access point.

2. Evil Twin Aps

- In this type of attack, the fraudulent AP advertises the same network name (SSID) as a legitimate WLAN, causing nearby Wi-Fi clients to connect to them.
- The only effective defense against Evil Twins is server authentication from 802.1X.

3. Denial of Service

- This is the most common and simplest attack. It can cripple or disable a wireless network by limiting the access to the services.
- This can be done by simply sending a large amount of traffic at a specific target.
- Here the amount of traffic generated to affect a target device is much higher than the capabilities of a target machine.
- A denial of service attack can also be used in conjunction with a rogue access point. For example, a rogue access point could be setup in a channel that is not used by the legitimate access point. Then the denial of service attack could be launched at the channel currently being used causing endpoint devices to try to re-associate onto a different channel which is used by the rogue access point.

4. Configuration Problems

- Simple configuration problems are often the cause of many vulnerabilities. A novice user can set up one of these devices quickly and gain access. However, they also open up their network to external use without further configuration.
- Other issues with configuration include weak passphrases, weak security algorithm deployments (i.e. WEP vs WPA vs WPA2), and default SSID usage.

5. Passive Capturing

- Passive capturing is performed by simply getting within the range of a target wireless LAN and then listening and capturing data.
- This information can be used for a number of things including attempting to break existing security settings and analyzing non-secured traffic.
- It is almost impossible to really prevent this type of attack because of the nature of a wireless network; what can be done is to implement high security standards using complex parameters.

6. Misbehaving Clients

- Sometimes clients form unauthorized Wi-Fi connections accidentally or intentionally. By doing this, they put themselves and corporate data at risk.
- Some enterprises use Group Policy Objects to configure authorized Wi-Fi connections and prevent end-user changes. Others use host-resident agents to monitor Wi-Fi client activity and disconnect high-risk connections.

4.3.4 Securing Wireless Network

The following are some of the ways by which you can secure wireless network.

1. Use an inconspicuous network name (SSID)

- The Service Set Identifier (SSID) is one of the most basic Wi-Fi network settings. Avoid using too common SSID, like “wireless” or the vendor’s default name.
- This can make it easier for someone to crack the personal mode of WPA security.

2. Use Enterprise WPA2 with 802.1X authentication

- Use enterprise mode of Wi-Fi security, because it authenticates every user individually - Everyone can have their own Wi-Fi username and password. So if a laptop or mobile device is lost or stolen, or an employee leaves the company, all you have to do is change or revoke that particular user's log-ins.
- In contrast, in personal mode, all users share the same Wi-FI password, so when devices go missing or employees leave you have to change the password on every single device.
- Another advantage of enterprise mode is that every user is assigned his or her own encryption key. That means users can only decrypt data traffic for their own connection — no snooping on anyone else's wireless traffic.

3. Use firewalls to secure your Wi-fi network

- Use A hardware firewall. A hardware firewall does the same thing as a software one, but it adds one extra layer of security.
- The best part about hardware firewalls is that most of the best wireless routers have a built-in firewall that should protect your network from potential cyber attacks.
- If your router doesn't have one, you can install a good firewall device to your router in order to protect your system from malicious hacking attempts against your home network.

4. Restrict access

Only allow authorized users to access your network. Each piece of hardware connected to a network has a media access control (MAC) address. You can restrict access to your network by filtering these MAC addresses.

5. Encrypt the data on your network

Use strong encryption algorithm to encrypt data. There are several encryption protocols available to provide this protection. Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and WPA2 encrypt information being transmitted between wireless routers and wireless devices. WPA2 is currently the strongest encryption.

6. Maintain antivirus software

Install antivirus software and keep the virus definitions up-to-date. Many antivirus programs also have additional features that detect or protect against spyware and adware.

7. Use file sharing with caution

File sharing between devices should be disabled when not needed. Allow file sharing over home or work networks, never on public networks. Create a dedicated directory for file sharing and restrict access to all other directories. Anything that is been shared should be password protected.

8. Keep your access point software patched and up-to-date

The manufacturer of your wireless access point periodically release updates. Update access point software website regularly.

9. Connect using a virtual private network

Many companies and organizations have a Virtual Private Network (VPN). VPNs allow employees to connect securely to their network when away from the office. VPNs encrypt connections at the sending and receiving ends and keep out traffic that is not properly encrypted.

4.4 HIPERLAN Standards

- There are two main standard families which are used for Wireless LAN :

(i) IEEE 802.11 (802.11b, 802.11a, 802.11g...)

(ii) ETSI HIPERLAN (HIPERLAN Type 1, Type 2, HiperAccess, HiperLink)

- HIPERLAN is a European (ETSI) standardization initiative for a High Performance Wireless Local Area Network.
- ETSI defined four types of HIPERLANs: HIPERLAN/1, HIPERLAN/2, HIPERACCESS and HIPERLINK.

4.4.1 HIPERLAN T-1

MU – May 12

Q. Write a short note on HIPERLAN. **(May 12, 5 Marks)**

- HIPERLAN-1 operates in the dedicated bandwidth **5.15 to 5.3 GHz** divided into 5 fixed channels.
- It supports data rate up to **23.5 Mbps** with coverage of 50m.
- HIPERLAN-1 terminals can move at the maximum speed of **1.4m/s**.
- It supports both **infrastructure based** and **ad-hoc networks**.
- It supports packet oriented structure and uses a variant of **CSMA/CA protocol**.
- Supports asynchronous as well as isochronous traffic.
- The protocol includes optional pre-session encryption and power saving mechanism.
- Fig. 4.4.1 presents the HIPERLAN-1 reference layer model (Protocol stack). Fig. 4.4.2 shows the HIPERLAN communication model.

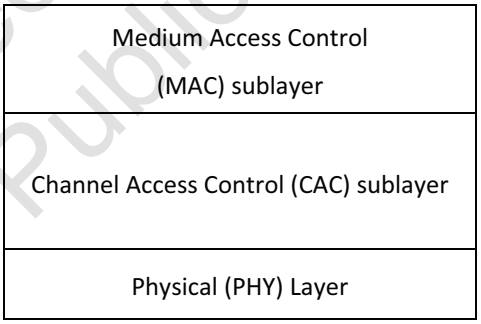


Fig. 4.4.1 : HIPERLAN -1 protocol stack

- The MAC layer receives MAC service data units (MSDU) form the higher layers through MAC service access point.
- It processes MSDU and generates HMPDU (HIPERLAN MAC Protocol Data Unit)
- This HMPDU then enters HIPERLAN CAC layer through a HIPERLAN–CAC service access point (HCSAP).
- The Channel Access Control (CAC) sub layer determines which nodes are allowed to transmit and specifies the access priorities.
- This layer offers a ***connection less service*** to the MAC sub layer.
- CAC protocol processes the HMPDU and produce HCPDU (HIPERLAN-CAC Protocol Data Unit) which finally constitute a payload of a physical data burst.

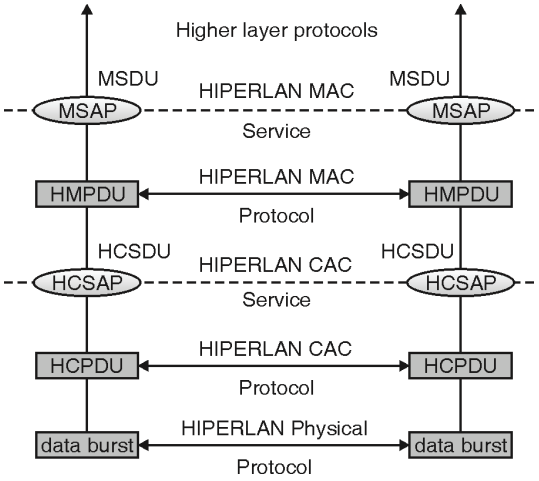


Fig. 4.4.2 : HIPERLAN Communication model

4.4.1(a) HIPERLAN-1 MAC Sublayer

MU – May 18

Q. Explain HIPERLAN 1 MAC Layer. **(May 18, 10 Marks)**

MAC sublayer functions are listed below.

1. MAC address mapping

- The standard defines internal address structure.
- The address of a HIPERLAN terminal contains two parts. The first part defines the network name and the second part determines the station.

2. Security

- To ensure communication security, the Encryption/Decryption algorithms are used.
- The algorithm requires an identification key and a common initialization vector for data encryption and decryption.
- The pseudorandom generator accepts the identification key and the initial vector and generates a sequence.
- The modulo-2 addition is performed on the sequence of user data and the sequence generated by the pseudorandom generator.
- Initialization vectors and identification keys can be frequently changed in order to achieve high security.

3. Addressing of MAC service access point (MSAP)

MSAP are addressed using 48 bit LAN-MAC address which are compatible to IEEE 802.x LANs.

4. Data forwarding

- The appealing feature of HIPERLAN/1 is ability to forward data packets using several relays. Relays can extend the communication on the MAC layer beyond the radio range.
- The forwarding can be of two types-point-point (unicast) or point-multipoint (multicast/broadcast).
- Each relay station maintains a routing table and a list of multipoint relays.

5. Power saving

Switch off terminals whenever they are not in use or keep in sleep mode when they don't have data to send.

4.4.1(b) HIPERLAN-1 CAC Layer

Functions of Channel Access Control (CAC) sub layer are listed below :

- Assures that terminal does not access illegal channels.
- Defines how a given channel can be accessed.
- Defines the priority scheme. It uses EY-NPMA (**E**limination **Y**ield **N**on-preemptive **P**riority **M**ultiple **A**ccess). EY-NPMA supports both asynchronous and isochronous (voice-oriented) transmission. EY-NPMA enables network to function with few collisions.
- Provides five priority levels for QoS supports. The mapping of a QoS on a priority level is done with the help of packet life time.
- Provides hierarchical independence with EY-NPMA.

EY-NPMA

- The most important part of CAC sub layer is the Elimination Yield Preemptive Priority Multiple Access (EY- NPMA) protocol.
- It is a variant of CSMA protocol with prioritization.
- It divides the medium access of different competing nodes into three phases.

1. Prioritization 2. Contention 3. Transmission

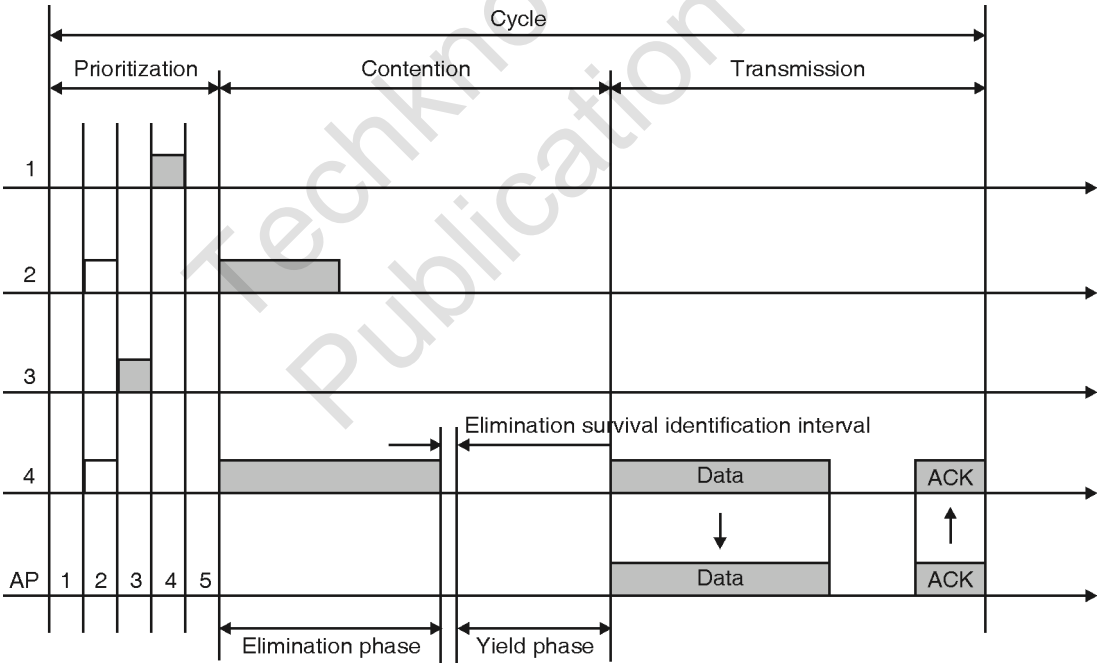


Fig. 4.4.3 : EY-NPMA protocol (Channel access cycle)

1. Prioritization

- Time is divided into channel access cycles. Each cycle starts with the channel access synchronization.
- The synchronization is followed by the prioritization phase. This phase contains five 168-bit slots starting from the slot of highest priority (p=1).
- If the terminal has the priority, *p* it senses the channel for the first (*p*-1) slots.
- If the channel remains idle, the node sends an access pattern.

- If the node finds that the channel is busy, it waits for the beginning of the next access cycle.
- More than one station can have the same priority.
- So, next contention phase is carried out to resolve contention problem.

2. Contention

- This phase is further divided into two phases : Elimination phase and Yield phase.
- The **elimination phase** is divided into 0-12 slots. Each terminal which has not been eliminated in the prioritization phase sends the elimination burst. The length of this burst is random between 0 to 12.
- After sending an elimination burst, each station senses the channel during elimination survival verification interval.
- A station gives up if the channel is occupied by some other station during this interval.
- The **yield phase** contains ten 168-bit slots. Each station senses channel during *n* slots (0-9).
- The probability that the given station senses the channel for *n* consecutive slots is 1/10.

3. Transmission

- If the station does not detect any activity in the channel during listening, it immediately starts transmitting and enters transmission phase.
- If the station has detected that the channel is busy, it has lost its cycle and waits till the beginning of the next access cycle.

4.4.1(c) HIPERLAN-1 Physical Layer

MU – May 16

Q. Explain in detail HIPERLAN-1 physical layer. **(May 16, 10 Marks)**

Functions of the physical layer of HIPERLAN are listed below :

- Modulation, demodulation (uses FSK,GMSK)
- Bit and frame synchronization
- Forward error correction mechanisms (uses BCH codes)
- Measurements of signal strength
- Channel sensing
- HIPERLAN-1 provides 3 mandatory and 2 optional channels according to their carrier frequencies.

(i) Mandatory channels

- Channel 0: 5.1764680 GHz
- Channel 1: 5.1999974 GHz
- Channel 2: 5.2235268 GHz

(ii) Optional channels

- Channel 3: 5.2470562 GHz
- Channel 4: 5.2705856 GHz

- HIPERLAN-1 uses non differential Gaussian minimum Shift Keying (non differential GMSK).
- It uses adaptive equalizer called decision feedback equalizer (DFE) to remove inter symbol interference (ISI) caused due to multipath propagation.

- HIPERLAN-1 also employs BCH error correcting codes to minimize the errors at physical layer.
- This code is able to correct a single error and detect two random errors, all errors bursts not longer than 5 – bits.
- Fig. 4.4.4 presents HIPERLAN-1 data packet format used at physical layer.

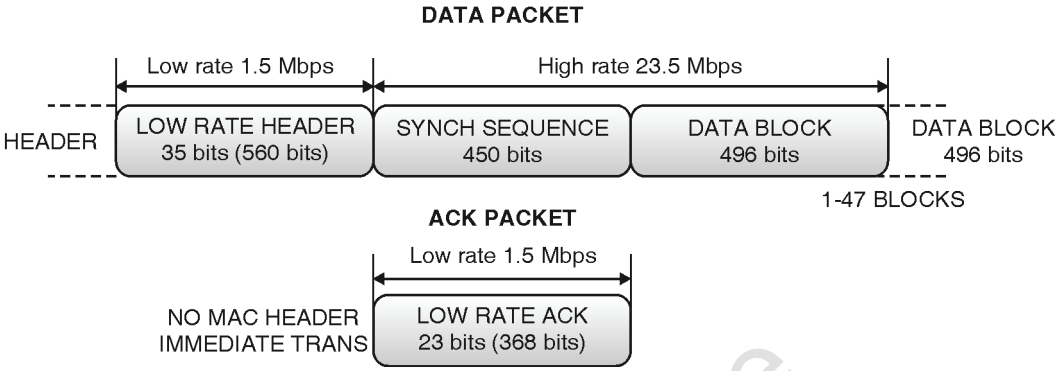


Fig. 4.4.4 : HIPERLAN-1 physical layer packet format for data and acknowledgement

4.4.2 HIPERLAN -2

MU – Dec. 18

Q.	Explain HIPERLAN-2 Data link control.	**(Dec. 18, 10 Marks)**

HIPERLAN2 allows interconnection in almost any type of fixed network.

Features of HIPERLAN- 2

- Operates at **5 GHz** frequency band
- Provides Connection-oriented service
- High speed transmission up to **54 Mbit/s** (same as IEEE 802.11a)
- Quality-of-Service (QoS) support
- Automatic frequency allocation
- Security support
- Mobility support
- Network and application independent
- Power saving

Reference model and configuration of HIPERLAN-2

- HIPERLAN-2 is designed to work in two configurations: business environment and home environment.
- Business environment is an access network which consists of several APs connected by a core network. Each AP serves a number of mobile terminals. HIPERLAN-2 also allows roaming between the APs.
- In home environment, an ad-hoc network is created.
- Fig. 4.4.5 presents the standard architecture of HIPERLAN-2 network.
- Two access points are connected to a **core network**.
- The Core network might be an ATM network, Ethernet LANs, UMTS 3G cellular network etc.
- Each access point contains two parts: an **Access Point Controller (APC)** and one or more **Access Point Transceiver (APT).**
- Four **mobile terminals (MT)** are also shown in Fig. 4.4.5.

- These MTs can move from one cell area to another. The access point automatically selects a frequency by using (dynamic frequency selection) DFS.

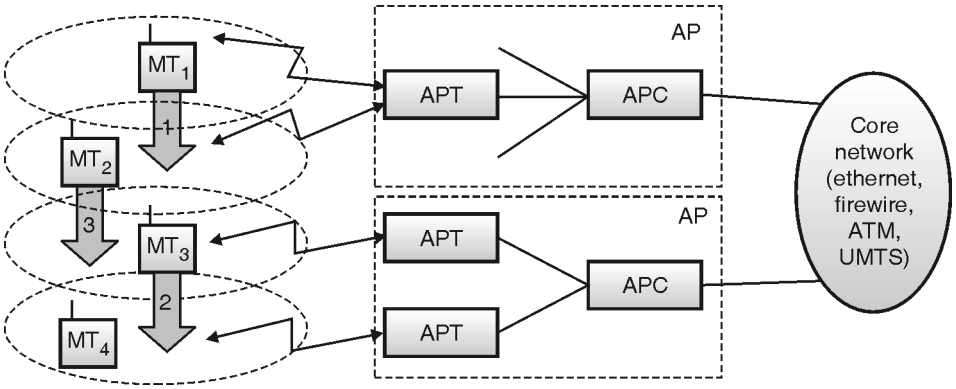


Fig. 4.4.5 : HIPERLAN/2 Basic structure and Handoff scenario

There are three types of handover which might occur :

1. Sector Handover (Inter sector)

- If the sectorized antennas are used for access point then AP supports this handover. MT moves from one sector to another sector that is controlled by the same APT.
- Sector handover is handled inside the DLC layer therefore not visible outside the AP.

2. Radio Handover (Inter-APT/Intra-AP)

- Radio handover is also handled within the AP.
- As shown in Fig. 4.4.5, MT_3 moves from one APT to another APT of the same AP.

3. Network Handover (Inter-AP/ Intra network)

- This handover occur when MT moves from one AP to another AP (in Fig. 4.4.6 MT_2).
- In this case, the core network and higher layers are also involved.

HIPERLAN-2 networks operate in two modes

1. Centralized Mode (CM)
2. Direct Mode (DM)

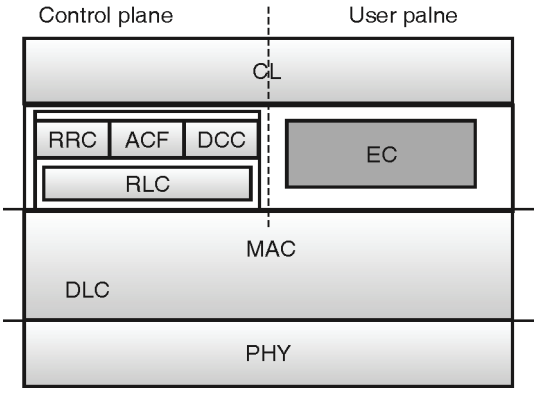
1. Centralized Mode (CM)

- This is an infrastructure based and mandatory mode.
- All APs are connected to a core network and MTs are associated with APs.
- If two MTs share the same cell then all data is transferred by AP.
- AP takes complete control of everything.

