SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF ELECTRICAL AND ELECTRONICS

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

UNIT – I – Wireless Communication –SEC1614

I. INTRODUCTION

1.1 BASIC CELLULAR SYSTEMS

There are two basic cellular systems; one is the circuit-switched system and the other is the packet- switched system.Circuit-Switched Systems In a circuit-switched system, each traffic channel is dedicated to a user until its cell is terminated. We can further distinguish two circuit-switched systems: one for an analog system and one for a digital system.

1.1.1 ANALOG SYSTEM

A basic analog cellular system1–3 consists of three subsystems: a mobile unit, a cell site, and a mobile telephone switching office (MTSO), as Fig. 1.1 shows, with connections to link the three subsystems.

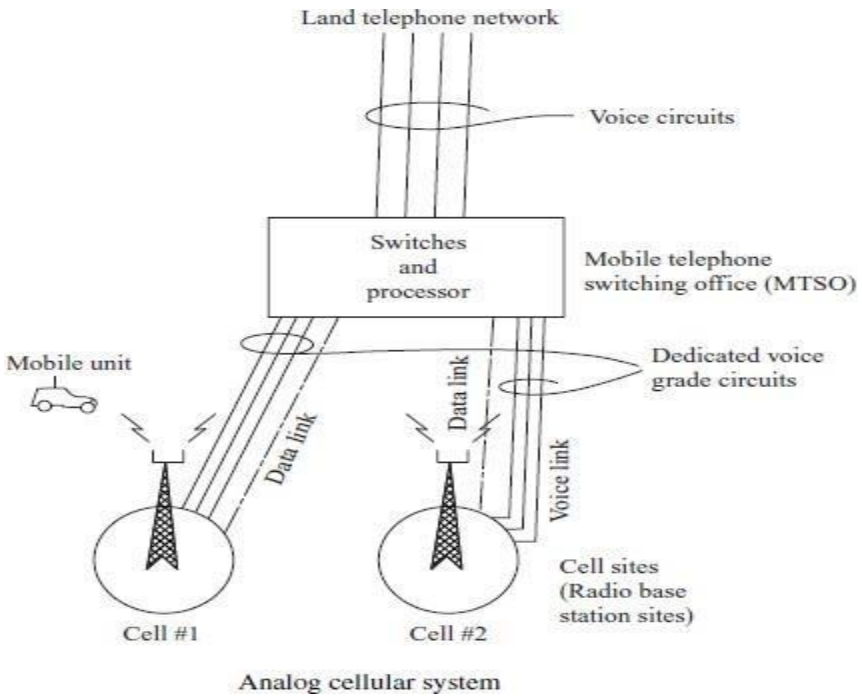


Figure 1.1 Analog Circuit switched system

Basic Components:

1. Mobile units. A mobile telephone unit contains a control unit, a transceiver, and an antenna system.

2. Cell site. The cell site provides interface between the MTSO and the mobile units. It has a control unit, radio cabinets, antennas, a power plant, and data terminals.

3. MTSO. The switching office, the central coordinating element for all cell sites, contains the cellular processor and cellular switch. It interfaces with telephone company zone offices, controls call processing, provides operation and maintenance, and handles billing activities.

4. Connections. The radio and high-speed data links connect the three subsystems. Each mobile unit can only use one channel at a time for its communication link. But the channel is not fixed; it can be any one in the entire band assigned by the serving area, with each site having multichannel capabilities that can connect simultaneously to many mobile units.

The MTSO is the heart of the analog cellular mobile system. Its processor provides central coordination and cellular administration. The cellular switch, which can be either analog or digital, switches calls to connect mobile subscribers to other mobile subscribers and to the nationwide telephone network. It uses voice trunks similar to telephone company interoffice voice trunks. It also contains data links providing supervision links between the processor and the switch and between the cell sites and the processor. The radio link carries the voice and signaling between the mobile unit and the cell site. The high-speed data links cannot be transmitted over the standard telephone trunks and therefore must use either microwave links or T-carriers (wire lines). Microwave radio links or T-carriers carry both voice and data between cell site and the MTSO.

1.1.2 DIGITAL SYSTEMS

A Basic Digital System consists of four elements: 1. Mobile Station 2. Base Transceiver Station (BTS) 3. Base Station Controller (BSC) 4. Switching Subsystems, as shown in Fig. 1.2.

1. **MS: It consists of two parts, mobile equipment (ME) and subscriber identify module (SIM). SIM contains all subscriber-specific data stored on the MS side.**
2. **BTS: Besides having the same function as the analog BTS, it has the Transcoder/Rate Adapter Unit (TRAU), which carries out coding and decoding as well as rate adaptation in case data rate varies.**
3. **BSC: A new element in digital systems that performs the Radio Resource (RR) management for the cells under its control. BSC also handles handovers, power management time and frequency synchronization, and frequency reallocation among BTSs.**
4. **Switching subsystems: Main components of Switching Subsystem is as follows:**

   a. **MSC: The main function of MSC is to coordinate the setup of calls between MS and PSTN users.**

   b. **VLR (Visitor Location Register): A database of all mobiles roaming in the MSC's area of control.**

   c. **HLR (Home Location Register):A centralized database of all subscribers registered in a Public Land Mobile Network (PLMN).**

   d. **AUC (Authentication Center): Provides HLR with authentication parameters and ciphering keys that are used for security purposes.**

   e. **EIR (Equipment Identity Register): A database for storing all registered mobile equipment numbers.**

   f. **EC (Echo Canceller): Used on the PSTN side of the MSC for all voice circuits.**

   g. **XC (Transcoder): Usually installs in each BTS. But for the cost reason, it can be installed in BSC or MSC.**

h. **OMC (Operational and Maintenance Center): This function resided in analog MSC but became a separated entity in digital systems**