2. Direct Mode (DM)

- This is an ad-hoc and optional mode.
- In this mode, data is directly exchanged between MTs if they can receive each other. But the network is still controlled by AP that contains a central controller (CC). The central controller can be connected to a core network and can operate in both centralized and direct modes.

HIPERLAN-2 Protocol Stack



MAC – Medium Access Control

DLC- Data Link Control

RRC-Radio Resource Control

ACF- Association Control Function

DCC-DLC connection control

RLC- Radio Link Control

EC – Error Control

CL – Convergence Layer

Fig. 4.4.6 : HIPERLAN-2 reference Model

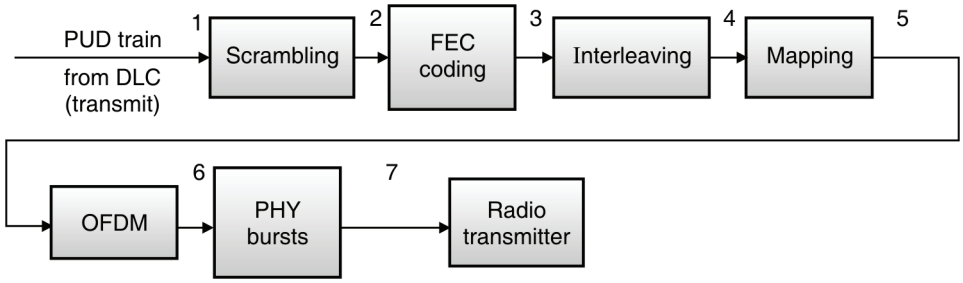
4.4.2(a) HIPERLAN-2 Physical Layer

- Many functions and features of PHY layer of HIPERLAN-2 are identical to IEEE 802.11a. It uses the same modulation scheme and provides the same data rate as IEEE 802.11a.
- Physical layer of HIPERLAN-2 performs the following functions.
  - Modulation(OFDM)
  - Forward Error Correction
  - Signal Detection
  - Synchronization etc.

Key features

- HIPERLAN-2 operates at **5GHz** frequency
- Maximum data rate of up to **54Mbit/s**
- It uses different modulation schemes such as BPSK, QPSK, 16-QAM, 64 –QAM to achieve different data rates.
- It employs **OFDM**.
- OFDM symbol duration - 4 µs
- Number of sub carriers - 52
- Number of pilot symbols - 4
- Subcarrier spacing - 312.5KHz
- Channel spacing - 20MHz
- Maximum transmit power is 200mW EIRP for the lower frequency band.

Fig. 4.4.7 illustrates the reference configuration of the transmission chain of a HIPERLAN-2 device.



1. Information bits
2. Scrambled bits
3. Encoded bits
4. Interleaved bits
5. Sub-carrier symbols
6. Complex baseband OFDM symbols
7. PHY bursts

Fig. 4.4.7 : HIPERLAN-2 Physical Layer reference configuration

The HIPERLAN-2 physical layer receives the PSDU from DLC Layer.

Step 1 : Scrambling

The first step then is scrambling of all data bits with the generator polynomial x^7+x^4+1. This is done for DC blocking and whitening of the spectrum. The outcome of this step is the scrambled bits.

Step 2 : FEC Coding

The next step is to apply FEC coding on these scrambled bits. This is done for error detection and correction. The result of this step is encoded bits.

Step 3 : Interleaving

Next, encoded bits are interleaved to mitigate the frequency selective fading. The result is interleaved bits.

Step 4 : Mapping

The mapping process first divides the bit sequence in group of 1, 2, 4 or 6 bits depending on the modulation schemes used such as BPSK, QPSK, 16-QAM,64-QAM respectively. These groups are mapped on to the appropriate modulation symbol. The result of this step is sub carrier modulation symbols.

Step 5 : OFDM Modulation

The OFDM modulation converts these symbols into a baseband signal. The symbol interval is 4μs.

Step 6 : PHY burst

In this step the physical burst is created. This burst contains preamble and payload.

Step 7 : Radio transmission

Finally radio transmission shifts the baseband signal into a carrier frequency.

4.4.2(b) HIPERLAN-2 Data Link Control Layer

- The Data Link control (DLC) layer is situated on top of the physical layer.
- DLC Layer contains the following sub functions :
  1. MAC function
  2. Error Control (EC)
  3. RLC sub layer that in turn is sub divided into RLC, RRC, ACF and DCC.

- DLC layer provides for a logical link between MT and AP over the OFDM physical layer.
- Data link control is divided into three parts: MAC, the Control Plane and the User plane.
- The user plane contains Error Control mechanism (EC).
- And the control plane contains RLC sub layer that provides most of the control functions given below.
  (i) ACF (Association Control Function) controls association and authentication of new MTs as well as performs synchronization task.
  (ii) DCC (DLC User Connection Control) controls connection setup, modification and release.
  (iii) RRC (**Radio resource control)** function performs the following tasks
    - Dynamic frequency selection
    - Measurements performed by MT
    - Reporting measurements to the AP
    - Frequency change by the AP and its associated MTs
    - Power saving procedure
    - Transmit power control
    - Handover between APs and within AP
- Fig. 4.4.8 shows HIPERLAN-2 MAC Frame format.

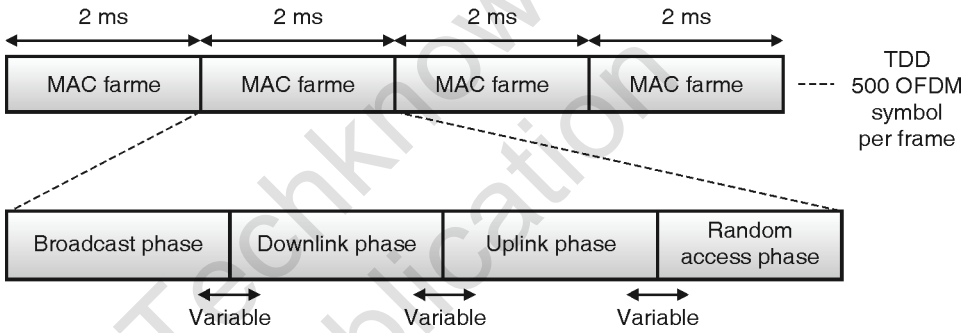


Fig. 4.4.8 : MAC frame structure of HIPERLAN-2

- HIPERLAN-2 medium access control is based on the TDMA/TDD.
- Each MAC frame is of 2ms duration and it is further divided into four phases.
  - **Broadcast Phase :** Carries the Broadcast Control Channel (BCCH) and Frame Control Channel (FCCH).
  - **Downlink phase :** Carries information from access point (AP) or Central Controller (CC) to the specified mobile terminal.
  - **Uplink phase :** Carries information from mobile terminal to AP or CC.
  - **Random access phase :** Used to transmit random access channel (RCH) .
- HIPERLAN-2 defines six different transport channels
  - **BCH (Broadcast channel) :** This channel conveys basic information for the radio cell to all MTs.
  - **FCH (Frame channel) :** Contains the exact description of the allocation of resources within the current MAC frame.

- **ACH (Access feedback channel) :** Gives feedback to MTs regarding random access during the RCH of the previous frame.
- **LCH (Long support channel) :** Transports user and control data for downlinks and uplinks.
- SCH (Short transport channel) : Transports control data for downlinks and uplinks.
- **RCH (Random channel) :** Using this channel, MTs can send information to AP/CC via slotted Aloha.

– HIPERLAN-2 also defines some logical channels for signaling, control and information transfer. These logical channels are mapped on SCH, LCH, and RCH transport channels.

- **SBCH :** Used only in downlink to broadcast control information related to the cell. It helps in handover, association, security and radio link control functions.
- **DCCH :** Conveys RLC sub layer signals between an AP and the MT.
- **UDCH :** Carries DLC PDU for convergence layer data.
- **LCCH :** It is used for error control functions for a specific UDCH.
- **ASCH :** It is used for association and re-association request messages.

4.5 Bluetooth

4.5.1 Introduction

– Bluetooth is a wireless LAN technology with very limited coverage (about 10m) and it does not need any infrastructure (Bluetooth is an example of ad hoc networks).

– Bluetooth technology was first developed by Ericsson. It was then formalized by a group of electronics manufacturers such as Ericsson, IBM, Intel, Nokia, and Toshiba who jointly form the Bluetooth Special Interest Group (SIG).

– Bluetooth technology was designed primarily to support simple wireless networking of personal consumer devices and peripherals, including cell phones, PDAs, and wireless headsets (Personal Area Network – PAN).

– Compared to Wi-Fi, Bluetooth networking is much slower, a bit more limited in range, and supports fewer devices.

Features of Bluetooth

– Bluetooth devices generally communicate at less than 1 Mbps.

– Operates in the **2.4 GHz** ISM band with 79 or 23 RF channels.

– GFSK (Gaussian Frequency Shift Keying) modulation is used and TDD (Time Division Duplex) is used for uplink and downlink separation.

– It applies **FHSS** with a **1600** hops/s hopping rate.

– It uses SCO (Synchronous Connection Oriented) links for voice and ACL (Asynchronous Connection less) links for Data.

– Uses FEC (forward error correction) with no retransmission.

– Uses 64 kbit/s duplex, point-to-point, circuit switched channels.

– Topology : Overlapping piconets (stars) forming a scatternet.

4.5.2 User Scenario

Many different configurations with Bluetooth based piconet are possible.

1. **Connection of peripheral devices :** Today most of the devices use wires to connect to the peripheral devices such as keyboard, mouse, headset, speakers etc. Each type of device has its own type of cable, connectors, plugs etc. In a wireless networks no wires are needed to connect such devices. Bluetooth piconet can be used to connect such peripherals without wires to the wireless terminals such as laptop or PDA.
2. **Support for ad hoc networking :** Ad-hoc networks are useful for tradeshows and exhibitions where several people come together and exchange data. Wireless networks can support this type of interaction. Small devices may not have WLAN adapters of IEEE802.11 standard, but cheaper Bluetooth chips built in.
3. **Bridging of Networks :** Using wireless piconets, a mobile phone can be connected to a PDA or laptop in a simple way. The mobile phone that has bluetooth chip can now act as a bridge between the local piconet and the global GSM network.

4.5.3 Architecture

MU – May 14

Q. With respect to Bluetooth protocol explain piconet and scatternet. **(May 14, 10 Marks)**

Piconet and Scatternet

1. **Piconet**
   - **Piconet** is a collection of Bluetooth devices which are synchronized to the same hopping sequence.
   - Each piconet has one device called Master (M). All other devices called slaves (S) are connected to the master.
   - The master determines the hopping sequence in the piconet and all slaves have to synchronize to this pattern. If a device wants to participate it has to synchronize to this.
   - There are two more types of devices: Parked device (P) and Stand-by devices(SB).
     - Parked devices can not actively participate in the piconet but are known and can be reactivated within some milliseconds.
     - Stand-by (SB) devices do not participate in the piconet.
   - A Master (M) can connect seven active slaves and up to 255 parked slaves per piconet.
   - All active devices in a piconet are assigned a 3-bit active member address (AMA). And all parked devices are assigned 8-bit parked member address (PMA).
   - The master (M) gives its clock and 48-bit device ID to all slaves in a piconet. Hopping sequence is determined by device ID and hopping pattern is determined by master's clock.
   - All active devices use the same hopping sequence and hops together.

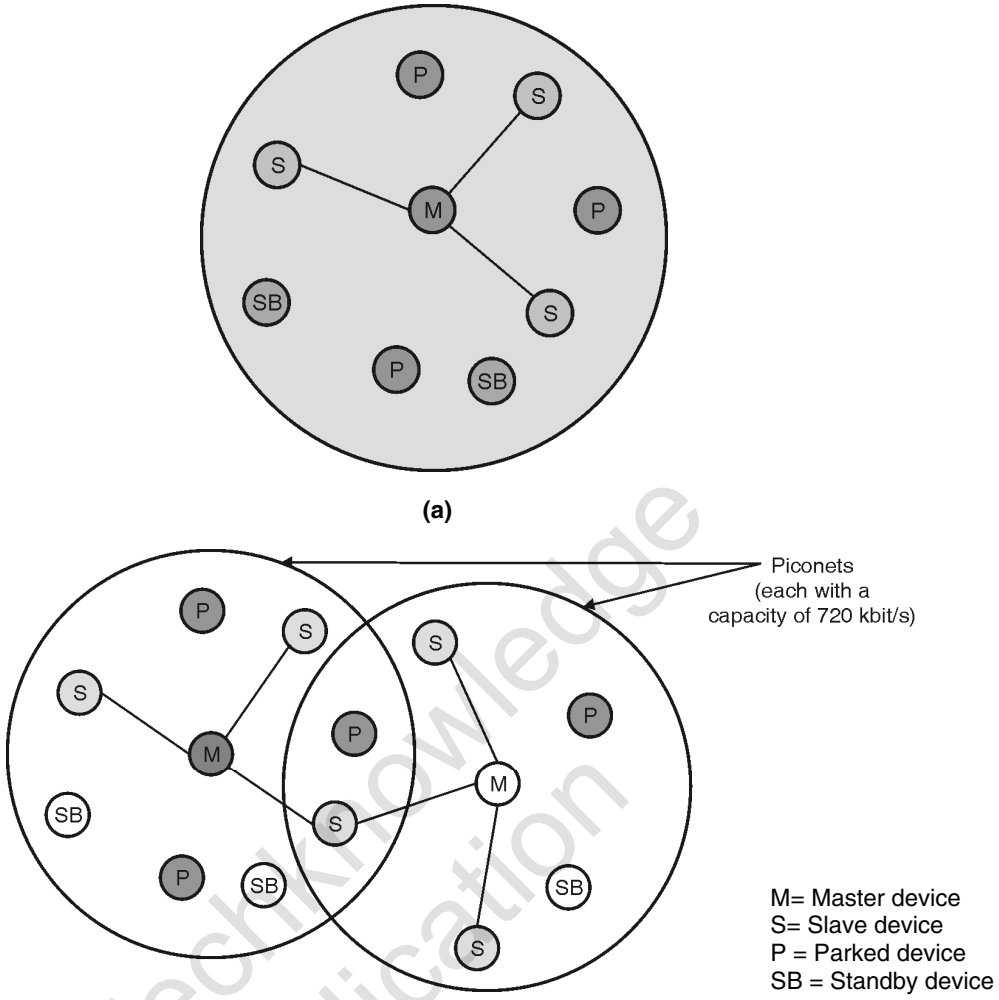


Fig. 4.5.1 : (a) Piconet (b) Scatternet

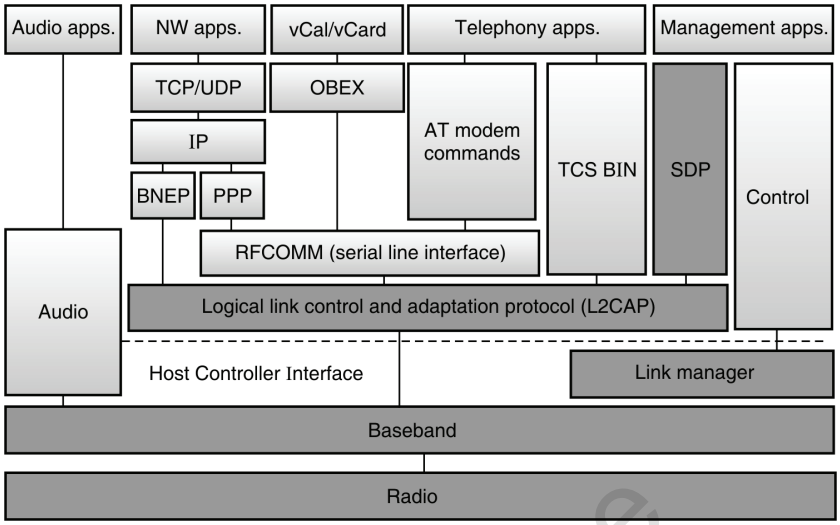
2. Scatternet

- **Scatternet** is a group of piconets. More than one piconet can be connected to form a scatternet through the sharing of common master or slave devices.
- Devices can be slave in one piconet and master in another.
- Communication between piconets can take place by jumping devices back and forth between the piconets.
- Each piconet in a scatternet uses a different hopping sequence that is always determined by the master of that piconet.

4.5.4 Bluetooth Protocol Stack

MU – May 12, Dec. 12, Dec. 13, May 16, Dec. 16, May 17, Dec. 17, May 18, Dec. 18

Q.	Draw and explain Bluetooth protocol stack in detail.	**(May 12, Dec. 12, Dec. 13, Dec. 18, 10 Marks)**
Q.	Explain in detail Bluetooth protocol architecture.	**(May 16, Dec. 16, May 17, May 18, 10 Marks)**
Q.	Describe Bluetooth architecture and protocol stack. Also discuss its limitations.	**(Dec. 17, 10 Marks)**



- AT : Attention sequence
- OBEX : Object exchange
- TCS BIN : Telephony control protocol specification – binary
- BNEP : Bluetooth network encapsulation protocol
- SDP : Service discovery protocol
- RFCOMM : Radio frequency comm.

Fig. 4.5.2 : Bluetooth protocol stack

Radio Layer

- Radio layer defines the carrier frequencies and output power.
- Bluetooth uses 2.4 GHZ license free band.
- Frequency hopping and TDD (time division duplex) is used for transmission with fast hopping rate of 1600 hops/s.
- It uses 79 hop carriers equally spaced with 1 MHz.
- Gaussian FSK used for modulation.

Baseband Layer

- Baseband layer performs frequency hopping to avoid interference and to access the medium.
- Defines physical links and many packet formats.
- It controls :
  - Device Addressing
  - Channel control (how devices find each other) through paging and inquiry methods
  - Power-saving operations
  - Flow control and synchronization among Bluetooth devices.

Link Manager Protocol (LMP)

- The link manager protocol (LMP) manages various aspects of the radio link between master and slave.
- The following functions are covered by LMP :
  - Authentication, pairing, and encryption
  - Synchronization
  - Capability negotiation

- QoS negotiation
- Power control
- Link supervision
- State and transmission mode change

Logical Link Control and Adaptation Layer Protocol (L2CAP)

- L2CAP is layered over the Baseband Protocol and resides in the data link layer.
- L2CAP provides :
  - Connection-oriented and connectionless data services to upper layer protocols with protocol multiplexing capability.
  - Segmentation and reassembly operation.
  - Group abstractions.
- L2CAP provides three different types of logical channels that are transported via ACL link between master and slave, these are :
  - Connectionless used for broadcast.
  - Connection-oriented for data transfer with QoS flow specification.
  - Signaling used to exchange signaling messages between L2CAP entities.

Host Controller Interface (HCI)

- The HCI provides a command interface to the baseband controller and link manager
- It provides access to hardware status and control registers.
- Essentially this interface provides a uniform method of accessing the Bluetooth baseband capabilities.
- The HCI exists across 3 sections, **The Host**, **Transport Layer, Host Controller**. Each of the sections has a different role to play in the HCI system.
- HCI defines the set of functions of a Bluetooth module that are accessible to the host and its application.
- HCI can be seen as a software/hardware boundary.

RFCOMM

- The RFCOMM protocol provides emulation of serial ports over the L2CAP protocol.
- It is a cable replacement protocol that provides a serial line interface to all the applications.
- The protocol is based on the ETSI standard TS 07.10.
- It supports multiple serial ports over a single physical channel.

Service Discovery Protocol (SDP)

- The service discovery protocol (SDP) helps the applications to discover which services are available and to determine the characteristics of those available services.
- SDP defines only the discovery of services not about their usage.
- New service is discovered as follows
  - Client sends a request to search for an interested service.
  - Then server responds to the client with the list of available services that match to client's criteria.
  - The client uses this list to retrieve additional service attribute for the service of interest.

Profiles

- Profiles are specifications which describe how Bluetooth should be used in a specific application and as thus ensures that all devices from different manufacturers can seamlessly work with one another. There are about a dozen profiles:
- Generic Access, Serial Port, Dialup Networking, FAX, Headset, LAN Access Point, Generic Object Exchange (OBEX), File Transfer, Object Push, Synchronization, Cordless Telephony, and Intercom.
- More profiles are under discussion within various Bluetooth SIG groups.
- The profile concept is used to decrease the risk of interoperability problems between different manufacturers' products.

Telephony Control Protocol Specification Binary (TCS-BIN)

To define call control signaling for the establishment of voice and data calls between Bluetooth devices TCS-BIN describes a binary, packet based, bit-oriented protocol.

4.5.4(a) Bluetooth Baseband States

MU – Dec. 15

Q. Explain how a Bluetooth network is established using baseband state transitions. **(Dec. 15, 10 Marks)**

- A typical Bluetooth device has a power of 100mW and can have a range of upto 100m.
- Having such huge power and relying on battery as its source will result in a huge wastage if the device lies idle for long time.
- Bluetooth defines several low-power states for a device. The major states present can be seen in the Fig. 4.5.3.
- **Standby :** A device which is currently ON and not part of any piconet is in standby mode. In this low-power mode only the native-clock runs.
- **Inquiry :** Now the movement to the next node i.e. inquiry state is based on either of two ways :
  1. **A device wants to establish a piconet :** The user wants to scan all the devices in its range. This inquiry procedure is started by sending an Inquiry access Code (IAC) to all devices in range.
  2. **Device in Standby that listens periodically :** A device which is in Standby may enter the Inquiry state periodically to search for IAC messages. If it finds one such, then it transfers the necessary information about itself and becomes a slave.
- **Page mode :** On successful inquiry, the device enters the page mode. In the page state two different roles are defined.
  1. After the master finds all the devices required for a connection, it sets up a piconet.
  2. The master then calculates special hopping sequences based on the device addresses received to contact each device individually.
  3. The slaves answer to calls by the master and synchronize their clocks accordingly.
  4. In the meantime, the master may continue to page more devices to the piconet.
  5. As soon as the device (slave) synchronizes to the hopping pattern of the piconet, it enters the connected state.
- **Connected :** The connected state contains the active state and three low power states.
- **Active :**
  - In active state the slave participates in the piconet by listening, transmitting and receiving. A master periodically synchronizes with these slaves.
  - The communication is done via ACL and SCO links.
  - Every device which is active needs to have a 3-bit Active Member Address (AMA).
  - In the active state, if the device is not transmitting, it can disconnect itself and go to standby by **detach** method.

– A Bluetooth also has the choice to go into either of the three low-power states which are :

1. Sniff

- Out of all the three low power states, this one has max. power consumption.
- Unlike in active state where the slave listens to piconet at every slot, here it listens at a reduced rate which can be programmed as per the need.
- The master also allocates a reduced number of slots for the slave in sniff mode.

2. Hold

- The device here stops all ACL link transmissions are stopped.
- If no activity is there in the piconet, the slave reduce the power consumption or participates in another piconet.

3. Park

- This state has the lower duty cycle and lowest power consumption of the three.
- It also release it 3-bit AMA address. Instead it gets a 8-bit PMA (Parked Member Access).
- It remains a member of the piconet but gives a chance for another device to become active.

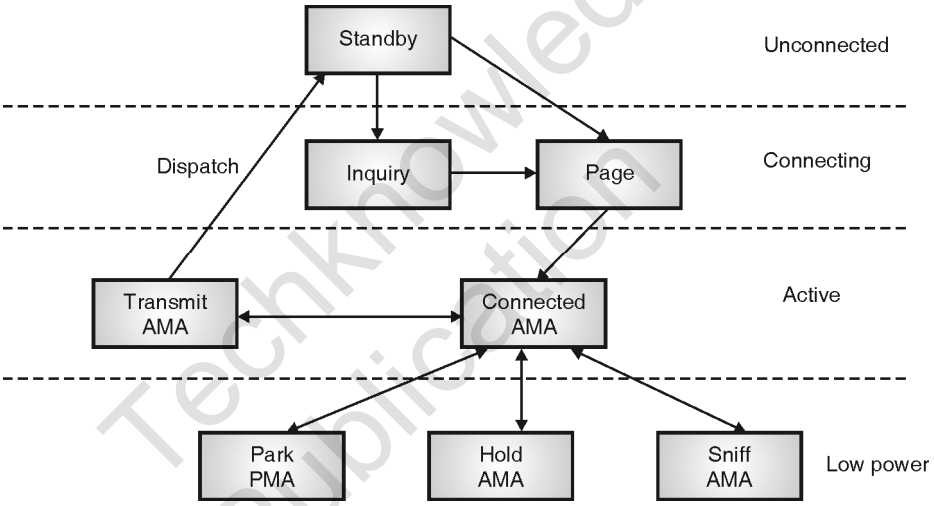


Fig. 4.5.3 : Bluetooth baseband states

4.6 Comparison of IEEE 802.11, HIPERLAN-1, HIPERLAN-2 and Bluetooth

MU - Dec. 12, Dec. 13, May 15, Dec. 15, May 16, Dec. 16, Dec. 17

Q.	Compare between IEEE 802.11 and HIPERLAN-2.	**(Dec. 12, Dec. 13, Dec. 17, 10 Marks)**
Q.	Compare HIPERLAN-1, HIPERLAN-2 and 802.11 W-LAN.	**(May 15, 10 Marks)**
Q.	Write a short note on HIPER LAN-1 VS HIPERLAN-2.	**(Dec. 15, 5 Marks)**
Q.	Compare HIPERLAN 2, BLUETOOTH, IEEE 802.11.	**(May 16, Dec. 16, 10 Marks)**

Table 4.6.1 : Comparison of IEEE 802.11, HIPERLAN and Bluetooth

Characteristic	IEEE 802.11	IEEE 802.11a	HIPERLAN-1	HIPERLAN-2	Bluetooth
Frequency	2.4 GHz	5GHz	5 GHz	5GHz	2.4 GHz
Max data rate	2 Mbps (11 Mbps with CCK)	54 Mbps	23.5Mbps	54 Mbps	<1Mbps

Characteristic	IEEE 802.11	IEEE 802.11a	HIPERLAN-1	HIPERLAN-2	Bluetooth
User throughput	6 Mbps	34Mbps	<20Mbps	34Mbps	<1Mbps
Connection	Point-to-point	Point-to-Multipoint	Provide multi-hop routing	Point-to-Multipoint	Point-to-Multipoint
Physical layer	FHSS/DSSS	OFDM	–	OFDM	FHSS
Authentication	None	None	None	x.509	Yes
Medium access	CSMA/CA	CSMA/CA	Variant of CSMA/CA i.e. EYNPMA protocol	CSMA/CA	Master is responsible for Medium access.
Transmit power	100mW	0.05/0.25/1W TPC	0.01/0.1/1 W	0.2 to 1 W	1 to 100 mW
Error control	ARQ	ARQ,FEC at PHY layer	FEC at Physical layer. It uses BCH codes.	ARQ/FEC at PHY layer	ARQ/FEC at MAC layer
Architecture	Infrastructure based architecture with additional support for ad hoc networks	Infrastructure based architecture with additional support for ad hoc networks	Infrastructure based architecture with additional support for ad hoc networks	Infrastructure based architecture with additional support for ad hoc networks	Ad hoc network
QoS support	Optional -QoS is supported by providing Point Coordination Function (PCF)	Optional -QoS is supported by providing Point Coordination Function (PCF)	CAC sub layer of HIPERLAN1 provides five priority levels for QoS support. The mapping of a QoS on a priority level is done with the help of packet life time	Yes: Uses connection oriented service to provide QoS such as bandwidth, delay, jitter etc.	Link Manager protocol provides means to negotiate QoS such as flow specification.
Connectivity	Connectionless	Connectionless	Connection less	Connection-oriented	Connectionless+connection-oriented

Review Questions

Q. 1 Discuss the advantages and disadvantages of WLAN over wired network. Explain two basic types of WLAN architecture.

Q. 2 Explain in detail function of HIPERLAN-1 CAC sublayer.

Q. 3 Draw and explain IEEE 802.11 protocol architecture.

Q. 4 Discuss the PHY frame format of an IEEE 802.11 using FHSS technique.

Q. 5 Describe IEEE 802.11 MAC frame format.

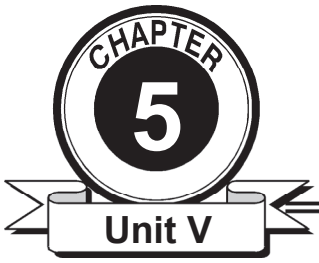
Q. 6 Describe MAC mechanism schemes used in IEEE802.11. Explain in detail MAC scheme that uses DCF with RTS/CTS extension.

Q. 7 Discuss Basic MAC schemes used in IEEE 802.11.

Q. 8 Write a short note on HIPERLAN-2.

Q. 9 Explain HIPERLAN-2 data link control layer.

❑❑❑



Mobility Management

Syllabus

5.1 Mobility Management : Introduction, IP Mobility, Optimization, IPv6

5.2 Macro Mobility : MIPv6, FMIPv6,

5.3 Micro Mobility : CellularIP, HAWAII, HMIPv6,

Introduction

IP Mobility is a mechanism that allows mobile device to move from one network to another network without changing its permanent IP address. This chapter discusses various protocols to support IP Mobility. **Mobile IP** was the first communication protocol developed by IETF to support IP mobility with the current version of IPV4. Later **Mobile IPV6 (MIPV6)** was developed as an update to IPV6 protocols to supports IP mobility. IPV6 header has some new features and options that supports IP mobility. The chapter also discusses various Micro mobility mechanisms to support fast and seamless handover while mobile device is changing its network or point of attachment.

5.1 Introduction to IP Mobility

- **IP mobility** refers to the set of mechanisms that allow an **IP** mobile node to move freely between different **IP** networks while maintaining **IP** connectivity in a transparent way.
- Current versions of the Internet Protocol (IPV4) assume that the point at which a computer attaches to the Internet or a network is fixed and its IP address identifies the network to which it is attached.
- Packets are sent to a mobile device based on the location information contained in the IP address.
- If a mobile device, or **mobile node**, moves to a new network while keeping its IP address unchanged, its address does not reflect the new point of attachment.
- Consequently, existing routing protocols cannot route packets to the mobile node correctly.
- In this situation, we must reconfigure the mobile node with a new IP address representing its new location. Thus, under the current Internet Protocol (IPV4) , if the mobile node moves without changing its address, it loses routing; and if it does change its address, it loses connections.
- One of the most desirable features of **IP mobility** mechanisms is the ability of maintaining connectivity without interrupting ongoing communications.

5.1.1 Mobile IP

- **Mobile IP** (or MIP) is an IETF standard communications protocol that is designed to allow **mobile** device users to move from one network to another while maintaining a permanent **IP** address.

  Mobile IP is an enhancement of the internet protocol (IP) that adds mechanisms for forwarding internet traffic to mobile devices when they are connecting through other than their home network. Fig. 5.1.1 shows generic Mobile IP topology.

- Every host will have a "Home Address (Permanent IP)" within a "Home Network". A home network has a "Home Agent" that provides several services for the mobile node
- Traffic destined to the "Home Address" of mobile node (MN) will always be routed to the "Home Agent."
- If the mobile node is in its "Home Network", traffic will be forwarded directly the mobile node.
- If the mobile node has moved to some other network called "Foreign Network", traffic will be IP tunneled by the "Home Agent" to a "Care-of- Address". The Care- of- address defines the current location of the mobile node.
- Every Foreign network has 'Foreign agent (FA) '. The foreign agent can provide several services to the mobile node during its visit to the foreign network. The FA can have the COA (care or address) acting as a tunnel endpoint when forwarding packets to the MN.

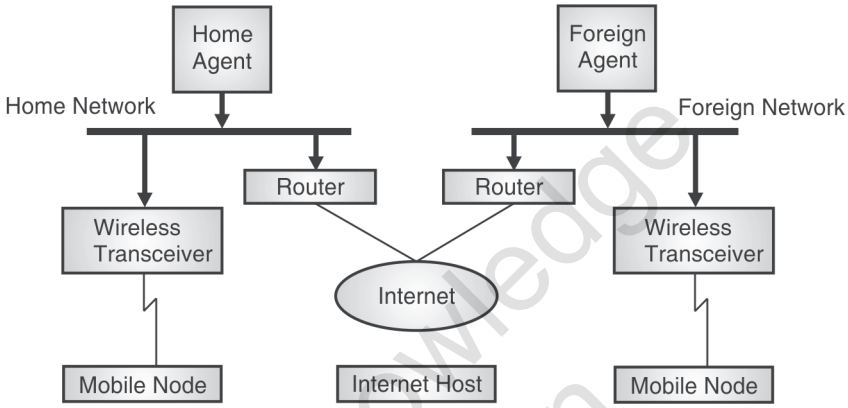


Fig. 5.1.1 : Mobile IP topology

5.1.2 Optimization

Triangular routing

- With Mobile IPv4 there is always a triangular traffic pattern. As shown in Fig. 5.1.2 the IP packet from a CN (Correspondent Node) destined to an MN needs to be routed to its HA first and then tunneled to the foreign agent of the MN.
- If the Corresponding Node (CN)and MN are very near, then also the IP packet has to travel a long way to reach the MN. This in efficient behavior of a non optimized mobile IP is called ***Triangular Routing***.
- The triangle is made of the three segments : CN to HA, HA to COA/MN and MN back to CN.

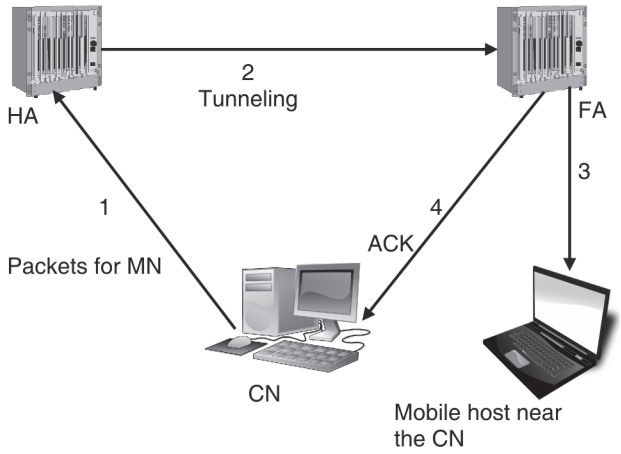


Fig. 5.1.2 : Triangular Routing

Route optimization to avoid triangular routing

To solve triangular routing problem, a route optimization protocol has been introduced. Basically this protocol defines some messages as to inform CN of an upto date location of MN. Once the current location of the MN is known, the CN itself performs tunneling and sends packet directly to MN.

The optimized mobile IP protocol needs four additional messages; these are :

1. Binding request

If a node wants to know where the MN is currently located, it can send a binding request to the HA.

2. Binding update

The HA sends a binding update to the CN and informs the CN the current location of an MN. The binding update can request an acknowledgement.

3. Binding acknowledgement

On request, after receiving a binding update message, anode returns a binding acknowledgement.

4. Binding warnings

- A binding warning message is sent by anode if it decapsulates a packet for an MN but it is not the FA for that MN currently.
- If CN receives the binding warning, it requests the HA for a new binding update.
- If the HA receives the warning it directly sends a binding update to the CN.
- Fig. 5.1.3 explains how these four messages are used together when an MN changes its FA and also shows the exchange of messages in optimization protocol.

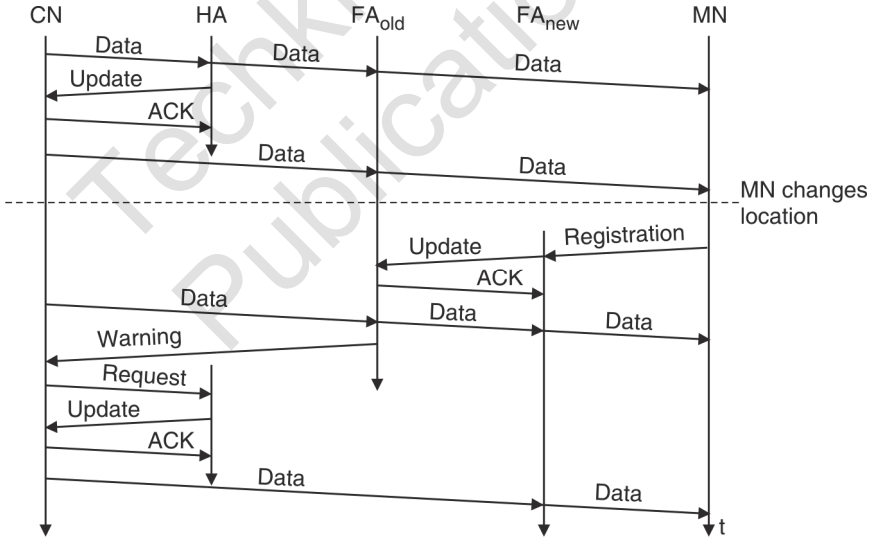


Fig. 5.1.3 : Optimized mobile IP working

- The CN requests the current location of MN from the HA.
- HA returns the COA of the MN via update message.
- CN acknowledge this updated message and stores mobility binding.
- Now CN can send data directly to the current foreign agent FA_{old}. FA_{old} now forwards these data to MN.
- The MN might now change its location and register with an new foreign agent FA_{new}.
- FA_{new} informs FA_{old} about new registration of MN via an update message and FA_{old} acknowledged this update message.

- CN doesn't know about the current location of MN, its till tunnels its packets for MN to the old foreign agent FA_{old}.
- The FA_{old} notices packets destined to MN but also knows MN currently not in current FA.
- FA_{old} might now forward these se packets to the new COA of MN which is new foreign agent.
- Thus the packets that are in transit are not lost. This behavior is another optimization to basic mobile IP and provides smooth handover.
- FA_{old} sends binding warning message to CN. CN then requests a binding update.
- The HA sends an update to inform the CN about the new location, which is acknowledged. Now CN cans end data directly to FA_{new}, and avoid triangular binding.
- However, the optimization will not work if the MN does not want to reveal its current location to the CN because of security.

5.2 IPv6 – Internet Protocol Version 6

- To overcome these problems, IPv6 also known as **IPng** (Internet Protocol next generation) was proposed. In IPv6, the Internet protocol was extensively modified to accommodate the growth and new demands of the Internet. The format and the length of the IP addreses were changed along with the packet format.
- Related protocols such as ICMP were also modified. Other protocols in the network layer, such as ARP, RARP, IGMP were either deleted or included in ICMPv6 protocol. Routing protocols such as RIP and OSPF were slightly modified to accommodate these changes. The fast spreading use of Internet and new services such as mobile IP, IP telephony, and IP-capable mobile telephony, may require the total replacement of IPv4 by IPv6.

Advantages of IPv6

1. **Larger address space :** An IPv6 address is 128 bit long. Compared with the 32 bit long IPv4 address, this is huge increase in address space.
2. **Better Header format :** IPv6 uses a new header format in which options are separated from the base header and inserted when needed, between the base header and the upper layer data. This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.
3. **New Options :** IPv6 has new options to allow for additional functionalities.
4. **Allowance for extension :** IPv6 is designed to allow the extension of protocol if required by new technologies or applications.
5. **Support for resource allocation :** In IPv6, the ***type-of-service*** field has been removed, but mechanism called ***Flow label*** has been added to enable the source to request special handling of packet. This mechanism can be used to support traffic such as real-time audio and video.
6. **Support for more security :** The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

Features of Ipv6 to support mobility

- No special mechanisms are needed for securing mobile IP registration. In every Ipv6 node **address auto configuration** i.e. the mechanism for acquiring a COA is inbuilt.
- **Neighbor discovery** mechanism is also mandatory for every Ipv6 node. So special foreign agents are no longer needed to advertise services.
- Combining the features of address auto configuration and neighbor discovery enables every Ipv6 mobile node to create and obtain a topologically correct address or the current point of attachment.
- Every Ipv6 node can send binding updates to another node, so the MN can send its COA directly to the CN and HA. The FA is no longer needed. The CN processes the binding updates and makes corresponding entries in its routing cache.

- The MN is now able to decapsulates the packets
  - To detect when it needs a new COA and
  - To determine when to send binding updates to the HA and CN
- A **soft handover** is possible with Ipv6. The MN sends its new COA to the old router serving the MN at the old COA, and the old router can encapsulate all incoming packets for the MN and forwards them to new COA.

Limitation of Ipv6

It does not solve any firewall or privacy problems. Additional mechanisms on higher layers are needed for this.

Ipv6 Header

Fig. 5.2.1 shows both Ipv4 and Ipv6 header format.