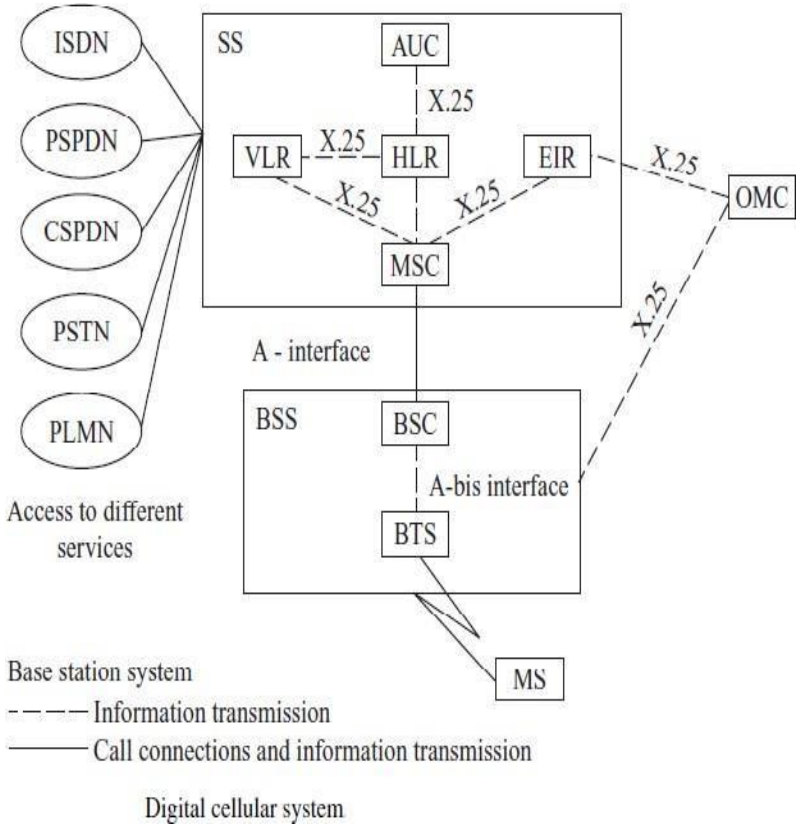


Figure 1.2 Digital Cellular System

1.1.3 PACKET SWITCHED SYSTEM

A cellular packet-switched system has six elements as follows:

1. **MS (Mobile Station)**
2. **Node B**
3. **RNC (Radio Network Controller)**
4. **SGSN (Service GPRS Support Node)**
5. **GGSN (Gateway GPRS Support Node)**
6. **CGF (Changing Gateway Function)**

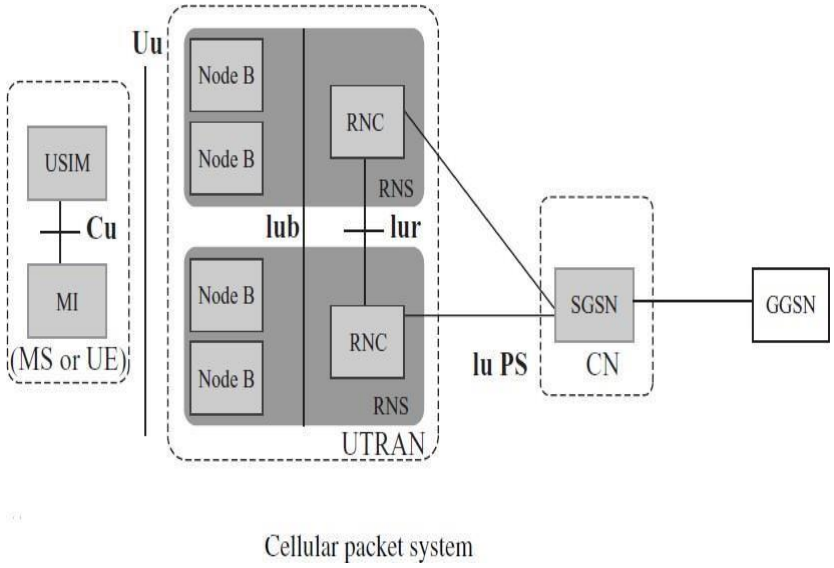


Figure 1.3 Packet Switched System

- **MS: Provides the voice and packet data services. It is also called UE (User Equipment).**
- **Node B: The name for base station in GSM.**
- **RNC (Radio Network Controller): Controls the radio resources of the Node Bs that are connected to it. Its function is similar to BSC. A device PCU (Packet Control Unit) converts the data stream into packet format.**
- **SGSN (Service GPRS Support Node): Analogous to MSC/VLR in the circuit-switched system. This includes mobility management, security, and access control functions. It interfaces to HLR.**
- **GGSN (Gateway GPRS Support Node): The point of interface with external packet data networks such as the Internet.**
- **CGF (Changing Gateway Function): Mainly for billing.**
- ***RNS (Radio Network Subsystem):* It consists of RNC and Node B. UTRAN consists of two or more RNS.**

1.2 PERFORMANCE CRITERIA

- **Main components of Performance criteria are as follows:**
- **Voice Quality**
- **Data Quality**
- **Picture/Vision Quality**
- **Service Quality**
- **Special Features**

1. **Voice Quality**

Voice quality is very hard to judge without subjective tests for users' opinions. In this technical area, engineers cannot decide how to build a system without knowing the voice quality that will satisfy the users. In military communications, the situation differs: armed forces personnel must use the assigned equipment.