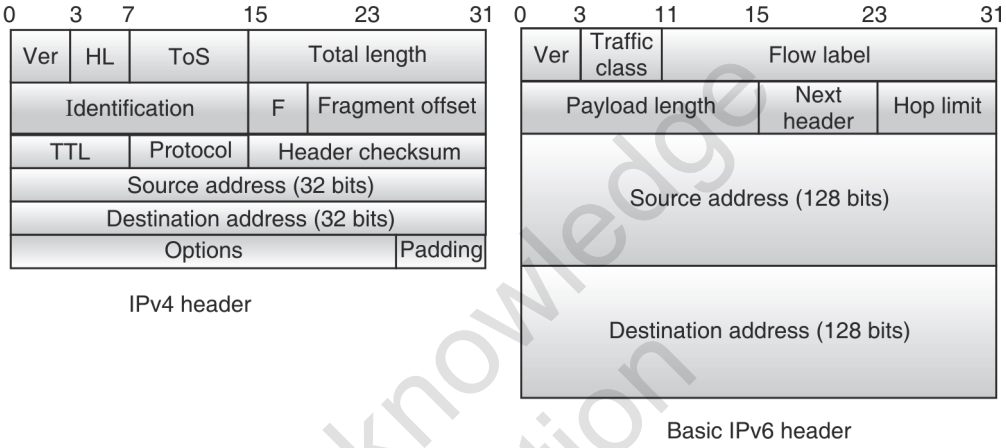


Fig. 5.2.1 : Comparison of Ipv4 and Ipv6 Header format

Fields of Ipv6 header :

1. **Version :** 4 bits - IPv6 version number.
2. **Traffic Class :** 8 bits - Used to specify different classes or priorities of IPv6 packets.
3. **Flow Label :** 20 bits - Used for specifying special router handling from source to destination(s) for a sequence of packets. It distinguish the different types of packets such as audio, video, txt etc. and accordingly provides quality of services to them.
4. **Payload Length :** 16 bits unsigned - Specifies the length of the data in the packet.
5. **Next Header :** 8 bits - Specifies the next encapsulated protocol. The values are compatible with those specified for the IPv4 protocol field.
6. **Hop Limit :** 8 bits unsigned - For each router that forwards the packet, the hop limit is decremented by 1. When the hop limit field reaches zero, the packet is discarded. This replaces the TTL field in the IPv4 header that was originally intended to be used as a time based hop limit.
7. **Source address :** 16 bytes - The IPv6 address of the sending node.
8. **Destination address :** 16 bytes - The IPv6 address of the destination node.

5.3 Macro Mobility

5.3.1 MIPv6 (Mobile IPv6)

- The first IP Mobility protocol, **Mobile IP** (discussed in Section 5.1.1) was developed for **IPv4**. The Mobile IP protocol solves the TCP/IP Layer 3 mobility problem, by assigning a permanent IP address to the mobile node.

- Mobile IP supports of both MIPv4 and MIPv6, but IPv4 has a couple of drawbacks. The main drawback of IPV4 is address exhaustion, making MIPv6 the future option for mobility protocol in IP Networks.
- **Mobile IPv6** (MIPv6) is a protocol developed as a subset of IPv6 to support mobility.
- MIPv6 is an update of the Mobile IP standard designed to authenticate mobile devices using IPv6 addresses.
- In traditional IP routing, IP addresses represent a topology. Routing mechanisms rely on the assumption that each network node will always have the same point of attachment to the Internet, and that each node's IP address identifies the network link where it is connected.
- In this routing scheme, if you disconnect a mobile device from the Internet and want to reconnect through a different network, you have to configure the device with a new IP address, and the appropriate netmask and default router.
- Otherwise, routing protocols have no means of delivering packets, because the device's network address doesn't contain the necessary information about the node's network point of attachment to the Internet.
- Mobile IPv6 allows a mobile node to transparently maintain connections while moving from one subnet to another.
- Each device is identified by its home address although it may be connecting to through another network. When connecting through a foreign network, a mobile device sends its location information to a home agent, which intercepts packets intended for the device and tunnels them to the current location.

5.3.2 FMIPv6 (Fast Hand Over for Mobile IPV6)

- Mobile IPv6 (MIPv6) enables a Mobile Node (MN) to maintain its connectivity to the Internet when moving from one Access point to another. This process is referred to as **'handover'**.
- During handover, there is a period during which the Mobile Node is unable to send or receive packets. This period is called '**Hand over latency**'.
- Hand over latency results from the standards handover procedure such as movement detection, new Care of address configuration, binding updates etc.
- This Hand over latency is often unacceptable to real-time traffic such as Voice over IP (VoIP).
- The fast handover for mobile IPv6 (FMIPv6) aims at reducing the long handover latency in mobile IPv6 by fast movement detection and fast binding update.
- It uses anticipation based on layer 2 trigger information of the mobile node (MN) to obtain a new care-of address at the new link while still connected to the previous link, thus reducing handover delay.
- Furthermore, it also reduces packet loss by buffering before the real link layer handover takes place.

5.4 Micro Mobility

- Mobile IP represents a simple and scalable global mobility solution but lacks the support for fast handoff control and paging.
- Imagine a large number of mobile devices changing networks quite frequently ; a high load on the home agents as well as on the networks is generated by registration and binding update messages.
- IP micro-mobility protocols can complement mobile IP by offering fast and almost seamless handover control in limited geographical areas.
- The basic underlying idea is the same for all micro-mobility protocols: Keep the frequent updates generated by local changes of the points of attachment away from the home network and only inform the home agent about major changes, i.e., changes of a region.
- In some sense all micro-mobility protocols establish a hierarchy.
- The following section presents three of the most commonly used approaches.

5.4.1 Cellular IP

Why Cellular IP ?

- Mobile IP exhibits several problems when there is a large number of mobile devices changing network frequently and moving very fast. In such cases, a high load on home agents and on the network is generated by registration and binding update messages.
- Mobile IP is basically designed only for **macro level mobility** and relatively **slow moving hosts**.
- Cellular IP (CIP) is a new robust, simple, and flexible protocol for highly mobile hosts.
- CIP complements Mobile IP by supporting **local mobility**.
- It can accommodate large number of users by separating **idle hosts** from **active hosts**.

CIP architecture

The architecture of Cellular IP is shown in Fig. 5.4.1. It consists of three major components.

- Cellular IP gateway (GW),
- Cellular IP node or the base station (BS)
- Cellular IP mobile host (MH)

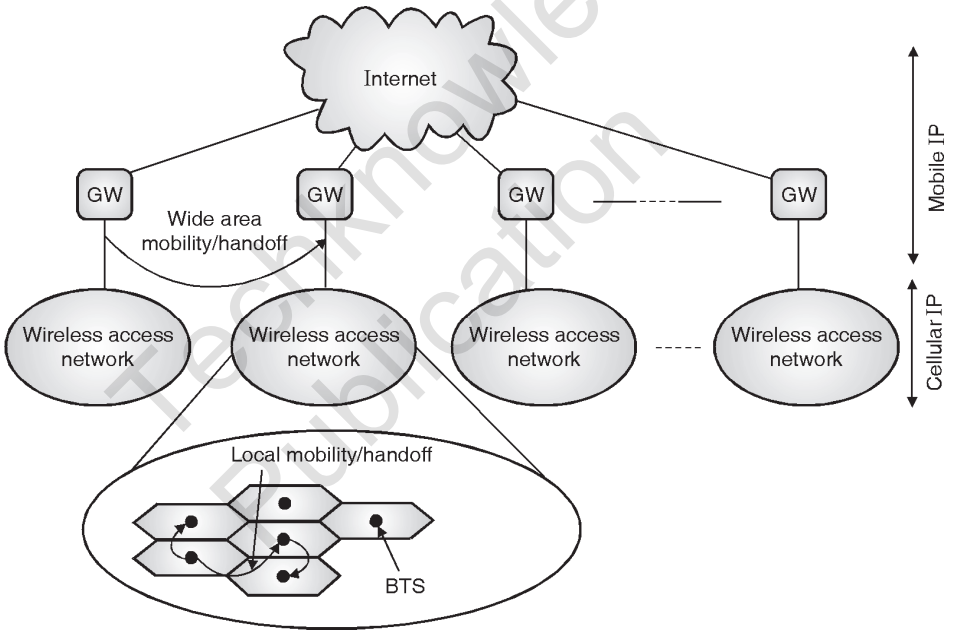


Fig. 5.4.1 : Cellular IP access network (architecture)

- An important component of a Cellular IP network is the **base station (BS)**. A cellular IP network consists of several interconnected BSs.
- The BSs communicate with mobile hosts (MHs) via wireless interface and also route IP packets inside the cellular network. The base stations are built on regular IP forwarding engines, but IP routing is now replaced by Cellular IP routing and cellular location management.
- **CIP gateway router** connects a cellular IP network and the regular Internet.
- Mobility between gateways is managed by Mobile IP while mobility within access networks is handled by Cellular IP.
- Now the IP address of gateway serves as the care-of-address for all mobile hosts that are currently attached to the network.

Routing in CIP

- **Uplink packets** (packets originated from mobile host) are routed from mobile host to the gateway on a hop-by-hop basis.
- The path taken by these packets is cached in base stations. This cache is called **routing cache.**
- To route **downlink packets** addressed to a mobile host the path used by recent packets transmitted by the host (that are already stored in route cache) is reversed.
- A mobile host may wants to maintain its routing cache mappings even though it is not regularly transmitting data packets.
- Such mobile hosts transmit route-update packets at regular interval to keep their routing cache mappings valid. These packets are empty data packets addressed to the gateway.

Paging in CIP

- In Cellular IP, an **idle mobile host** is one that has not received data packets for a system specific time.
- For such idle hosts, their downlink soft state routes timeout and are removed from the routing cache.
- These hosts transmit **paging-update** packets at regular intervals. The paging update packet is an empty IP packet addressed to the gateway. It is distinguished from route update packet by its IP type parameter.
- Similar to data and route update packets, paging update packets are routed on a hop-by-hop basis to the gateway. Base stations may optionally maintain paging cache.
- Thus all idle mobile hosts have mappings in paging caches but not in routing caches.
- In addition, active mobile hosts will have mappings in both routing as well as paging cache.
- Packets addressed to a mobile host are normally routed by routing cache mappings. Paging occurs when a packet is addressed to an idle mobile host and the gateway or base stations find no valid routing cache mapping for the destination.
- The paging cache is used to avoid broadcast search procedures found in cellular systems.
- If there is no entry in the paging cache, then the packet addressed to an idle mobile host is broadcast in the access network. This may happen when transmitting first packet to the any host.
- Idle mobile hosts that receive a packet, move from idle to active state and immediately transmit a route-update packet.

Handover in CIP

- CIP implements MCHO (Mobile controlled handover) thus, in CIP, handoff is initiated by Mobile Host (MH).
- MH listens to the beacon transmitted by BSs and initiates handover based on signal strength measurements.
- To perform a handoff, an MH tunes its radio to the new BS. It then sends a route update packet to this new BS.
- This creates entry in a routing cache on route to the gateway, thus, configuring the downlink route to the new BS.
- During the handoff process time, downlink packets may be lost. The mappings associated with the old base station are not cleared at handover, rather, they timeout as the associated soft-state timers expire.
- The mappings associated with the old BS are cleared after the expiry of a timer.
- Before the timeout, both the old and new downlink routes remain valid and packets are delivered through both the BSs. Thus, Cellular IP uses semisoft handover to improve handoff performance.

Advantages of CIP

1. Provides easy Global migration
2. Cheap Passive Connectivity

3. Efficient Location Management
4. Flexible Handoff
5. Simple Memory less Mobile hosts

5.4.2 HAWAII

HAWAII (Handoff-Aware Wireless Access Internet Infrastructure) tries to keep micro-mobility support as transparent as possible for both home agent and MN.

Working

Step 1 : On entering an HAWAII domain, a mobile node obtains a co-located COA.

Step 2 : MN registers with the HA.

Step 3 : When MN moving another cell inside the foreign domain, the MN sends a registration request to the new base station as to a foreign agent.

Step 4 : The base station interprets the registration request and sends out a handoff update message, which reconfigures all routers on the paths from the old and new base station to the crossover router. When the routing has been reconfigure successfully, the base station sends a registration reply to the MN, again as if it were a foreign agent.

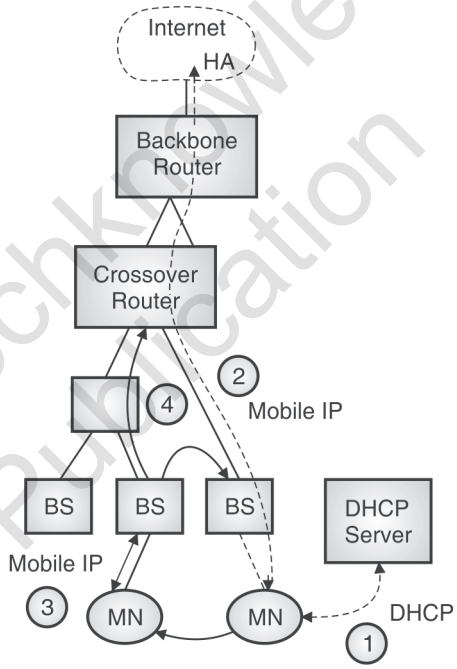


Fig. 5.4.2 : Basic architecture of HAWAII

Advantages

1. **Security :** Challenge response extensions are mandatory. In contrast to cellular IP, routing changes are always initiated by the foreign domain's infrastructure.
2. **Transparency :** HAWAII is mostly transparent to mobile nodes.

Disadvantages

- Co-located COA raises DHCP security issues(DHCP has no strong authentication).
- Decentralized security-critical functionality(Mobile IP registration processing during handover)in base stations.
- Authentication of HAWAII protocol messages unspecified (potential attackers: stationary nodes in foreign network).

- MN authentication requires PKI or AAA infrastructure.
- There are no provisions regarding the setup of IPsec tunnels.
- No private address support is possible because of co-located COAs.

5.4.3 HMIPv6 – Hierarchical Mobile IPv6

- Hierarchical Mobile IPV6 (HMIPv6) provides micro-mobility support by installing a **mobility anchor point (MAP)**. MAP is an entity which is responsible for a certain domain and acts as a local HA within this domain for visiting MNs.
- Fig. 5.4.3 shows basic architecture of Hierarchical Mobile IP.
- The MAP receives all packets on behalf of the MN, encapsulates and forwards them directly to the MN's current address **LCOA** (Link COA).

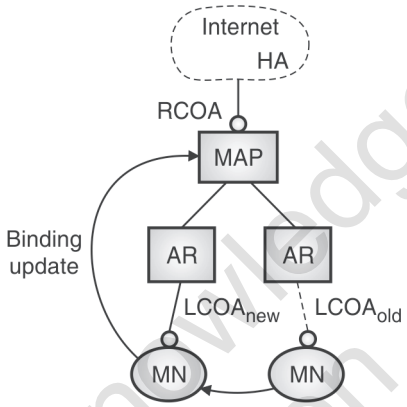


Fig. 5.4.3 : Basic architecture of hierarchical mobile IP

Advantages

1. **Security :** MNs can have (limited) location privacy because LCOAs can be hidden.
2. **Efficiency :** Direct routing between CNs sharing the same link is possible

Disadvantages

1. **Transparency :** Additional infrastructure component (MAP).
2. **Security :** Routing tables are changed based on messages sent by mobile nodes. This requires strong authentication and protection against denial of service attacks. Additional security functions might be necessary in MAPs

Review Questions

Q. 1 What is a need of Micro Mobility? Explain HAWAII in details.

Q. 2 Draw a neat sketch of IPv6 header. Compare IPv4 and IPv6 with respect to IP mobility.

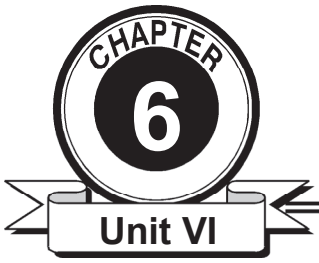
Q. 3 What advantages IPv6 offer over IPv4.

Q. 4 Explain MIPv6 and FMIPv6 for Micro mobility.

Q. 5 What is Cellular IP. Explain CIP architecture along with routing and paging procedure in CIP.

Q. 6 What are the problems with standard Mobile IP protocol? Explain how MIPv6 overcome these problems.

❑❑❑



Long Term Evolution of 3GPP

Syllabus

6.1 Long-Term Evolution (LTE) of 3GPP : LTE System Overview, Evolution from UMTS to LTE

6.2 LTE/SAE Requirements, SAE Architecture

6.3 EPS: Evolved Packet System, E-UTRAN, Voice over LTE (VoLTE), Introduction to LTE-Advanced,

6.4 System Aspects, LTE Higher Protocol Layers, LTE MAC layer, LTE PHY Layer,

6.5 Self Organizing Network (SON-LTE),SON for Heterogeneous Networks (HetNet), Introduction to 5G

Introduction

In chapter 2 we discussed about 2G (GSM , GPRS) and 3G (UMTS) networks. This chapter focuses on 4G network architecture LTE (Long Term Evolution). The chapter discusses detailed system architecture and other system aspects of Long Term Evolution (LTE). With LTE providing much higher data rate and low latency, it is also important that it supports voice transmission. VoLTE is a technology that transmits Voice over LTE network. Also Self Organizing Networks (SON) which supports dynamic configuration of LTE base stations (eNB) to automate the human efforts for setting up network has been discussed.

6.1 Long Term Evolution : Overview

6.1.1 LTE System Overview

- 3GPP stands for Third Generation Partnership Project.
- Under 3GPP, widely used 3G standards UMTS WCDMA/HSPA were developed.
- LTE (Long Term Evolution) is the 4G successor to the 3G UMTS system.
- LTE Provides much higher data speeds, low latency and greatly improved performance as well as lower operating costs.
- LTE came into market around in 2010. Initial deployments gave little improvement over 3G HSPA and were sometimes treated as 3.5G or 3.99G.
- Later the full capability of LTE was realized. It provided a full 4G level of performance.
- The first deployments were simply known as LTE, but later deployments were designated 4G LTE Advanced.

6.1.2 Evolution from UMTS to LTE

- Since the inception of cell phone technologies, many mobile generations have been seen.
- The first generation was analog (FM) technology, which is no longer available.
- The second generation (2G) brought **digital technology** into this. Multiple incompatible 2G standards were developed. Only two of them, GSM and IS-95A CDMA, have survived.
- Next, the third generation (3G) standards came into market. Again, multiple standards were developed, mainly WCDMA by the 3GPP and cdma 2000 by Qualcomm. Both have survived and are still used today.
- The 3G standards were continually updated into what is known as 3.5G.

- WCDMA was upgraded to HSPA, and cdma 2000 was expanded with 1xRTT EV-DO releases A and B. Both are still widely deployed.
- The Third Generation Partnership Project (3GPP), developed the widely used UMTS WCDMA/HSPA 3G standards. As a 4G successor to WCDMA, 3GPP developed Long-Term Evolution (LTE). Thus, LTE was created as an upgrade to the 3G standards.
- Release 8 of LTE was completed in 2010, followed by release 9. Now, release 10 is also available which defines
- LTE-Advanced (LTE-A) is also under development.

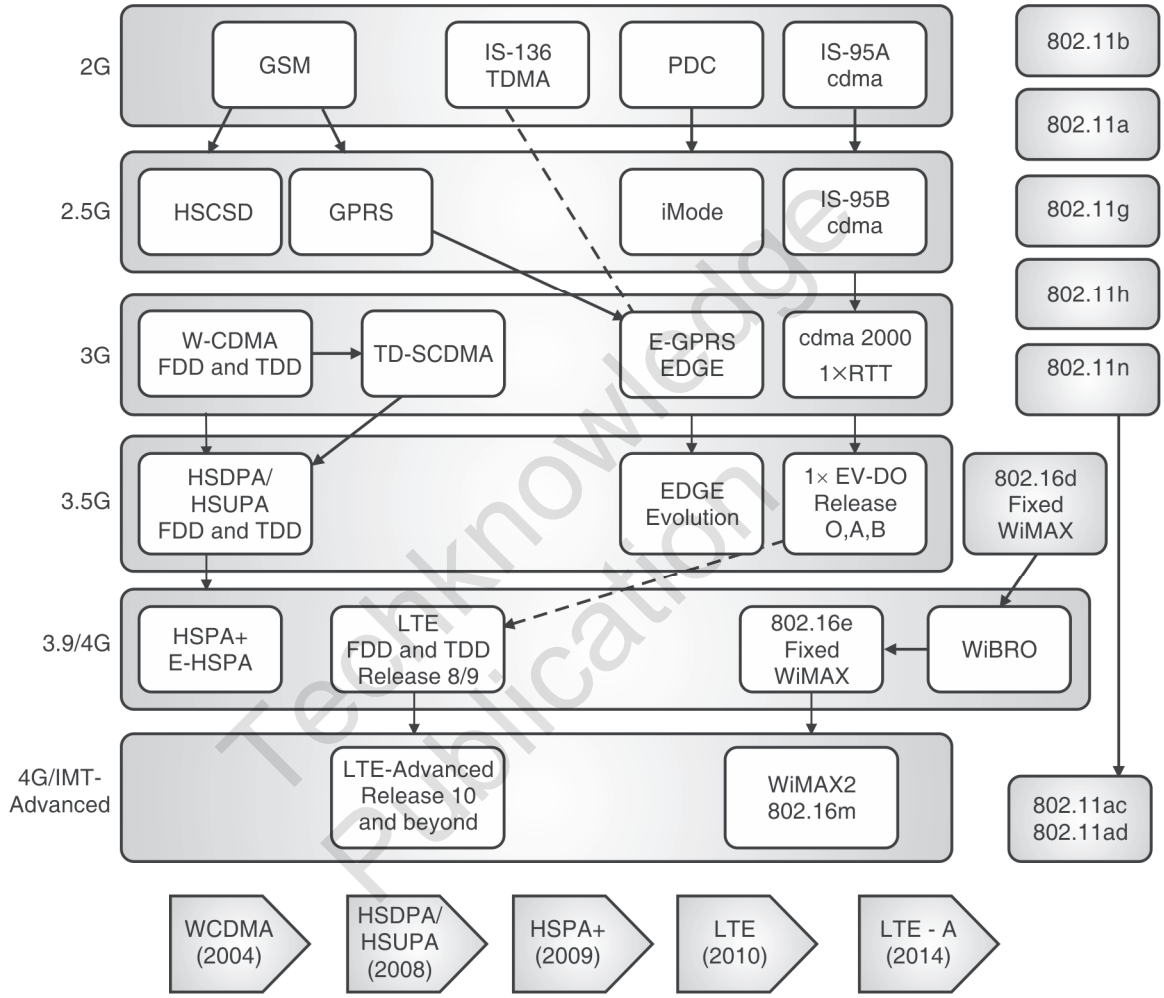


Fig. 6.1.1 : Evolution from UMTS to LTE

Table 6.1.1 : Comparison of all 3G and 4G technologies

Technology	WCDMA	HSPA	HSPA+	LTE	LTE-A
Release	Rel 99/4	Rel 5,6	Rel 7	Rel 8	Rel 9,10
Rollout	2003/4	2005-8	2009	2010	2014
Down link Rate	384Kbps	14 Mbps	28Mbps	150 Mbps	1Gbps
Uplink Rate	128 kbps	5,7 kbps	11Mbps	75M bps	
Delay	150 ms	100 ms	50 ms	10 ms	<10

6.2 SAE/LTE Architecture

6.2.1 SAE Requirements

- As the mobile communication generations evolved, radio interfaces also evolved.
- Soon it was realized that, the system architecture needs to be also evolved in order to support very **high data rate** and **low latency** requirements for 3G LTE.
- Requirement of SAE architecture for LTE includes:
  1. Flat architecture consisting of just one type of node, the base station, known as **eNodeB** in LTE.
  2. Effective protocols for the support of packet-switched services.
  3. Open interfaces and support of multivendor equipment interoperability.
  4. Efficient mechanisms for operation and maintenance, including self-optimization functionalities
  5. Support of easy deployment and configuration.

6.2.2 SAE Architecture

- System Architecture Evolution (SAE) is a new network architecture designed to simplify LTE networks. It establish a flat architecture similar to other IP based communications networks.
- SAE uses an eNB and Access Gateway (aGW) and removes the RNC and SGSN from the equivalent 3G network architecture. This allows the network to be built with an "All-IP" based network architecture.
- SAE also includes entities to allow full inter-working with other related wireless technology (WCDMA, WiMAX, WLAN, etc.). These entities can specifically manage and permit the non-3GPP technologies to interface directly with the network.
- The high-level network architecture of LTE is comprised of following three main components :
  (i) The User Equipment (UE)
  (ii) The Evolved UMTS Terrestrial Radio Access Network (E-UTRAN)
  (iii) The Evolved Packet Core (EPC)

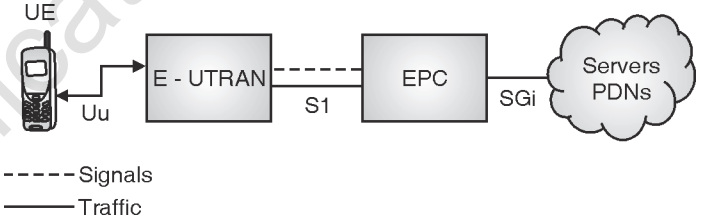


Fig. 6.2.1 : LTE reference model (High level network architecture)

- The evolved packet core (EPC) provides the means to communicate with packet data networks in the outside world such as the internet, private corporate networks or the IP multimedia subsystem.
- Between EU and E-UTRAN there is **Uu** interface,
- EPC is connected to E-UTRAN via **S1** interface and to the outside world via **SGi** interface.

6.2.2(a) Evolved Packet System (EPS)

- EPS refers to the architecture of the LTE mobile standard.
- It includes the Evolved Packet Core (EPC), the Radio Networks (E-UTRAN), the End User Equipment (UE) and the Services.
- EPS is based entirely on packet switching unlike legacy UMTS and GSM technologies that still use circuit switching .

6.2.2(b) The User Equipment (UE)

- UE is nothing but the mobile equipment.
- The internal architecture of the UE for LTE is identical to the one used by UMTS and GSM.

- The mobile equipment comprised of the following important modules:
  - **Mobile Termination (MT) :** This handles all the communication functions.
  - **Terminal Equipment (TE) :** This terminates the data streams.
  - **Universal Integrated Circuit Card (UICC) :** This is also known as the SIM card for LTE equipment. It runs an application known as the Universal Subscriber Identity Module (USIM).
- A **USIM** stores user-specific data very similar to 3G SIM card. This keeps information about the user's phone number, home network identity and security keys etc.

6.2.2(c) The E-UTRAN

The architecture of evolved UMTS Terrestrial Radio Access Network (E-UTRAN) has been illustrated in Fig. 6.2.2.

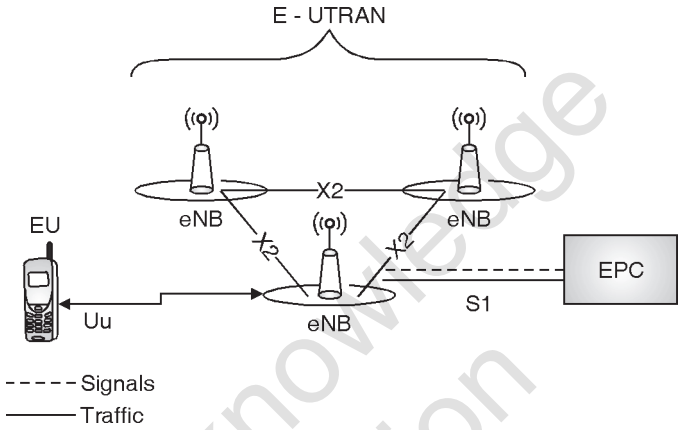


Fig. 6.2.2 : Architecture of E-UTRAN

- The E-UTRAN handles the radio communications between the mobile equipment (ME) and the evolved packet core (EPC). It contains only one component, the evolved base stations, called **eNodeB** or **eNB**.
- Each eNB is a base station that controls the mobiles in one or more cells.
- The base station that is currently communicating with a mobile is known as its serving eNB.
- Each eBN connects with the EPC by means of the S1 interface.
- Two nearby base stations can be connected via the X2 interface, which is mainly used for signaling and packet forwarding during handover.

6.2.2 (d) Evolved Packet Core (EPC) (The core network)

The architecture of Evolved Packet Core (EPC) is fully IP based has been illustrated in Fig. 6.2.3.

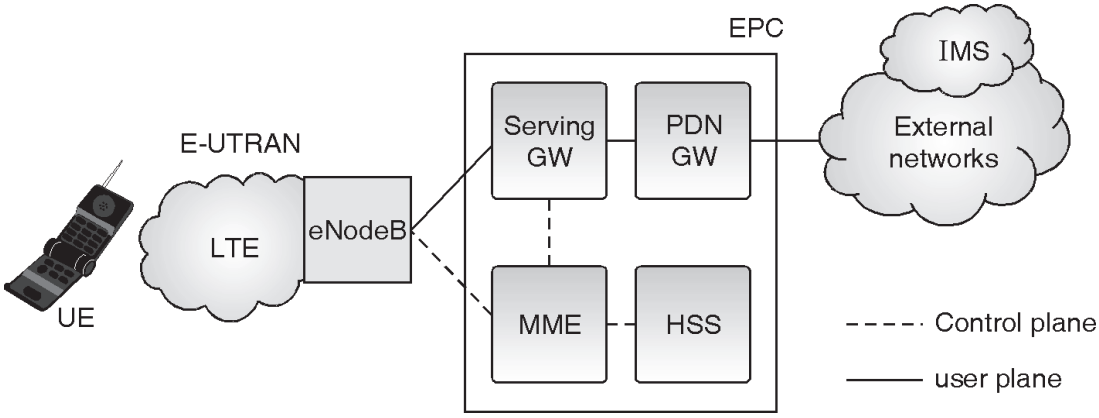


Fig. 6.2.3 : Basic EPS architecture

Evolved Packet Core (EPC) components

It contains following important components :

1. Serving GW

- The serving gateway (S-GW) acts as a router, and forwards data between the base station and the PDN gateway.
- It is also responsible for inter-eNB handovers in the U-plane.
- It provides mobility between LTE and other types of networks (such as between 2G/3G and P-GW).
- The SGW keeps context information such as parameters of the IP bearer and routing information, and stores the UE contexts when paging happens.
- It is also responsible for replicating user traffic for lawful interception.

2. PDN GW

The PDN GW is the point of interconnect between the EPC and the external IP networks. PDN GW routes packets to and from the PDNs. The functions of the PGW include :

- Policy enforcement
- Packet filtering
- Charging support
- Lawful interception
- Packet screening

3. HSS

- The HSS (for Home Subscriber Server) is a database that contains user-related and subscriber-related information.
- It is similar to - Home Location Register (HLR) and Authentication Centre (AuC) used in 3G networks.

4. MME

- The MME (for Mobility Management Entity) deals with the control plane.
- It handles the signaling related to mobility and security for E-UTRAN access. The MME is responsible for the tracking and the paging of UE in idle-mode. It is the termination point of the Non-Access Stratum (NAS).
- Fig. 6.2.4 shows the entire SAE architecture.

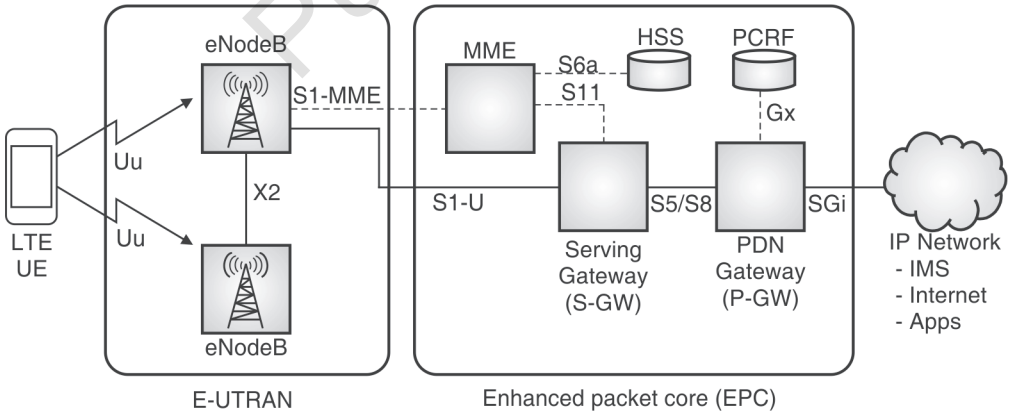


Fig. 6.2.4 : LTE/SAE Architecture

6.3 Voice over LTE (VoLTE)

- VoLTE stands for **V**oice **O**ver **L**ong **T**erm **E**volution.
- It is a digital packet voice service that is delivered over IP via an LTE access network.

- When 3GPP started designing the LTE system, prime focus was to create a system which can achieve **high data** throughput with **low latency**.
- LTE is an all IP network and the ability to carry voice was not given much importance. Therefore, for LTE networks to carry traditional circuit switched voice calls, a different solution was required.
- This solution to carry voice over IP in LTE networks is commonly known as "VoLTE". Basically VoLTE systems covert voice into data stream, which is then transmitted using the data connection.
- VoLTE is based on the IMS(IP multimedia system).
- IMS is an architectural framework for delivering multimedia communications services such as voice, video and text messaging over IP networks.

Voice over LTE - VoLTE basics

- VoLTE, Voice over LTE is an IMS (IP multimedia System) based technique.
- VoLTE enables the system to be integrated with the suite of other applications for LTE.
- To make implementation of VoLTE easy and cost effective to operators, cut down version of IMS network was defined. This not only reduced the number of entities required in the IMS network, but it also simplified the interconnectivity.
- This considerably reduced the costs for network operators as this had been a major issue for acceptance of IMS. The reduced IMS network for LTE has been shown in Fig. 6.3.1.

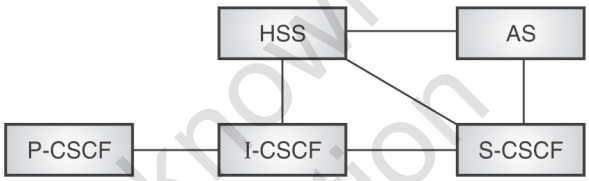


Fig. 6.3.1 : Reduced IMS network for VoLTE

The entities within the reduced IMS network used for VoLTE are explained below :

(i) IP-CAN IP, Connectivity Access Network : This consists of the EUTRAN and the MME.

(ii) P-CSCF, Proxy Call State Control Function : The P-CSCF is the user to network proxy. All SIP signaling to and from the user runs via the P-CSCF whether in the home or a visited network.

(iii) I-CSCF, Interrogating Call State Control Function : The I-CSCF is used for forwarding an initial SIP request to the S-CSCF. When the initiator does not know which S-CSCF should receive the request.

(iv) S-CSCF, Serving Call State Control Function : The S-CSCF performs a variety of actions within the overall system, and it has a number of interfaces to enable it to communicate with other entities within the overall system.

(v) AS, Application Server : It is the application server that handles the voice as an application.

(vi) HSS, Home Subscriber Server : The IMS HSS or home subscriber server is the main subscriber database used within IMS. The IMS HSS provides details of the subscribers to the other entities within the IMS network, enabling users to be granted access or not dependent upon their status.

The IMS calls for VoLTE are processed by the subscriber's S-CSCF in the home network. The connection to the S-CSCF is via the P-CSCF.

Benefits of VoLTE

The implementation of VoLTE offers many benefits, both in terms of cost and operation.

VoLTE provides following benefits :

- Provides a more efficient use of spectrum than traditional voice;
- Meets the rising demand for richer, more reliable services;

- Eliminates the need to have voice on one network and data on another;
- Can be deployed in parallel with video calls over LTE and multimedia services, including video share, multimedia messaging, chat and file transfer;
- Ensures that video services are fully interoperable across the operator community, just as voice services are,
- Increases handset battery life by 40 % (compared with VoIP);
- Provides rapid call establishment time.

6.4 Introduction to LTE-Advanced

- LTE Advanced adds a number of additional capabilities to the basic LTE to provide very much higher data rates and much better performance.
- LTE provides improved performance particularly at cell edges and other areas where performance would not normally have been so good.

6.4.1 LTE Advanced Key Features

The main aims for LTE Advanced :

- **Peak data rates :** Downlink - 1 Gbps; uplink - 500 Mbps.
- **Spectrum efficiency :** 3 times greater than LTE.
- **Peak spectrum efficiency :** Downlink - 30 bps/Hz; uplink - 15 bps/Hz.
- **Spectrum use :** The ability to support scalable bandwidth use and spectrum aggregation where non-contiguous spectrum needs to be used.
- **Latency :** From Idle to Connected in less than 50 ms.
- Cell edge user throughput to be twice that of LTE.
- Average user throughput to be 3 times that of LTE.
- **Mobility :** Same as that in LTE
- **Compatibility :** LTE Advanced shall be capable of interworking with LTE and 3GPP legacy systems.

These are many of the development aims for LTE Advanced.

6.4.2 LTE - Advanced : System Aspects

- The main new functionalities introduced in LTE-Advanced are;
  - Carrier Aggregation (CA)
  - Enhanced use of multi-antenna techniques (MIMO)
  - Support for Relay Nodes (RN)
- LTE-Advanced is the all IP based cellular networks that can offer higher user data rates and lower latency.
- In LTE-Advanced lower latency can be achieve by adopting terminal state of being idle or active. This can significantly reduce control plane latency and signaling compare to earlier generation.
- Higher user data rates can be achieved by adopting several techniques including: MIMO support, Modulation techniques like OFDM, bandwidth flexibility, and the support of FDD (Frequency Division Duplex) and TDD (Time Division Duplex) modes of operation.

6.4.2(a) Carrier Aggregation

- The increase in bandwidth in LTE-Advanced is achieved through aggregation of carriers. Carrier aggregation can be used for both FDD and TDD.

- Each aggregated carrier is referred to as a '**component carrier'**. The component carrier can have a bandwidth of 1.4, 3, 5, 10, 15 or 20 MHz.
- Maximum of five component carriers can be aggregated, hence the maximum bandwidth is 100 MHz.
- The number of aggregated carriers can be different in DownLink and UpLink; however the number of UpLink component carriers is never larger than the number of DownLink component carriers.

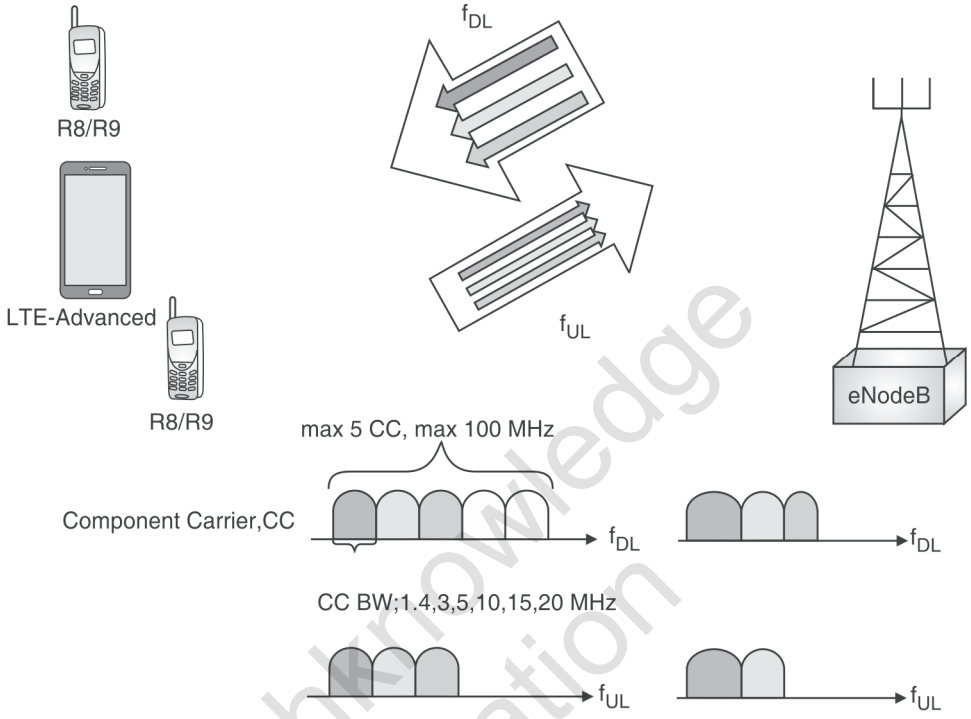


Fig. 6.4.1 : Carrier aggregation

- There are two types of carrier aggregation: continuous and non-continuous.
- In continuous aggregation, contiguous component carriers within the same operating frequency band are aggregated so called intra-band contiguous.
- For non-contiguous allocation it could either be intra-band, (i.e. the component carriers belong to the same operating frequency band, but are separated by a frequency gap) or it could be inter-band, in which case the component carriers belong to different operating frequency bands (Refer Fig. 6.4.2)

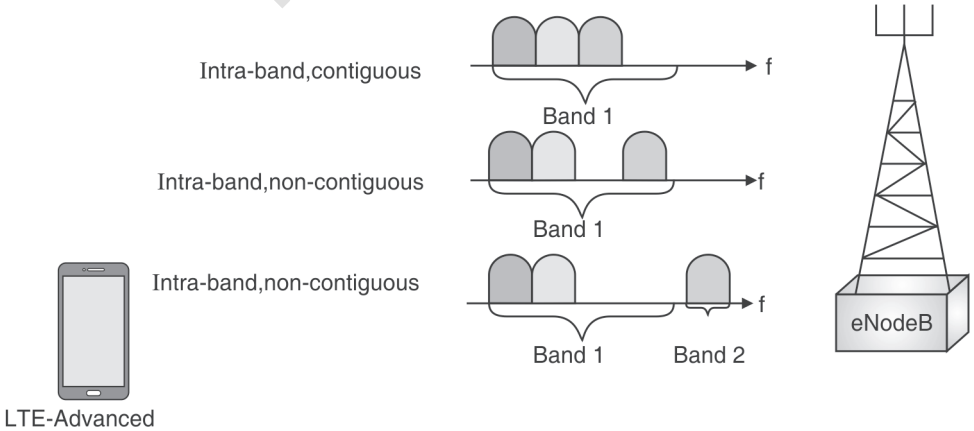


Fig. 6.4.2 : Intra and Inter band carrier aggregation

- For each component carrier there is a one **serving cell**.
- The coverage of the serving cells may differ due to the component carrier frequencies.