- **CM: For any given commercial communications system, the voice quality will be based on the following criterion: a set value *x* at which *y* percent of customers rate the system voice quality (from transmitter to receiver) as good or excellent; the top two circuit merits (CM) of the five listed below.**

CM	Score	Quality Scale
CM5	5	Excellent (speech perfectly understandable)
CM4	4	Good (speech easily understandable, some noise)
CM3	3	Fair (speech understandable with a slight effort, occasional repetitions needed)
CM2	2	Poor (speech understandable only with considerable effort, frequent repetitions needed)
CM1	1	Unsatisfactory (speech not understandable)

- **MOS: As the percentage of customers choosing CM4 and CM5 increases, the cost of building the system rises.**

- **The average of the CM scores obtained from all the listeners is called mean opinion score (MOS). Usually, the toll-quality voice is around MOS ≥4.**

- **DRT (Diagnostic Rhyme Test): An ANSI standardized method used for evaluation of intelligibility. It is a subjective test method. Listeners are required to choose which word of a rhyming pair they perceived. The words differ only in their leading consonant. The word pairs have been chosen such that six binary attributes of speech intelligibility are measured in their present and absent states. This attribute profile provides a diagnostic capability to the test.**

2. **Data Quality:**

   There are several ways to measure the data quality such as bit error rate, chip error rate, symbol error rate, and frame error rate. The chip error rate and symbol error rate are measuring the quality of data along the transmission path. The frame error rate and the bit error rate are measuring the quality of data at the throughput.

3. **Picture/Vision Quality**

   There are color acuity, depth perception, flicker perception, motion perception, noise perception, and visual acuity. The percentage of pixel (picture element) loss rate can be characterized in vertical resolution loss and horizontal resolution loss of a pixel.

4. **Service Quality**

   Three items are required for service quality.

   Coverage: The system should serve an area as large as possible. With radio coverage, however, because of irregular terrain configurations, it is usually not practical to cover 100 percent of the area for two reasons:

   a. The transmitted power would have to be very high to illuminate weak spots with sufficient reception, a significant added cost factor.

   b. The higher the transmitted power, the harder it becomes to control interference. Therefore, systems usually try to cover 90 percent of an area in flat terrain and 75 percent of an area in hilly terrain. The combined voice quality and coverage criteria in AMPS

Required grade of service: For a normal start-up system, the grade of service is specified for a blocking probability of .02 for initiating calls at the busy hour. This is an average value. However, the blocking probability at each cell site will be different. At the busy hour, near freeways, automobile traffic is usually heavy, so the blocking probability at certain cell sites may be higher than 2 percent, especially when car accidents occur. To decrease the blocking probability requires a good system plan and a sufficient number of radio channel.

Number of dropped calls*:* During Q calls in an hour, if a call is dropped and Q−1 calls are completed, then the call drop rate is 1/Q. This drop rate must be kept low. A high drop rate could be caused by either coverage problems or handoff problems related to inadequate channel availability or weak reception.

5. **Special Features**

A system would like to provide as many special features as

- **Call Forwarding**
- **call waiting**
- **voice stored (VSR) box**
- **automatic roaming**
- **short message service (SMS)**
- **multimedia service (MMS)**
- **push-to-talk (PTT)**
- **Navigation services.**