- The RRC connection is handled by one cell called the Primary serving cell, served by the Primary component carrier.
- The other component carriers are all referred to as **Secondary component carrier** serving the Secondary serving cells.

6.4.2(b) MIMO (Multiple Input and Multiple Output)

MIMO is used to increase the overall bitrate through transmission of two or more different data streams on two or more different antennas.

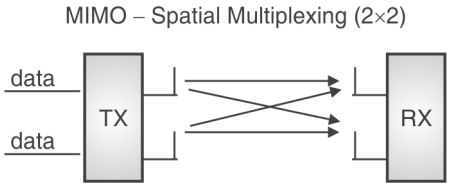
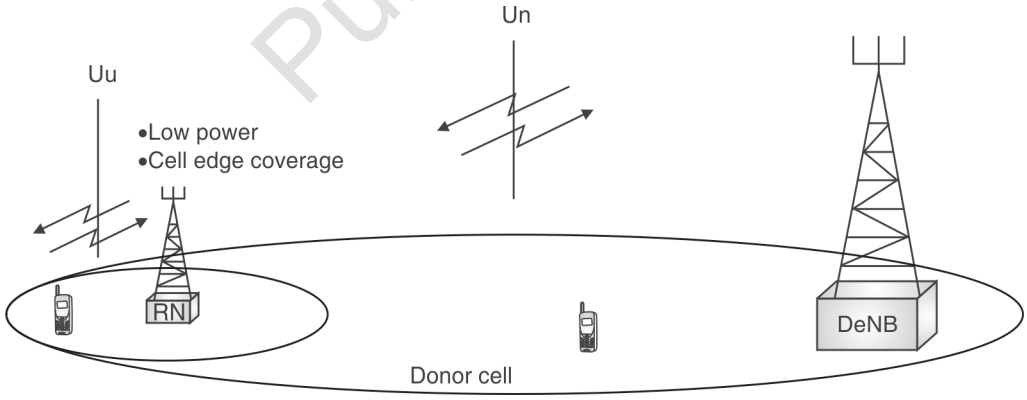


Fig. 6.4.3 : MIMO

A major change in LTE-Advanced is the introduction of 8x8 MIMO in the Down Link and 4x4 in the Up link.

6.4.2(c) Relay Nodes

- In LTE-Advanced, the heterogeneous network planning i.e. a mix of large and small cells is possible through Relay Nodes (RNs).
- The Relay Nodes are low power base stations that provides enhanced coverage and capacity at cell edges. It also serves as hot-spot areas and it can also be used to connect to remote areas without fiber connection.
- The Relay Node is connected to the Donor eNB (DeNB) via a radio interface, **Un**.
- Un is a modification of the E-UTRAN air interface Uu.
- In the Donor cell the radio resources are shared between UEs served directly by the DeNB and the Relay Nodes.
- When the Uu and Un use different frequencies the Relay Node is referred to as a **Type 1a RN**
- When Uu and Un uses the same frequencies, it is called **Type 1 RN**.
- In case of Type 1RN, there is a high risk for self interference in the Relay Node, when receiving on Uu and transmitting on Un at the same time (or vice versa). This can be avoided through time sharing between Uu and Un, or having different locations of the transmitter and receiver.



f=f, inband, type 1 Relay Node – risk for self interference

f≠ f, outband, type 1a Relay Node

Fig. 6.4.4 : Network extension using Relay Node

- Fig. 6.4.4 shows the Relay Node (RN) is connected to the DeNB via the radio interface Un. UEs at the edge of the donor cell are connected to the RN via Uu, while UEs closer to the DeNB are directly connected to the DeNB via the Uu interface. The frequencies used on Un and Un can be different, outband, or the same, inband.

6.4.2(d) Coordinated Multipoint (CoMP)

One of the key issues with many cellular systems is that of poor performance at the cell edges. To improve the performance at cell edges, LTE-Advanced introduces coordinated multipoint (CoMP) scheme.

In CoMP there are two important components :

1. TX (Transmit) points
2. RX (Receive) Points

- A number of TX points provide coordinated transmission in the DL (DownLink).
- Similarly a number of RX points provide coordinated reception in the UL (UpLink).
- A TX/RX-point constitutes of a set of co-located TX/RX antennas providing coverage in the same sector.
- The set of TX/RX-points used in CoMP can either be at different locations, or co-sited but providing coverage in different sectors. They can also belong to the same or different eNBs.
- In Fig. 6.4.5 two simplified examples for DL CoMP is shown.

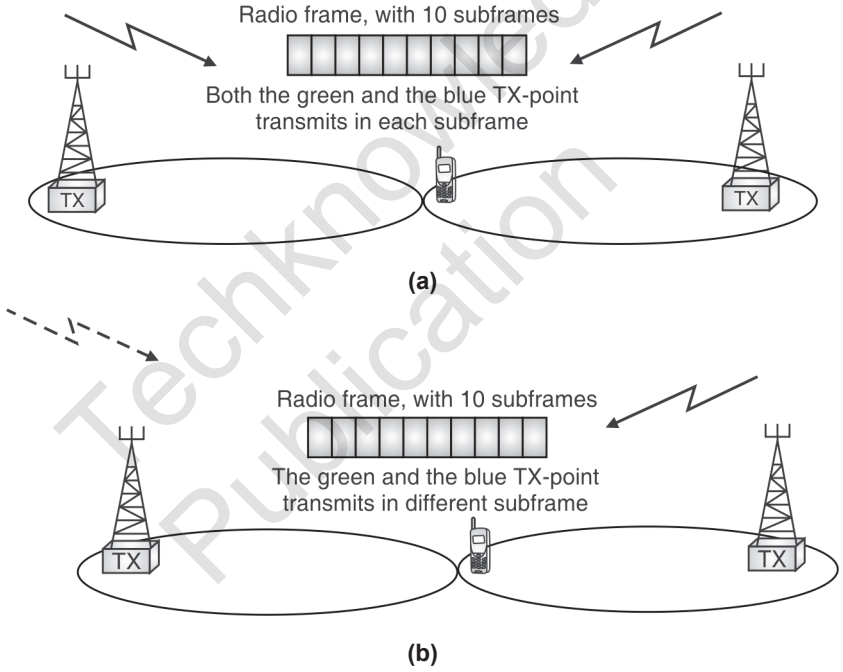


Fig. 6.4.5 : Down Link CoMP (a) Joint Transmission (b) Dynamic point selection

- In both these cases Down link (DL) data is available for transmission from two TX-points. When two, or more,
- TX-points, transmit on the same frequency in the same subframe it is called Joint Transmission.
- When data is available for transmission at two or more TX-points but only scheduled from one TX-point in each subframe it is called Dynamic Point Selection.
- In case of Uplink (UL) CoMP, there is a Joint Reception i.e. a number of RX-points receive the UL data from one UE, and the received data is combined to improve the quality.
- When CoMP is used additional radio resources for signaling is required e.g. to provide UE scheduling information for the different DL/UL resources.

6.4.3 LTE Advanced Architecture

6.4.3(a) Architecture

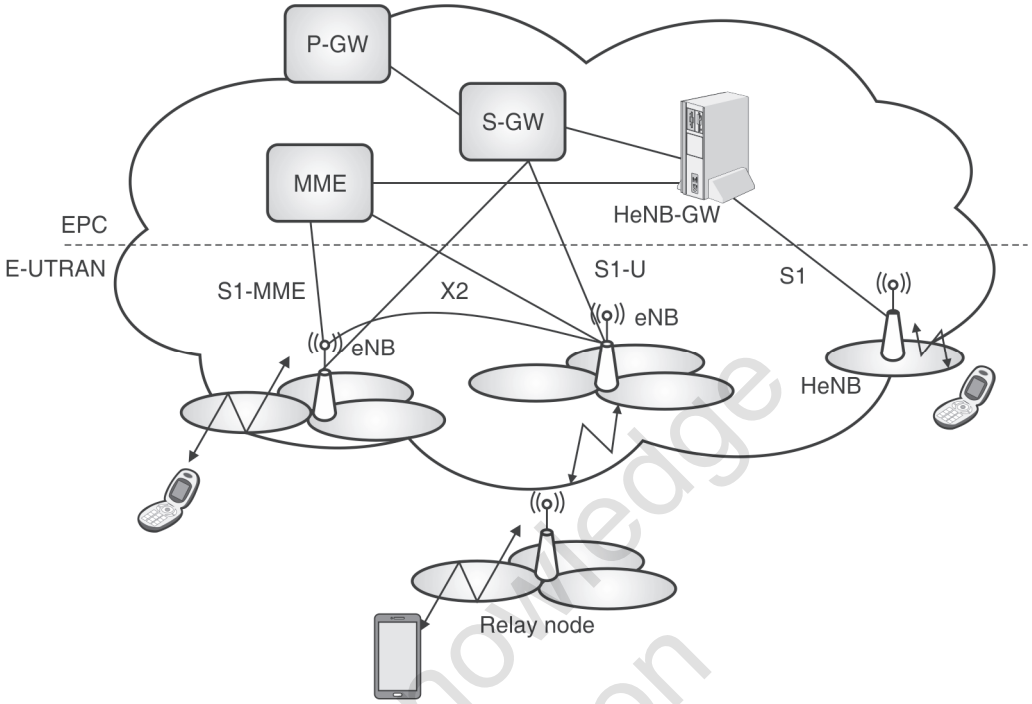


Fig. 6.4.6 : LTE Advanced architecture

- The Fig. 6.4.6 depicts LTE Advanced (LTE-A) Architecture for E-UTRAN.
- It consists of P-GW, S-GW, MME, S1-MME, eNB, HeNB, HeNB-GW and Relay Node etc. Following are the functions of these architecture entities.

P-GW

- It stands for PDN Gateway.
- It interfaced with S-GW using S5 interface and with operator's IP services using SGi interface.
- It has connectivity with PCRP using Gx interface.
- It connects UE to packet data networks.
- P-GW assigns IP address to the UE. One UE can have connectivity with more than one PGWs in order to have access to multiple PDNs.
- It takes care of packet filtering, policy enforcement and charging related services. Moreover it fulfils connectivity between 3GPP (LTE, LTE-A) and non 3GPP (WiMAX, CDMA etc.) technologies.

S-GW

- It stands for Serving Gateway.
- It interfaces with MME using S11 interface and with SGSN using S4 interface.
- It connects with PDN-GW using S5 interface as mentioned above.
- EPC gets terminated at this node/entity. It is connected with E-UTRAN via S1-U interface.
- Each UE in LTE-A is associated to unique S-GW which has several functions.

- It helps in inter-eNB handover as well as inter-3GPP mobility.
- It helps in inter-operator charging. It does packet routing and packet forwarding.

MME

- It stands for Mobility Management Entity.
- It is major control plane element in LTE advanced architecture.
- It takes care of authentication, authorization and NAS signaling related security functions.
- It takes care of selecting either S-GW or PDN-GW or P-GW.

S1-MME

It provides connectivity between EPC and eNBs.

eNB

- It is main building block or system in LTE-A.
- It provides interface with UEs or LTE-A phones.
- It has similar functionality as base station used in GSM or other cellular systems.
- Each of the eNBs serve one or several E-UTRAN cells. Interface between two eNBs is known as X2 interface.

HeNB

- It stands for Home eNodeB or Home eNB.
- It is known as Fem to cell.
- It is used to improve coverage in the indoor region of office or home premises.
- It can be interfaced directly to EPC or via Gateway.

HeNB-GW

- It provides connectivity of HeNB with S-GW and MME.
- It aggregates all the traffic from number of Home eNBs to core network.
- It uses S1 interface to connect with HeNBs.

Relay Node :

It is used for improving network performance.

6.4.3(b) Comparison of LTE and LTE-A

- Both the LTE and LTE-Advanced are fourth generation wireless technologies designed to use for high speed broadband internet access.
- The specifications are published by 3rd Generation Partnership Project (3GPP).
- LTE is specified in 3GPP release 8 and LTE Advanced is specified in 3GPP release 10.
- LTE is the short form of Long Term Evolution. It uses FDD and TDD duplex modes for the UEs to communicate with the eNodeB. The LTE uses OFDMA modulation in the downlink (from eNodeB to UEs) and SC-FDMA modulation in the uplink. Various physical channels and logical channels are designed to take care of data as well as control information. It supports peak data rate of 300MBPS in the downlink and 75MBPS in the uplink (theoretically).
- TE-Advanced is the upgraded version of LTE technology to increase the peak data rates to about 1GBPS in the downlink and 500MBPS in the uplink. In order to increase the data rates LTE-Advanced utilizes higher number of antennas and added carrier aggregation feature.
- Table 6.4.2 summarizes the key differences between LTE and LTEA.

Table 6.4.2 : Difference between LTE and LTEA

Specifications	LTE	LTE Advanced
Standard	3GPP Release 9	3GPP Release 10
Bandwidth	Supports 1.4MHz, 3.0MHz, 5MHz, 10MHz, 15MHz, 20MHz	70MHz Downlink(DL), 40MHz Uplink(UL)
Data rate	300 Mbps Downlink(DL) 4x4MIMO and 20MHz, 75 Mbps Uplink(UL)	1Gbps Downlink(DL), 500 Mbps Uplink(UL)
Theoretical Throughput	About 100Mbps for single chain (20MHz,100RB,64QAM), 400Mbps for 4x4 MIMO. 25% of this is used for control/signaling (OVERHEAD)	2 times than LTE
Maximum No. of Layers	2(category-3) and 4(category-4,5) in the downlink, 1 in the uplink	8 in the downlink, 4 in the uplink
Maximum No. of codewords	2 in the downlink, 1 in the uplink	2 in the downlink, 2 in the uplink
Spectral Efficiency(peak,b/s/Hz)	16.3 for 4x4 MIMO in the downlink, 4.32 for 64QAM SISO case in the Uplink	30 for 8x8 MIMO in the downlink, 15 for 4x4 MIMO in the Uplink
PUSCH and PUCCH transmission	Simultaneously not allowed	Simultaneously allowed
Modulation schemes supported	QPSK, 16QAM, 64QAM	QPSK, 16QAM, 64QAM
Access technique	OFDMA (DL),DFTS-OFDM (UL)	Hybrid OFDMA(DL), SC-FDMA(UL)
Carrier aggregation	Not supported	Supported
Applications	Mobile broadband and VOIP	Mobile broadband and VOIP

6.4.4 LTE Protocol Stack

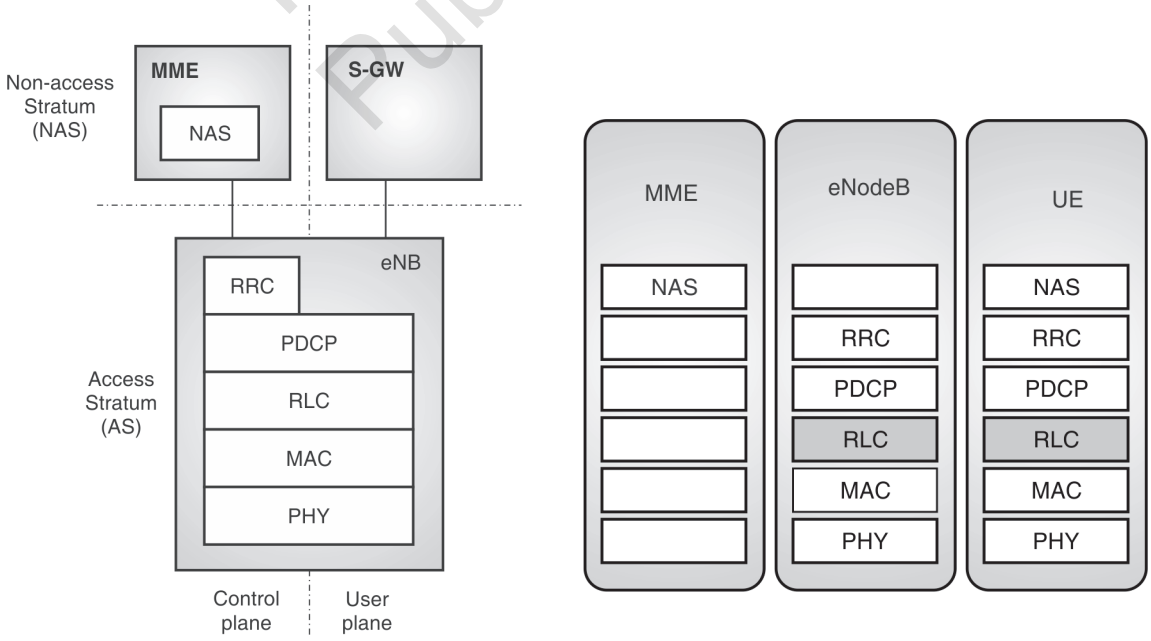


Fig. 6.4.7 : LTE Protocol stack

- Fig. 6.4.7 depicts LTE protocol stack. It is divided into two main parts - NAS (Non-Access Stratum) and AS (Access Stratum).
- Further it is categorized into **control plane** and **user plane**.
- User plane of eNB consists of PHY, MAC, RLC and PDCP layers.
- Control plane of eNB consists of these 4 layers and in addition RRC layer also.

Following are functions of each layer.

PHY

- This layer takes care of frame formation as per TDD or FDD topology and as per OFDMA structure.
- Moreover, it takes care of modulation and coding of different control and traffic channels.
- It covers scrambling and codeword to layer mapping functionalities.
- It incorporates reference signals which are used for channel estimation and channel equalization.

MAC-Medium Access Control

It takes care of following functions :

- Multiplexing/demultiplexing of RLC Packet Data Units (PDUs).
- Scheduling information reporting.
- Error correction through Hybrid ARQ (HARQ).
- Local Channel Prioritization.
- Padding.

RLC-Radio Link Control

- Error correction through Automatic Repeat reQuest (ARQ).
- Segmentation according to the size of the transport block and re-segmentation in case a retransmission is needed.
- Concatenation of SDUs for the same radio bearer.
- Protocol error detection and recovery.
- In-sequence delivery.

PDCP-Packet Data Convergence Protocol

- Header compression.
- In-sequence delivery and retransmission of PDCP Session Data Units (SDUs).
- Duplicate detection.
- Ciphering and integrity protection.

RRC-Radio Resource Control

- Broadcast system information related to Non-Access Stratum (NAS) and Access Stratum (AS).
- Establishment, maintenance, and release of RRC connection.
- Security functions including key management.
- Mobility functions.
- QoS management functions.
- UE measurement reporting and control of the reporting.
- NAS direct message transfer between UE and NAS.

NAS-Non Access Stratum

Connection/session management between UE and the core network.

- Authentication.

- Registration.
- Bearer context activation/deactivation.
- Location registration management.

6.5 Higher Protocol Layers

Higher layer protocols include :

(i) Radio Link Control - RLC

(ii) Packet Data Convergence Protocol - PDCP and

(iii) Radio Resource Control - RRC

6.5.1 Radio Link Control (RLC)

- RLC – Radio Link Control protocol is a data link layer protocol (Layer 2 protocol).
- An RLC entity receives/delivers RLC SDUs from/to upper layer and sends/receives RLC PDUs to/from its peer RLC entity via lower layers.
- If RLC entity configured at the eNB, there is a peer RLC entity configured at the UE and vice versa. (Fig 6.5.1 (b)) RLC performs following major functions :
  - Error correction through Automatic Repeat reQuest (ARQ).
  - Segmentation according to the size of the transport block and re-segmentation in case a retransmission is needed.
  - Concatenation of SDUs for the same radio bearer.
  - Protocol error detection and recovery.
  - In-sequence delivery.

RLC Modes :

An RLC entity can be configured to perform data transfer in one of the following three modes.

1. Transparent Mode (TM)

- As the name suggests the Transparent mode entity in RLC does not add any overhead to the upper layer SDUs.
- The entity just transmits the SDUs coming from upper layer to MAC.

  In this mode :
  - Segmentation or reassembly of RLC SDUs is not allowed
  - No RLC headers are added.
  - Does not guarantees delivery
- RLC TM is used for transmission of paging messages on PCCH, system information transmitted on BCCH and SRB0 messages transmitted on CCCH.

2. Unacknowledged Mode (UM)

RLC Unacknowledged Mode is used for transmission of **delay sensitive packets**, such as VoIP packets or audio/video streams.

In this mode :

- Segmentation or reassembly of RLC SDUs is allowed
- RLC headers are added.
- Does not guarantees delivery
- This mode is suitable for carrying streaming traffic.

3. Acknowledged Mode (AM)

RLC AM is used both in user plane and control plane packets. But in both the cases PDCP is the upper layer. So all the SDUs which come to RLC AM entity are security protected.

In this mode :

- Segmentation or reassembly of RLC SDUs is allowed
- RLC headers are added.
- Guarantees In-sequence delivery of SDUs. It supports HARQ mechanism to retransmit lost PDUs.
- This mode is suitable for carrying TCP traffic.