1.3 UNIQUENESS OF MOBILE RADIO ENVIRONMENT

The Propagation Attenuation

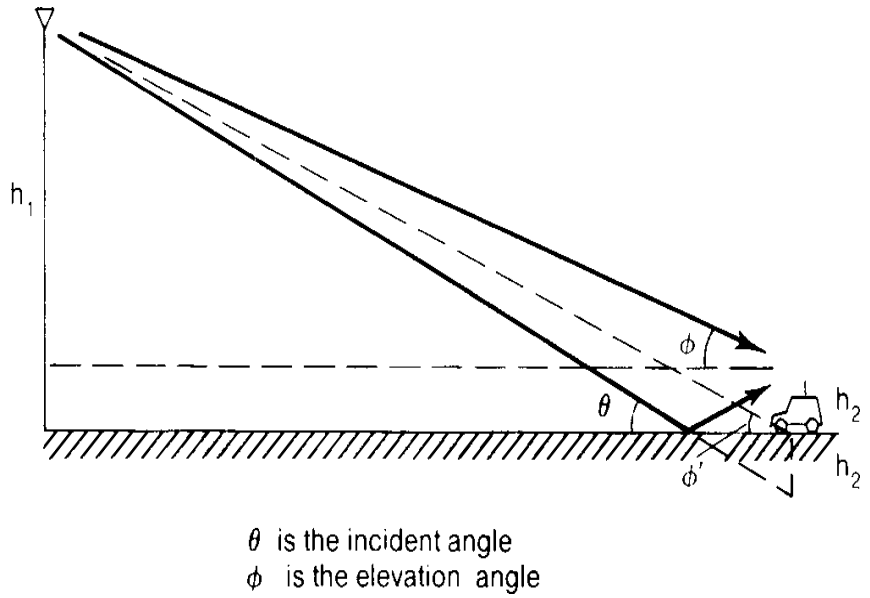


Figure 1.4 Mobile Radio Transmission Model

In general, the propagation path loss increases not only with frequency but also with distance. If the antenna height at the cell site is 30 to 100 m and at the mobile unit about 3 m above the ground, and the distance between the cell site and the mobile unit is usually 2 km or more, then the incident angles of both the direct wave and the reflected wave are very small, as Fig. 2.4 shows. The incident angle of the direct wave is 91, and the incident angle of the reflected wave is 02. 01 is also called the elevation angle. The propagation path loss would be 40 dB/dec,4 where "dec" is an abbreviation of decade, i.e., a period of 10. This means that a 40-dB loss at a signal receiver will be observed by the mobile unit as it moves from 1 to 10 km. Therefore C is inversely proportional to R^4

$$C \alpha R^{-4} = \alpha R^{-4}$$

where C = received carrier power R = distance measured from the transmitter to the receiver α = constant

1.3.1 Model of Transmission Medium

A mobile radio signal r(t), illustrated in Fig. 2.6, can be artificially characterized5 by two components m(t) and r0(t) based on natural physical phenomena. r (t) = m(t)ro(t) The component m(t) is called local mean, long-term fading, or lognormal fading and its variation is due to the terrain contour between the base station and the mobile unit. The factor r0 is called multipath fading, short-term fading, or Rayleigh fading and its variation is due to the waves reflected from the surrounding buildings and other structures.

1.3.2 Mobile Fading Characteristics

Rayleigh fading is also called multipath fading in the mobile radio environment. When these multipath waves bounce back and forth due to the buildings and houses, they form many standing-wave pairs in space. Those standing-wave pairs are summed together and become an irregular wave-fading structure. When a mobile unit is standing still, its receiver only receives a signal strength at that spot, so a constant signal is observed. When the mobile unit is moving, the fading structure of the wave in the space

is received. It is a multipath fading. The recorded fading becomes fast as the vehicle moves faster

1.4 OPERATIONS OF CELLULAR SYSTEM

- **Mobile unit initialization**
  - **Scan and select strongest set up control channel**
  - **Automatically selected BS antenna of cell**
    - **Usually but not always nearest (propagation anomalies)**
  - **Handshake to identify user and register location**
  - **Scan repeated to allow for movement**
    - **Change of cell**
  - **Mobile unit monitors for pages (see below)**
- **Mobile originated call**
  - **Check set up channel is free**
    - **Monitor forward channel (from BS) and wait for idle**
  - **Send number on pre-selected channel**

- **Paging**
  - **MTSO attempts to connect to mobile unit**
  - **Paging message sent to BSs depending on called mobile number**
  - **Paging signal transmitted on set up channel**
- **Call blocking**
  - **During mobile-initiated call stage, if all traffic channels busy, mobile tries again**
  - **After number of fails, busy tone returned**
- **Call termination**
  - **User hangs up**
  - **MTSO informed**
  - **Traffic channels at two BSs released**
- **Call drop**
  - **BS cannot maintain required signal strength**
  - **Traffic channel dropped and MTSO informed**
  - **Calls to/from fixed MTSO connects to PSTN**
  - **MTSO can connect mobile user and fixed subscriber via PSTN**
  - **MTSO can connect to remote MTSO via PSTN or via dedicated lines**
  - **Can connect mobile user in its area and remote mobile user**

1.5 CONCEPT OF FREQUENCY RESUSE SCHEMES

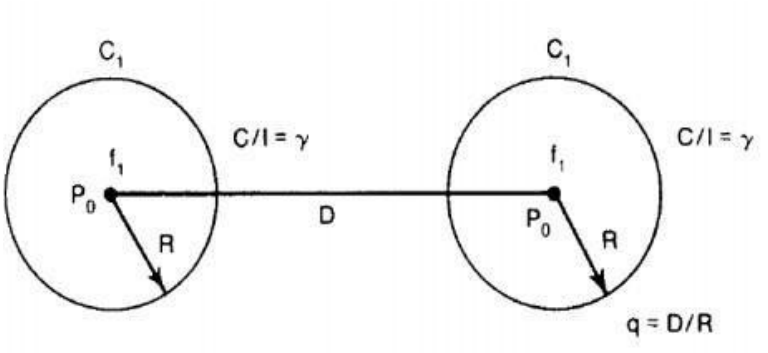


Figure 1.5 The ratio D/R

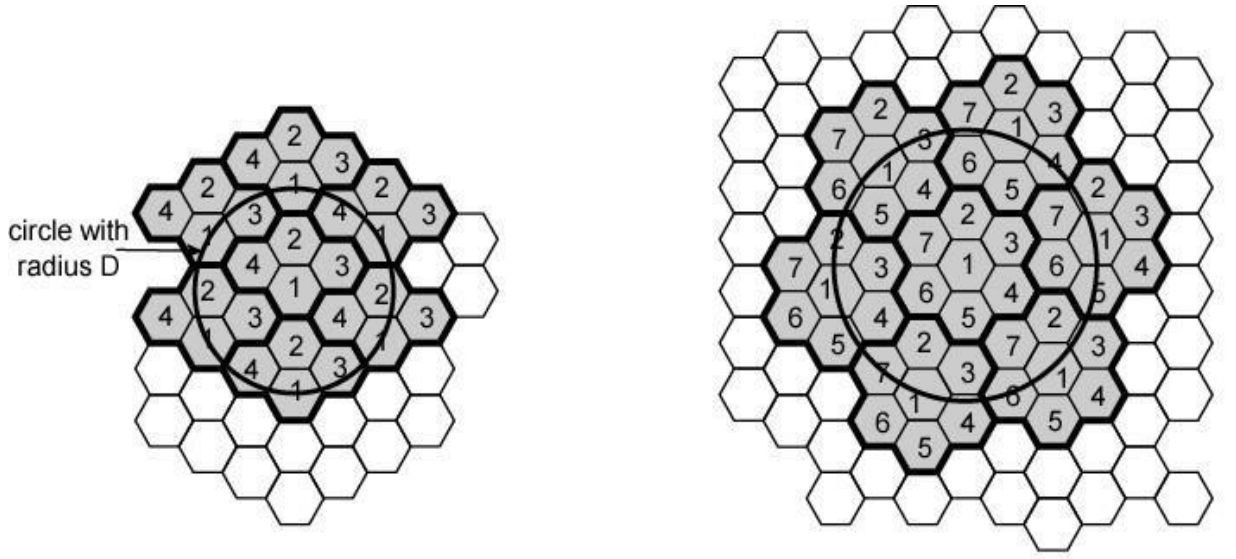
- ***N*** **cells all using same number of frequencies**
- ***K*** **total number of frequencies used in systems**
- **Each cell has *K/N* frequencies**

- — **Advanced Mobile Phone Service (AMPS) *K*=395, *N*=7 giving 57 frequencies per cell on average**

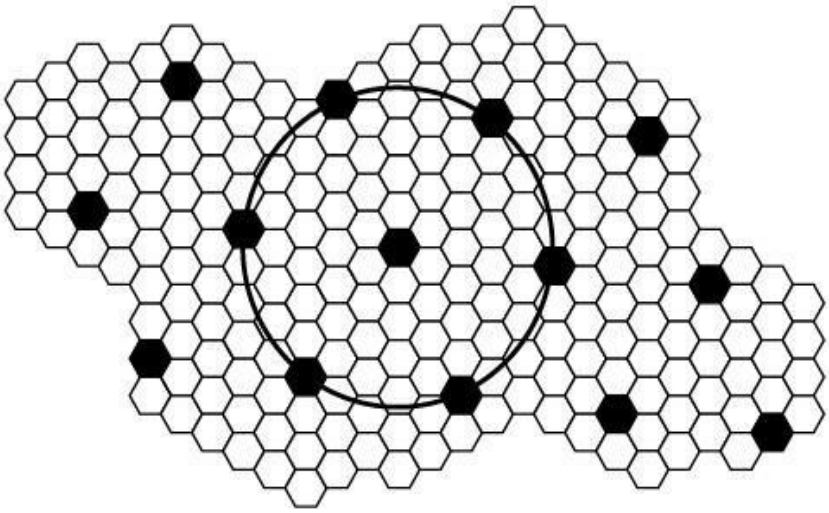
- **D = minimum distance between centers of cells that use the same band of frequencies (called co-channels)**
- **R = radius of a cell**
- **d = distance between centers of adjacent cells (d = R)**
- **N = number of cells in repetitious pattern**
  - — **Reuse factor**
  - — **Each cell in pattern uses unique band of frequencies**
- **Hexagonal cell pattern, following values of N possible**
  - **— $N = I^2 + J^2 + (I \times J)$, I, J = 0, 1, 2, 3, …**
- **Possible values of N are 1, 3, 4, 7, 9, 12, 13, 16, 19, 21, …**

A radio channel consists of a pair of frequencies, one for each direction of transmission that is used for full-duplex operation. A particular radio channel, say F1, used in one geographic zone as named it a cell, say C1, with a coverage radius R can be used in another cell with the same coverage radius at a distance D away. Frequency reuse is the core concept of the cellular mobile radio system. In this frequency reuse system, users in different geographic locations (different cells) may simultaneously use the same frequency channel. The frequency reuse system can drastically increase the spectrum efficiency, but if the system is not properly designed, serious interference may occur. Interference due to the common use of the same channel is called cochannel interference and is our major concern in the concept of frequency reuse.

Same frequency assigned in two different geographic areas, such as AM or FM radio stations using the same frequency in different cities. 2. Same frequency repeatedly used in a same general area in one system2—the scheme is used in cellular systems. There are many co channel cells in the system. The total frequency spectrum allocation is divided into K frequency reuse patterns as shown in figure 1.5, for K = 4, 7, 12, and 19.