RLC PDU (Protocol Data Unit)

- RLC PDUs can be categorized into RLC data PDUs and RLC control PDUs.
- RLC data PDUs are used by TM, UM and AM RLC entities to transfer upper layer PDUs (i.e. RLC SDUs).
- RLC control PDUs are used by AM RLC entity to perform ARQ procedures.

6.5.2 Packet Data Convergence Protocol (PDCP)

The PDCP layer is located above the RLC layer and below the IP layer (in the user plane) or the RRC layer (in the control plane).

- PDCP is a kind of interface between inside world and outside world.
- In other words, the data coming into the eNB first go through PDCP and then gets into RLC (Downlink). Data waiting in RLC trying to go out to the outside world has to go through PDCP to reach outside world(Uplink Path)

The major functions of PDCP layer

The major functions of PDCP layer are as follows.

- Header compression
- In-sequence delivery and retransmission of PDCP Session Data Units (SDUs)
- Duplicate detection
- Ciphering and integrity protection

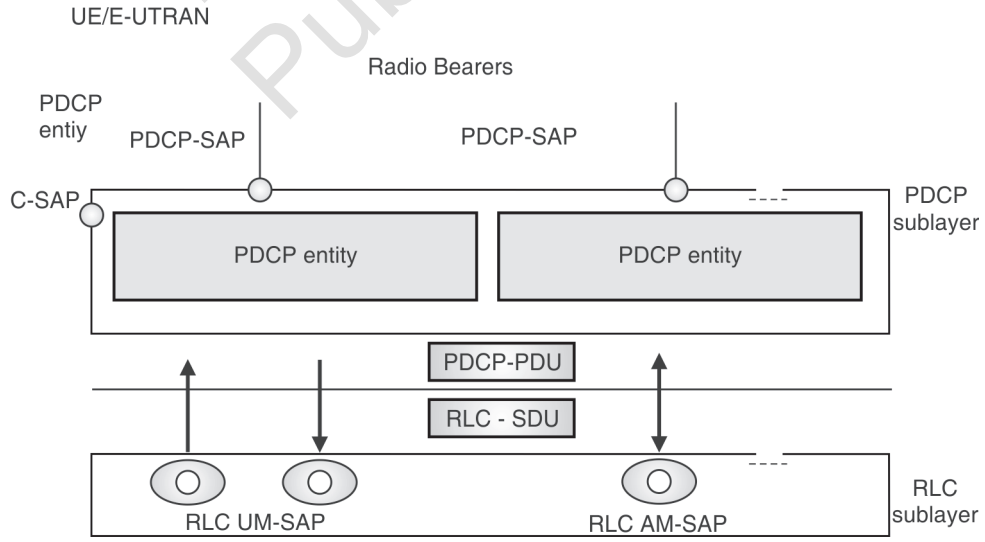


Fig. 6.5.1 : PDCP layer, structure view

- PDCP is directly connected to RLC Layer (RLC UM and RLC AM). Note that PDCP has no connection to RLC TM mode, meaning RLC TM mode data does not go through PDCP.

– Fig. 6.5.2 gives the complete functional overview of the PDCP

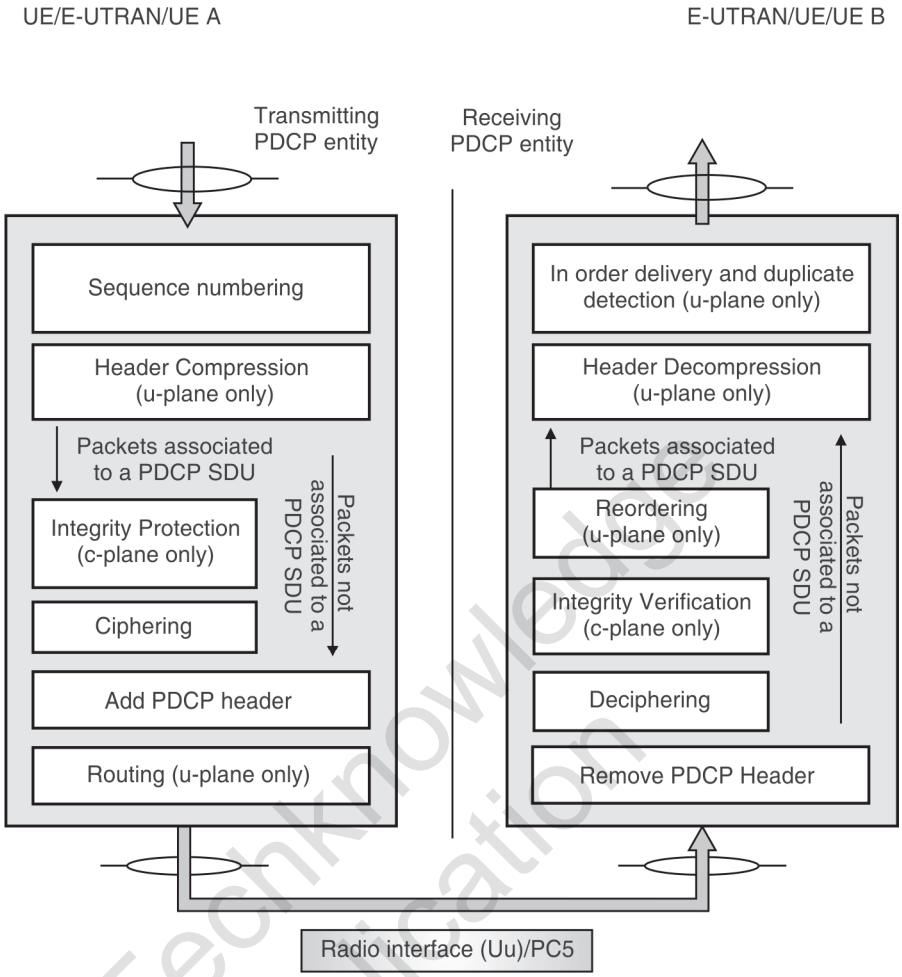


Fig. 6.5.2 : Functional overview of PDCP

6.5.3 Radio Resource Control (RRC)

– The RRC is the highest layer in the control plane of the Access Stratum (AS).

– The RRC layer controls communications between a UE and an eNB at the radio interface and the mobility of a UE crossing cells.

– The RRC also transfers messages of the Non-Access Stratum (NAS), which is located above the RRC layer.

– NAS messages are used to control communications between a UE and the Evolved Packet Core (EPC).

The main services and functions of the RRC sublayer include :

– Broadcast of System Information related to the non-access stratum (NAS)

– Broadcast of System Information related to the access stratum (AS)

– Paging

– Establishment, maintenance and release of an RRC connection between the UE and E-UTRAN

– Security functions including key management

– Establishment, configuration, maintenance and release of point to point Radio Bearers

– Mobility functions

- QoS management functions
- UE measurement reporting and control of the reporting
- NAS direct message transfer to/from NAS from/to UE.

6.6 LTE MAC Layer

As discussed earlier the MAC layer of LTE performs following functions.

- Error correction through Hybrid ARQ (HARQ).
- Logical channel to transport channel mapping
- Logical Channel Prioritization.
- Scheduling information reporting.
- Multiplexing/demultiplexing of RLC Packet Data Units (PDUs).

6.6.1 Error Correction through Hybrid ARQ

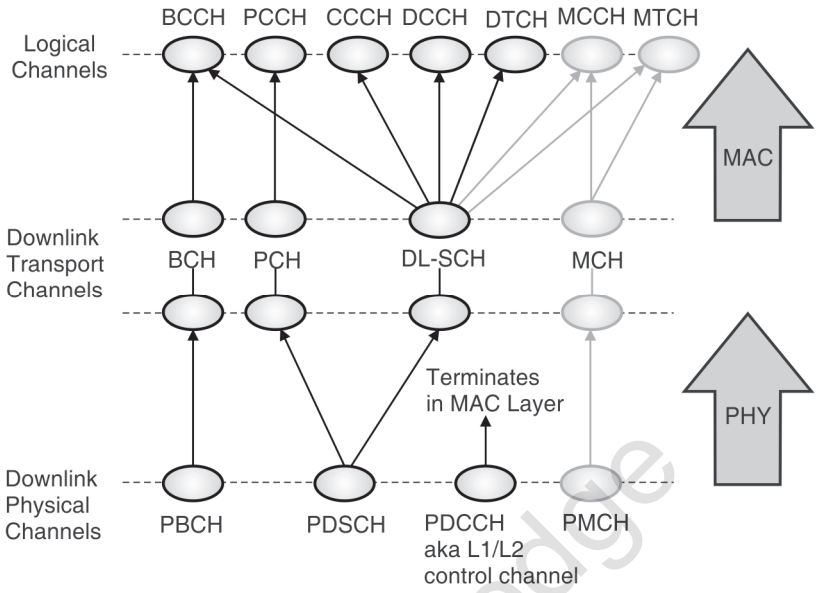
- The Hybrid Automatic Repeat-reQuest (HARQ) process is done in combination between the MAC and the PHY layer.
- The PHY performs the retention and re-combination and the MAC performs the management and signaling.
- The MAC indicates a NACK whenever there's a transport block (TB) CRC failure; the PHY usually indicates that failure.
- Retransmission is done by the eNodeB or the sender on the downlink using a different type of coding.
- The coding is sent and maintained in buffers in the eNodeB. Eventually, after one or two attempts, there will be enough data to reconstruct the signal.
- In HARQ operation, the retransmission does not have to be fully correct. It has to be correct enough that it can be combined mathematically with the previous transport block (TB) in order to produce a good transport block.

These are the basic steps of the HARQ process :

1. MAC sends "NACK" message when transport block (TB) fails CRC check.
2. Transport blocks with errors are retained.
3. PHY retransmits with different puncturing code
4. Retransmission is combined with saved transport block(s)
5. When correct transport block is decoded, MAC signals "ACK"
6. Multiple HARQ processes can run in parallel to retry several outstanding TBs.

6.6.2 Logical Channels to Transport Channel Mapping

- **Logical channels** exist at the top of the MAC. Types of logical channels include control channels (for control plane data) and traffic channels (for user plane data)
- **Transport channels** are in the transport blocks at the bottom of the MAC. They represent data transfer services offered by the PHY and are defined by how the information is carried, different physical layer modulations and the way they are encoded.
- When a valid transport block is available from the HARQ process, the transport channels are mapped to logical channels.
- Fig. 6.6.1 shows the mapping of logical channels to transport channels.



Logical Channels	Transport Channels
o PCCH : Paging Control Channel o BCCH : Broadcast Control Channel o CCCH : Common Control Channel o DCCH : Dedicated Control Channel o DTCH : Dedicated Traffic Channel o MCCH : Multicast Control Channel o MTCH : Multicast Traffic Channel	o PCH : Paging Channel o BCH : Broadcast Channel o DL-SCH : Downlink Shared Channel o MCH : Multicast Channel

Fig. 6.6.1 : Logical channels to Physical channel mapping for Down link

- Fig. 6.6.1 shows the physical layer control channel at the bottom of the picture.
- It is used for scheduling, signaling and other low-level functions.
- The downlink shared channel contains both a transport channel for paging and for downlink. The physical broadcast channel goes all the way through for broadcast.
- Multicast channels are grayed out in Fig. 6.6.1 because they are not being specified in Release 8 of the LTE standard. These channels will be re-addressed in Release 9.

Fig. 6.6.1 illustrates the following logical channels :

(i) Dedicated Traffic Channel (DTCH) : A point-to-point channel, dedicated to one UE, for the transfer of user information. A DTCH can exist in both uplink and downlink.

(ii) Broadcast Control Channel (BCCH) : A downlink channel for broadcasting system control information.

(iii) Paging Control Channel (PCCH) : A downlink channel that transfers paging information. This channel is used when the network does not know the location cell of the UE.

(iv) Common Control Channel (CCCH) : Uplink channel for transmitting control information between UEs and network. This channel is used by the UEs having no RRC connection with the network.

(v) Dedicated Control Channel (DCCH) : A point-to-point bi-directional channel that transmits dedicated control information between a UE and the network. Used by UEs that have an RRC connection.

6.6.3 Logical Channel Prioritization

- When the radio resources for a new transmission are allocated, the logical channel prioritization entity instructs the multiplexing and de-multiplexing entity to generate MAC PDUs from the MAC SDUs.
- The logical channel prioritization entity also decides how much data from each configured logical channel should be included in each MAC PDU whenever radio resource for a new transmission is available.

6.6.4 Scheduling

- Scheduling is a process through which eNodeB decides which UEs should be given resources (RBs), how much resource (RBs) should be given to send or receive data.
- In LTE, scheduling is done at per subframe basis i.e. every 1 mili second.
- Resources are composed of Physical Resource Blocks (PRB) and Modulation Coding Scheme (MCS).
- The MCS determines the bit rate, and thus the capacity, of PRBs.

  An LTE scheduler performs following function for efficient scheduling :

  (i) Link Adaptation : It selects the optimal combination of parameters such as modulation, channel Coding and transmit schemes.

  (ii) Rate Control : It is in charge of resource allocation among radio bearers of the same UE which are available at the eNB for DL and at the UE for UL.

  (iii) Packet Scheduler : It controls access to air interface resources amongst all active Users.

  (iv) Resource Assignment : It allocates air interface resources to selected active users on per TTI basis.

  (v) Power Control : Provides the desired SINR level for achieving the desired data rate, but also controls the interference to the neighbouring cells.

  (vi) HARQ (ARQ + FEC) : It allows recovering from residual errors by link adaptation.

6.7 PHY Layer

6.7.1 Generic Frame Structure

- The LTE specifications define both FDD and TDD modes of operation.
- The generic frame structure shown in Fig. 6.7.1 applies to both the DL and UL for FDD operation.

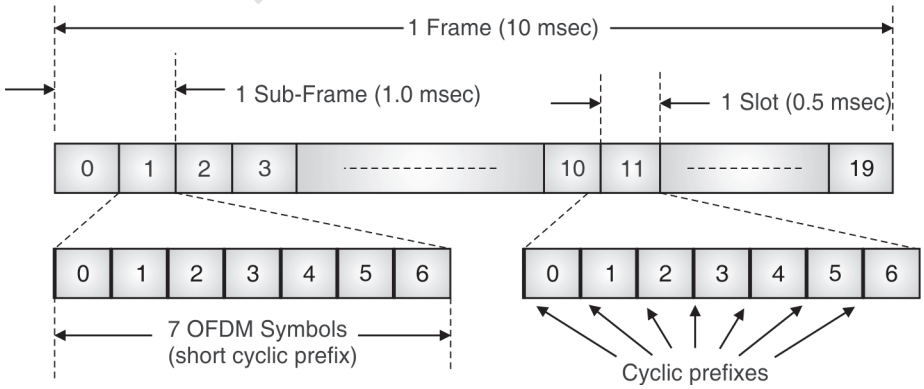


Fig. 6.7.1 : LTE Generic Frame Structure

- In OFDMA, users are allocated a specific number of subcarriers for a predetermined amount of time. These are referred to as physical resource blocks (PRBs) in the LTE specifications.

- PRBs thus have both a time and frequency dimension.
- Allocation of PRBs is handled by a scheduling function at eNodeB.
- LTE transmissions are segmented into frames, which are 10 msec in duration.
- One frames consist of 20 slot periods of 0.5 msec.
- Sub-frames contain two slot periods and are 1.0 msec in duration.

Downlink

- The LTE PHY specification accommodates bandwidths from 1.25 MHz to 20 MHz.
- The basic modulation scheme is OFDM which is very robust in the presence of severe multipath fading.
- Downlink multiplexing is accomplished via **OFDMA**.
- The DL supports physical channels, which convey information from higher layers in the LTE stack.
- Physical channels map to transport channels, which are service access points (SAPs) for the L2/L3 layers.
- Depending on the assigned task, physical channels and signals use different modulation and coding parameters.

6.7.2 Downlink Multiplexing

- OFDMA is the basic multiplexing scheme employed in the LTE downlink.
- In OFDMA, groups of 12 adjacent subcarriers are grouped together on a slot-by-slot basis to form physical resource blocks (PRBs).
- A PRB is the smallest unit of bandwidth assigned by the base station scheduler.

6.7.3 Physical Channels

- Three different types of physical channels are defined for the LTE downlink.
- LTE DL physical channels are :
  - Physical Downlink Shared Channel (PDSCH)
  - Physical Downlink Control Channel (PDCCH)
  - Common Control Physical Channel (CCPCH)
- Physical channels are mapped to specific transport channels.
- Transport channels are SAPs for higher layers.
- Each physical channel has defined algorithms for: Bit scrambling , Modulation, Layer mapping , CDD precoding , Resource element assignment Layer mapping and pre-coding are related to MIMO applications.

6.7.4 Transport Channels

Transport channels are included in the LTE PHY and act as service access points (SAPs) for higher layers.

Downlink Transport channels

1. **Broadcast Channel (BCH)**
   - Fixed format
   - Must be broadcast over entire coverage area of cell
2. **Downlink Shared Channel (DL-SCH)**
   - Supports Hybrid ARQ (HARQ)
   - Supports dynamic link adaption by varying modulation, coding and transmit power

- Suitable for transmission over entire cell coverage area
- Suitable for use with beam forming
- Support for dynamic and semi-static resource allocation
- Support for discontinuous receive (DRX) for power save

3. Paging Channel (PCH)

- Support for UE DRX
- Requirement for broadcast over entire cell coverage area
- Mapped to dynamically allocated physical resources

4. Multicast Channel (MCH)

- Requirement for broadcast over entire cell coverage area
- Support for MB-SFN
- Support for semi-static resource allocation

6.7.5 Mapping Downlink Physical Channels to Transport Channels

Transport channels are mapped to physical channels as shown in Fig. 6.7.2 Supported transport channels are :

1. Broadcast channel (BCH)
2. Paging channel (PCH)
3. Downlink shared channel(DL-SCH)
4. Multicast channel (MCH)

Transport channels provide the following functions :

- Structure for passing data to/from higher layers
- Mechanism by which higher layers can configure the PHY
- Status indicators (packet error, CQI etc.) to higher layers
- Support for higher-layer peer-to-peer signaling

6.8 Self Organizing Network (SON-LTE)

- SON stands for Self Organizing Network.
- It means that just add an **eNB** wherever you want to put and just connect power and switch on, it would configure all of its configuration by itself and makes itself ready for service.
- SON is like a 'Plug-and-Play' functionality.

  Normally when a system operator constructs a network, they go through following steps.

  (i) Network Planning

  (ii) Bring the hardware (e.g., eNB) to the locations determined at Network Planning Process

  (iii) Hardware installation

  (iv) Basic configuration

  (v) Optimizing parameters
- The main goal of SON is to automate large portions of human efforts involved in above mentioned process.
- In a more general way SON frame work can be illustrated in Fig. 6.8.1.

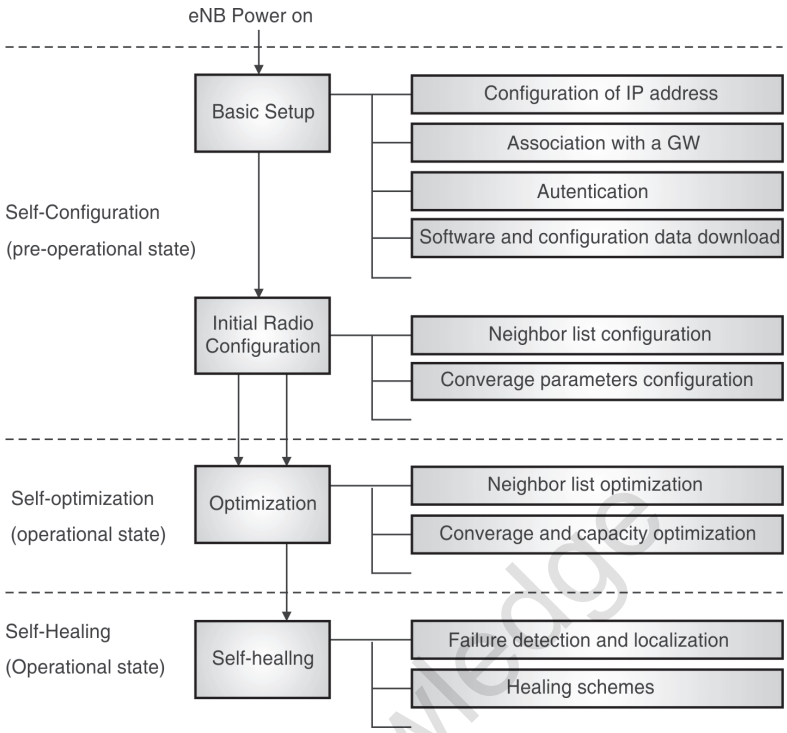


Fig. 6.8.1 : SON Framework

SON Architectures

- The self-organization functionality can be located at one place even split in different nodes.
- Self-Optimization algorithms can be located in OAM or eNB or both of them.
- According to the location of optimization algorithms, SON can be divided into the three main architectures:

1. Centralized SON
2. Distributed SON
3. Hybrid SON

- The all three versions differ with respect to data acquisition, data processing and configuration management.