(a) Frequency reuse pattern for N = 4 (b) Frequency reuse pattern for N = 7



(c) Black cells indicate a frequency reuse for N = 19

Figure 1.6 N-cell reuse pattern

1.6 CO-CHANNEL INTERFERENCE REDUCTION FACTOR

Reusing an identical frequency channel in different cells is limited by cochannel interference between cells, and the co-channel interference can become a major problem. Here we would like to find the minimum frequency reuse distance in order to reduce this cochannel interference. Assume that the size of all cells is roughly the same. The cell size is determined by the coverage area of the signal strength in each cell. As long as the cell size is fixed, cochannel interference is independent of the transmitted power of each cell. It means that the received threshold level at the mobile unit is adjusted to the size of the cell. Actually, cochannel interference is a function of a parameter q defined as

$$q = D / R$$

The parameter q is the co-channel interference reduction factor. When the ratio q increases, co- channel interference decreases. Furthermore, the separation D is a function of KI and C/I,

$$D = f(KI, C/I)$$

where KI is the number of co-channel interfering cells in the first tier and C/I is the received carrier-to-interference ratio at the desired mobile receiver

In a fully equipped hexagonal-shaped cellular system, there are always six cochannel interfering cells in the first tier, as shown in Fig. 1.6; that is, KI = 6. The maximum number of KI in the first tier can be shown as six (i.e., 2π D/D ≈ 6). Cochannel interference can be experienced both at the cell site and at mobile units in the center cell. If the interference is much greater, then the carrier-to-interference ratio C/I at the mobile units caused by the six interfering sites is (on the average) the same as the C/I received at the center cell site caused by interfering mobile units in the six cells. According to both the reciprocity theorem and the statistical summation of radio propagation, the two C/I values can be very close. Assume that the local noise is much less than the interference level and can be neglected. C/I then can be expressed, as

$$\frac{C}{I} = \frac{R^{-\gamma}}{6 \cdot D^{-\gamma}} = \frac{1}{6 \cdot q^{-\gamma}} = \frac{q^{\gamma}}{6}$$

where γ is a propagation path-loss slope5 determined by the actual terrain environment. In a mobile radio medium, γ usually is assumed to be 4. K_I is the number of cochannel interfering cells and is equal to 6 in a fully developed system, as shown in Fig. 1.6. The six cochannel interfering cells in the second tier cause weaker interference than those in the first tier.

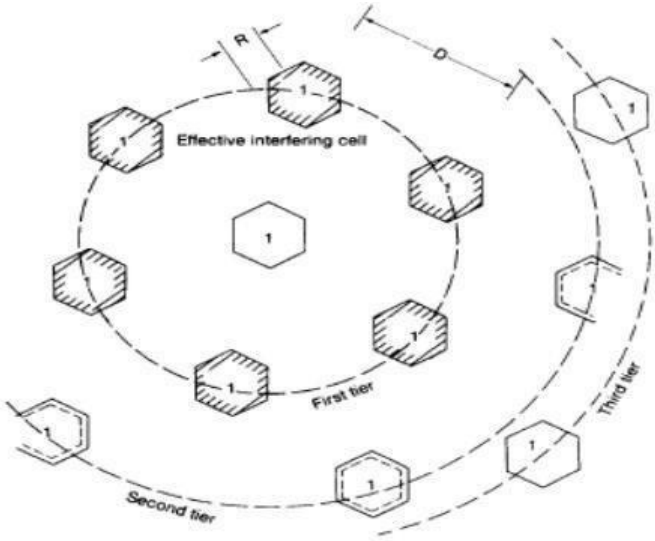


Figure 1.7 Six effective interfering cell of cell 1

1.6.1 DESIRED C/I FROM A NORMAL CASE IN A OMNI DIRECTIONAL ANTENNA SYSTEM

There are two cases to be considered: (1) the signal and cochannel interference received by the mobile unit and (2) the signal and cochannel interference received by the cell site.

Both cases are shown in Fig. 1.7. Nm, and Nb are the local noises at the mobile unit and the cell site, respectively. Usually, Nm and Nb are small and can be neglected as compared with the interference level. As long as the received carrier-to-interference ratios at both the mobile unit and the cell site are the same, the system is called a balanced system. In a balanced system, we can choose either one of the two cases to analyze the system requirement; the results from one case are the same for the others.

Assume that all Dk are the same for simplicity, as shown in Fig. 1.7; then D = Dk , and q = qk , and

$$\frac{C}{I} = \frac{R^{-\gamma}}{6D^{-\gamma}} = \frac{q^{\gamma}}{6}$$

Thus $q^{\gamma} = 6\frac{C}{I}$ **and** $q = \left(6\frac{C}{I}\right)^{1/\gamma}$