1. Centralized SON

- In Centralized SON, optimization algorithms are stored and executed from the OAM System. Here, the SON functionality resides in a small number of locations, at a high level in the architecture.
- Fig. 6.8.2 shows an example of Centralized SON. Here, all SON functions are located in OAM systems, so it is easy to deploy them but does not support those simple and quick optimization cases.
- To implement Centralized SON, existing Northbound Interface (Itf-N), which is the interface between the Element Manager and the Network Manager, needs to be extended.
- Also, as the number of nodes in the network increases, computational requirements will also increase, which might cause problems in scalability.

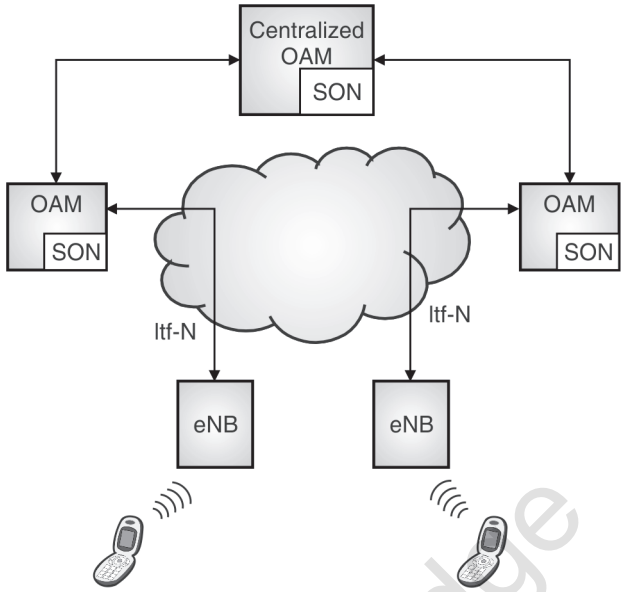


Fig. 6.8.2 : Centralized SON

2. Distributed SON

- In Distributed SON, optimization algorithms are executed in eNBi. SON functionality resides in many locations at a relatively low level in the architecture.
- This increases the deployment efforts.
- Fig. 6.8.3 shows an example of Distributed SON. When this architecture is implemented in large number of nodes, it has to be ensured that there is a coordination between them so that the network as a whole is optimised.

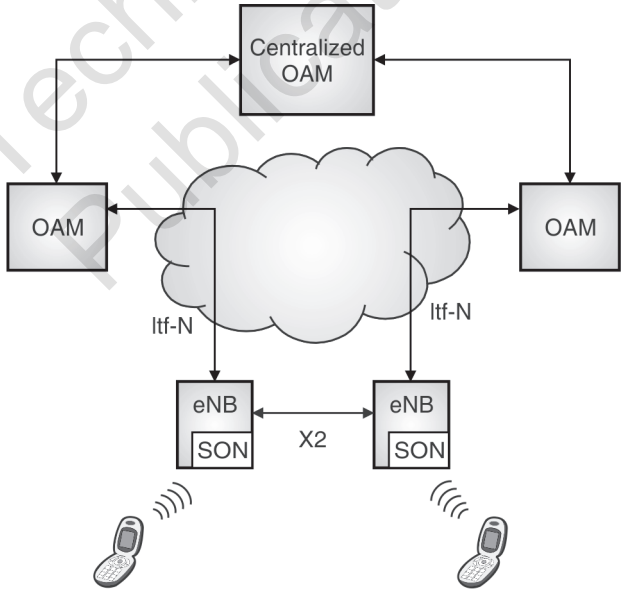


Fig. 6.8.3 : Distributed SON

3. Hybrid SON

- In Hybrid SON, part of the optimization algorithms are executed in the OAM system, while others are executed in eNB.
- Fig. 6.8.4 shows an example of Hybrid SON.
- In Hybrid SON, simple and quick optimization schemes are implemented in eNB and complex optimization schemes

are implemented in OAM so as to provide flexibility to support different kinds of optimization cases.

- But on the other hand, it costs lots of deployment effort and interface extension work.

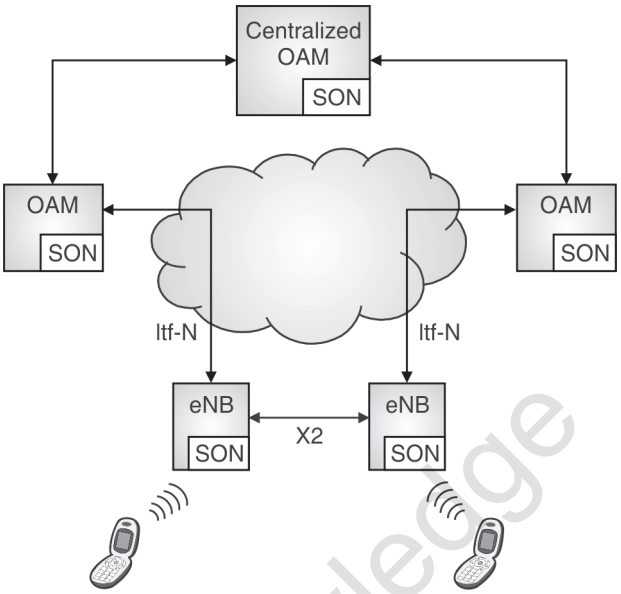


Fig. 6.8.4 : Hybrid SON

6.9 SON for Heterogeneous Networks (HetNet)

- It is assumed that there will be 50 billion connected devices by 2020. Demands for higher data rates continues to increase.
- High-quality video streaming, social networking and M2M communication over wireless networks are growing exponentially.
- Hence, a new paradigm called heterogeneous networks (HetNet) are being considered by network operators.
- HetNet stands for Heterogeneous Network, which involves a mix of radio technologies, different cell types, distributed antenna systems, and WiFi working together seamlessly.

  The HetNet involves several aspects :

  - Use of multiple radio access technologies
  - Operation of different cell sizes
  - Backhaul

Multiple Size cells

HetNet introduces two main types of cells : Small cells and Macro cells.

1. Small cells :

- **Small cells** have smaller coverage and capacity and are of three types. Micro , Pico and Femto cells. (Listed as in order of decreasing base station power).
- The idea of merging small cells with the macro cell network has the advantage of offloading traffic from the macro cell sites to the smaller cells while the macro cell operates at its normal capacity.
- Table 6.9.1 compared all the cells based on certain characteristics.

Table 6.9.1 : Properties of different cells

Characteristics	Femto	Pico	Micro	Macro
Indoor/Outdoor	Indoor	Indoor or out door	Out door	Outdoor
Number of users	4 to 16	32 to 100	200	200 to 1000++
Maximum output power	20 to 100mW	250 mW	2 to 10 W	40 to 100 W
Maximum cell radius	10 to 50 m	200 m	2km	10 to 40 km
Bandwidth	10 MHz	20 MHz	20 to 40 MHz	60 to 75 MHz
Technology	3G/4G/WiFi	3G/4G/WiFi	3G/4G/WiFi	3G/4G
Backhauls	DSL, Cable, fiber	Microwave, millimeter wave	Fiber, Microwave	Fiber, Microwave

- Small cells are deployed in hotspots to increase capacity. Hotspots are the areas where user density is more. They are also deployed to fill in the areas not covered by the macro network (E.g. cell edges) – both out doors and indoors.
- These small cells can also be deployed within the user premises, residential or official, thereby bringing the network closer to the customer.

(i) Microcells

- Microcells, typically cover smaller areas maybe up to a kilometre.
- They usually transmit within a range of milliwatts to a few watts.
- Microcells are deployed for providing temporary cellular coverage and capacity to places like sports stadiums, convention centres etc.
- Sometimes, microcells may use distributed antenna systems (DAS) to improve bandwidth and reliability.

(ii) Pico Cells

- Pico cells are deployed on the macro cell edges or hotspots to improve coverage or throughput.
- Pico sells are open to all User Equipments (UEs)
- Pico sells can be used for both indoor and outdoor purpose.
- This coverage area is around 200m. And us usually they served around 32 to 100 users.

(iii) Femto Cells

- Femto cells are typically user-installed to improve coverage area within a small vicinity, such as home office or a dead zone within a building.
- Femto cells can be obtained through the service provider or purchased from a reseller.
- Femto cells are open to specific UEs – called CSG (Closed Subscription group) .
- A UE close to femto can't connect to femto if it is not in CSG. In that case it connects to macro instead.
- Femto cell usually serves to 4 to 16 users.
- Its coverage area is 10 to 50 m.

2. Macro cells

Macro cells have large coverage and capacity and are controlled by High power base stations. These are the cells which have been traditionally used in all cellular systems.

Base stations in HetNets

- Heterogeneous networks consist of different types of base stations supporting different types of cells such as Macro, Micro, Pico and Femto cells.
  - Macro cells are controlled by High Power eNBs.

- Small Cells (Micro, Pico and Femto) are controlled by Low power eNBs. Low Power nodes include micro, pico, Remote Radio Heads (RRH), relay nodes and femto nodes.

- These can use the same or different technologies.
- In LTE networks, the actual cell size depends not only on the eNodeB power but also on antenna position, as well as the location environment; e.g. rural or city, indoor or outdoor etc.

Different nodes, for small cells, used in LTE/LTE-A HetNets are listed below :

1. Home eNodeB (HeNB)

- These nodes are used to form Femto cells.
- It is a low power eNodeB which is mainly used to provide indoor coverage, for Closed Subscriber Groups (CSG). For example, in office premises.
- HeNBs are privately owned and deployed without coordination with the macro-network.

2. Relay Node (RN)

- Relay 4 interface Uu.

3. RRHs (Remote Radio Head)

- RRH is connected to an eNB via fibre can also be used to provide small cell coverage.
- It is an alternative solution to a BTS housed in a shelter at the bottom of the tower.
- It is a distributed base station, in which the majority of the base station equipment is no longer located in the shelter, but in an enclosure at the top of the tower near the antenna.
- This separate but integrated radio frequency (RF) unit is called a remote radio unit or remote radio head.
- It is compact in size. RRH is generally used to extend the coverage of a base station sub-system in the remote rural areas.
- Fig. 6.9.1 shows the typical HetNet architecture.

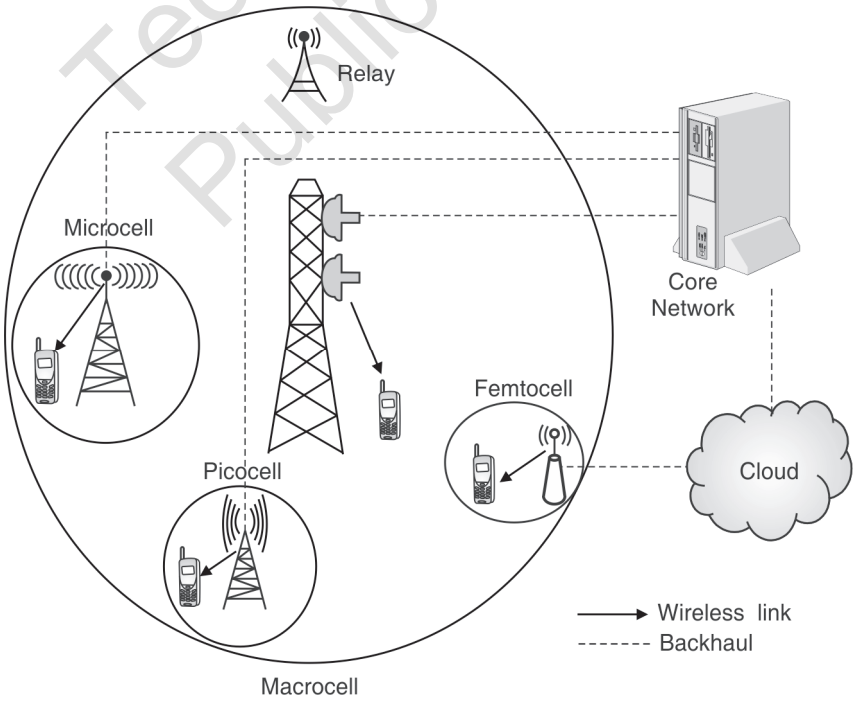


Fig. 6.9.1 : Heterogeneous Network Architecture

- A key component of such heterogeneous networks, which helps in meeting the above requirements is network intelligence via the SON (Self Organizing Network).
- SON is automation technology that enables the network to set itself up and self-manage resources and configuration to achieve optimal performance in an integrated network approach.
- The self-organizing and self-optimizing capability of the small cell smoothen the path for implementation of such heterogeneous networks.
- A self-organizing **micro base station** can automatically detect the surrounding radio environment conditions and automatically plan and configure radio parameters such as frequency, scrambling code, and transmission power.
- A traditional base station cannot do this.

6.10 Introduction to 5G

6.10.1 Overview

- 5G is not just one technology, it is actually a combination of several technologies in one. The system, however, will be a smart and know when to make use of which technology for maximum efficiency.
- 5G will be much more faster than 4G. It will provide data rate up to 10Gbps.
- It will provide 100% coverage area. That is better coverage even at the cell boundaries.
- 5G will also provide low network latency (up to 1 msec) which will be helpful for the critical applications like industry, healthcare and medical.
- 5G technology aims to provide wide range of future industries from retail to education, transportation to entertainment and smart homes to healthcare.
- 5G technology will provide ubiquitous connectivity means everything. from vehicles to mobile networks to industries to smart homes will be connected together.
- 5G will utilize Extremely High frequency spectrum band between 3GHz to 30 GHz. These are called millimetre waves. These wave can travel at very high speed but covers short distance since they cannot penetrate obstacles..
- Unlike 4G that requires high powered cellular base stations to transmit signal over long distance, 5G will use a large number of small cell stations that may be located on small towers or building roofs.
- 5G makes the use of Massive MIMO (Multiple Input Multiple Output) standards to make is 100 times faster as opposed to standard MIMO. Massive MIMO makes the use of as much as 100 antennas. Multiple antennas allow for better and faster data transmission.
- The 5G network will come with 100 times more devices in market.

5G standards

- 5G technology standard are still under development. So, no firm standards is in place at this time; the market is still figuring out the essential 5G features and functionalities.
- The primary 5G standards bodies involved in these processes are the 3rd Generation Partnership Project (3GPP), the Internet Engineering Task Force (IETF), and the International Telecommunication Union (ITU).

6.10.2 5GAA (Autonomous Association)

- The 5G Automotive Association (5GAA) is a global, cross-industry organization of companies that work together to develop end–to-end solution for future mobility and transportation services.
- These companies include the automotive, technology, and telecommunications industries (ICT).
- 5GAA was created on September 2016. It consists of 8 founding members: AUDI AG, BMW Group, Daimler AG, Ericsson, Huawei, Intel, Nokia, and Qualcomm Incorporated. More than 110 companies have now joined 5GAA.
- The 5G Automotive Association is a strong advocate of Cellular-Vehicle 2X (C-V2X). The following are the key objectives of 5GAA.

1. Making vehicles smarter

- Communication and connectivity are key to the development of autonomous vehicles.
- Cellular based technologiesV2X : vehicle-to-everything communication protocol allows vehicles to communicate with other vehicles (V2V), pedestrians (V2P), networks (V2N), and the surrounding infrastructure (V2I).

2. Making Vehicle Safer

- Cellular Vehicle-to-Everything (C-V2X) is a unified connectivity platform designed to offer vehicle-to-vehicle (V2V), vehicle-to-roadside infrastructure (V2I) and vehicle-to-pedestrian (V2P) communication.
- C-V2X will improve safety on roads by tremendously facilitating the flow of information between vehicles, pedestrians and road infrastructure. This will enable connected vehicles to anticipate and avoid dangerous situations, reducing collisions and potentially saving lives.

3. Improving driving experience

C-V2X will provide real-time traffic information to optimize user's trip, finding the closest free parking space or enabling predictive maintenance to save drivers both time and money.

6.10.3 The Key Technology : C-V2X (Cellular - Vehicle To everything)

Cellular-V2X (C-V2X) as initially defined as LTE V2X in 3GPP Release 14 is designed to operate in several modes.

It provides one solution for integrated V2V, V2I and V2P operation with V2N by using existing cellular network infrastructure :

1. Device-to-Device Communication

- Device-to-device communication is Vehicle-to-Vehicle (V2V), Vehicle-to-(Roadway) Infrastructure (V2I) and Vehicle-to-Pedestrian (V2P) direct communication.
- In the device-to-device mode (V2V, V2I, V2P) operation, C-V2X does not necessarily require any network infrastructure. It can operate without a SIM, without network assistance and uses GNSS as its primary source of time synchronization.

2. Device-to-Cell Tower Communication

Device-to-cell tower is another communication link which enables network resources and scheduling and utilizes existing operator infrastructure.

3. Device-to-Network Communication

- Device-to-network is the V2N solution using traditional cellular links to enable cloud services to be part and parcel of the end-to-end solution.

- Collectively, the transmission modes of shorter-range direct communications (V2V, V2I, V2P) and longer-range network-based communications (V2N) comprise what we call Cellular-V2X

6.10.4 Applications of 5G Network

5GAA focuses on more than simply providing faster data rate. 5G technology aims to provide wide range of future industries from retail to education, transportation to entertainment and smart homes to healthcare.

1. High Speed Mobile Networks

- 5G will revolutionize the mobile experience with data rate up to 10 to 20 GBPS download speed. It is equivalent to a fiber optic Internet connection accessed wirelessly.
- Another important feature of 5G technology is Low latency which is significant for autonomous driving and mission critical applications. 5G networks are capable of latency less than a millisecond.

2. Entertainment and Multimedia

- Almost 50 percentage of mobile Internet traffic is used for video downloads globally. This trend will increase in future and high definition video streaming will be common in future.
- 5G will offer a high definition virtual world on your mobile phone. Live events can be streamed via wireless network with high definition.
- HD TV channels can be accessed on mobile devices without any interruptions. Entertainment industry will hugely benefit from 5G wireless networks. Augmented reality and virtual reality requires HD video with low latency. 5G network is powerful enough to power AR and VR with amazing virtual experience.

3. Internet of Things - Connecting everything

- Internet of Things (IoT) is another broad area that will use 5G wireless network. Internet of Things will connect every objects, appliances, sensors, devices and applications into Internet.
- IoT applications will collects huge amount of data from millions of devices and sensors. 5G is the most efficient candidate for Internet of Things due to its flexibility, unused spectrum availability and low cost solutions for deployment.
- IoT can benefit from 5G networks in many areas like: Smart Homes, Smart Cities, Industrial IoT, Fleet Management etc.

4. Virtual reality and Augmented Reality

As Virtual reality (VR) and Augmented Reality (AR) needs faster data rate, low latency and reliability. 5G networks will unlock the potentials of VR and AR.

6.10.5 Millimeter Wave

- We all know that frequency spectrum is a scarce resource. The existing bands are crowded. One way to get around this problem is to simply transmit signals on a whole new swath of the spectrum, one that's never been used for mobile service before.
- So now, all 5G service providers are experimenting with broadcasting on millimeter waves, Millimeter waves are higher frequency waves than the radio waves. Millimeter wave is the band of spectrum between 30 gigahertz (Ghz) and 300 Ghz (Extremely High Frequency). It lies between the super high frequency (SHF) band, and the far infrared (IR) band. They are called millimeter waves because their wavelength vary from 1 to 10 mm, compared to the radio waves that serve today's smartphones. The radio waved wavelength is in tens of centimeters.
- Millimetre waves were first investigated in the 1890s by Indian scientist Jagadish Chandra Bose.

- Until now, only operators of satellites and radar systems used millimeter waves for real-world applications.
- There is one major drawback to millimeter waves, though – they can't easily travel through buildings or obstacles and they can be absorbed by foliage and rain. That's why 5G networks will likely augment traditional cellular towers with another new technology, called small cells.

Review Questions

Q. 1 With a neat sketch explain SAE architecture.

Q. 2 What is the need of VoLTE. Explain VoLTE in details.

Q. 3 What additional features does LTE advanced contain compared to LTE? Explain LTE-A architecture in detail.

Q. 4 Explain protocol stack of LTE.

Q. 5 What are the functions of LTE – MAC layer? Explain in detail.

Q. 6 Explain the Generic frame structure of LTE.

Q. 7 Explain different transport and logical channels used by LTE.

Q. 8 What do you mean by Self Organizing Networks? Explain SOIN architecture.

Q. 9 What are heterogeneous networks? Explain HetNet architecture in details.

Q. 10 What are the applications of 5G networks? What is millimeter wave?

Q. 11 Compare between LTE and LTE Advanced.

❑❑❑