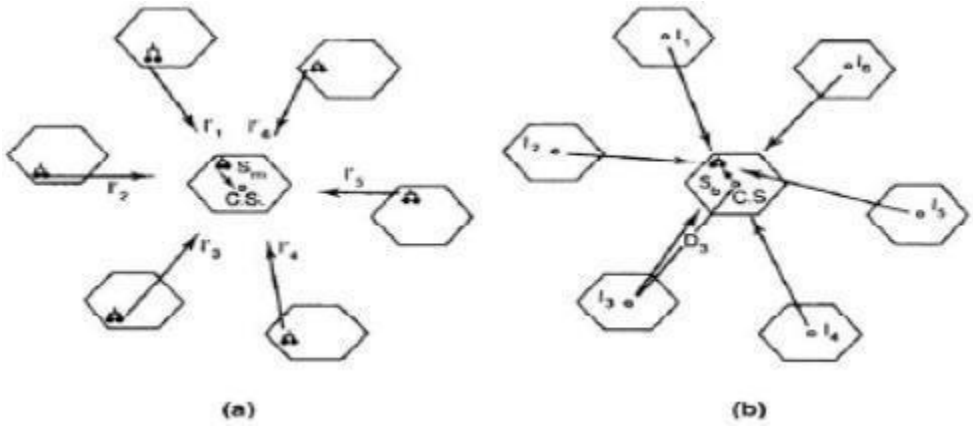


Figure 1.8 Co channel interference from six interferers, (a) Receiving at the cell site; (b) receiving at the mobile unit.

The value of C/I is based on the required system performance and the specified value of γ is based on the terrain environment. With given values of C/I and γ , the cochannel interference reduction factor q can be determined. Normal cellular practice is to specify C/I to be 18 dB or higher based on subjective tests. Because a C/I of 18 dB is measured by the acceptance of voice quality from present cellular mobile receivers, this acceptance implies that both mobile radio multipath fading and cochannel interference become ineffective at that level. The path-loss slope γ is equal to about 4 in a mobile radio environment.

$$q = D/R = (6 \times 63.1)^{1/4} = 4.41$$

The 90th percentile of the total covered area would be achieved by increasing the transmitted power at each cell; increasing the same amount of transmitted power in each cell does not affect the result. This is because q is not a function of transmitted

power. The factor q can be related to the finite set of cells K in a hexagonal-shaped cellular system by

$$q = \frac{\Delta}{=}\sqrt{3K}$$

Substituting q yields K = 7

This indicates that a seven-cell reuse pattern is needed for a C/I of 18 dB. The seven-cell reuse pattern is shown in Fig. 1.7. Based on q = D/R, the determination of D can be reached by choosing a radius R. The greater the value of q, the lower the cochannel interference. The value q may not be large enough to maintain a carrier-to-interference ratio of 18 dB. This is particularly true in the worst case.

1.7 CELL SPLITTING

The motivation behind implementing a cellular mobile system is to improve the utilization of spectrum efficiency.19 The frequency reuse scheme is one concept, and cell splitting is another concept. When traffic density starts to build up and the frequency channels Fi in each cell Ci cannot provide enough mobile calls, the original cell can be split into smaller cells. Usually the new radius is one-half the original radius. There are two ways of splitting.

New cell radius = old cell radius/2 New cell area = old cell area/4

Let each new cell carry the same maximum traffic load of the old cell; then, in New theory,

traffic load/Unit area= 4 × traffic load/unit area

There are two kinds of cell-splitting techniques:

Permanent splitting. The installation of every new split cell has to be planned ahead of time; the number of channels, the transmitted power, the assigned frequencies, the choosing of the cell-site selection, and the traffic load consideration should all be considered. When ready, the actual service cut-over should be set at the lowest traffic point, usually at midnight on a weekend. Hopefully, only a few calls will be dropped because of this cut-over, assuming that the downtime of the system is within 2 h.

Dynamic splitting. This scheme is based on using the allocated spectrum efficiency in real time. The algorithm for dynamically splitting cell sites is a tedious job, as we cannot afford to have one single cell unused during cell splitting at heavy traffic hours.

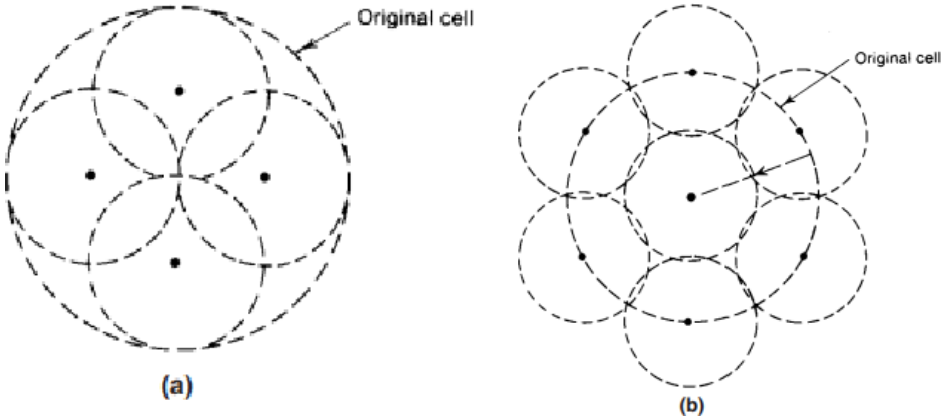
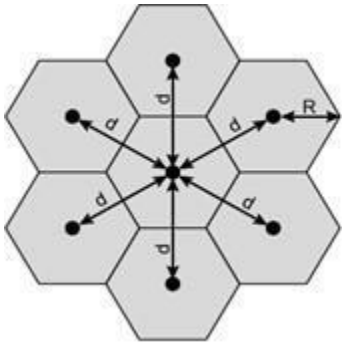


Figure 1.9 Cell Splitting

1.8 Shape of Cells



- **Hexagon**
  - **Provides equidistant antennas**
  - **Radius defined as radius of circum-circle**
- **Distance from center to vertex equals length of side**
  - **Distance between centers of cells radius *R* is**
  - **Not always precise hexagons**
- **Topographical limitations**
- **Local signal propagation conditions**
- **Location of antennas**

1.9 CONSIDERATION OF THE COMPONENTS OF CELLULAR SYSTEM

The elements of cellular mobile radio system design have been mentioned in the previous sections. Here we must also consider the components of cellular systems, such as mobile radios, antennas, cell-site, base-station controller, and MTSO. They would affect our system design if we do not choose the right one. The general view of the cellular system is shown in Fig. 1.5. Even though the EIA (Electronic Industries Association) and the FCC have specified standards for radio equipment at the cell sites and the mobile sites, we still need to be concerned about that equipment. The issues affecting choice of antennas, switching equipment, and data links are briefly described here

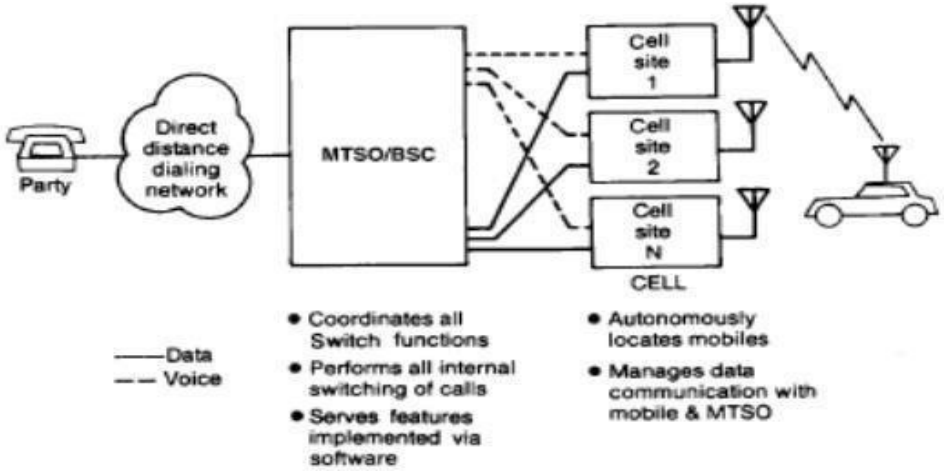


Figure 1.10 Components of Cellular System

Antennas: Antenna pattern, antenna gain, antenna tilting, and antenna height6 all affect the cellular system design. The antenna pattern can be omnidirectional, directional, or any shape in both the vertical and the horizon planes. Antenna gain compensates for the transmitted power. Different antenna patterns and antenna gains at the cell site and at the mobile units would affect the system performance and so must be considered in the system design. The antenna patterns seen in cellular systems are different from the patterns seen in free space. If a mobile unit travels around a cell site in areas with many buildings, the omnidirectional antenna will not duplicate the omnipattern.

In addtion, if the front-to-back ratio of a directional antenna is found to be 20 dB in free space, it will be only 10 dB at the cell site. An explanation for these phenomena is given in Chapter 8.

Antenna tilting can reduce the interference to the neighboring cells and enhance the weak spots in the cell. Also, the height of the cell-site antenna can affect the area and shape of the coverage in the system.

Switching Equipment: The capacity of switching equipment in cellular systems is not based on the number of switch ports but on the capacity of the processor associated with the switches. In a big cellular system, this processor should be large. Also, because cellular systems are unlike other systems, it is important to consider when the switching equipment would reach the maximum capacity. The service life of the switching equipment is not determined by the life cycle of the equipment but by how long it takes to reach its full capacity. If the switching equipment is designed in modules, or as distributed switches, more modules can be added to increase the capacity of the equipment. For decentralized systems, digital switches may be more suitable. The future trend seems to be the utilization of system handoff. This means that switching equipment can link to other switching equipment so that a call can be carried from one system to another system without the call being dropped.

Data Links: The data links are shown in Fig.1.5. Although they are not directly affected by the cellular system, they are important in the system. Each data link can carry multiple channel data (10 kbps data transmitted per channel) from the cell site to the MTSO. This fast-speed data transmission cannot be passed through a regular telephone line. Therefore, data bank devices are needed. They can be multiplexed, many-data channels passing through a wideband T-carrier wire line or going through a microwave radio link where the frequency is much higher than 850 MHz. Leasing T1-carrier wire lines through telephone companies can be costly. Although the use of microwaves may be a long- term money saver, the availability of the microwave link has to be considered and is described

1.10 Frequency Management and Channel Assignment

Achieving optimum system capacity with a limited frequency spectrum is one of the main research issues in cellular communications. In a cellular system, frequency management and channel assignment are essential in order to achieve the basic objectives of spectrum utilization as well as adaptability to traffic density.

Depending upon the system parameters, the allocated frequency spectrum is divided into a number of frequency channels. These available frequency channels are then divided into the subsets that can be assigned to each cell. Different strategies are followed for the assignment of these channel sets to cells. Fixed channel assignment (FCA) technique and dynamic channel allocation techniques are covered in detail. Frequency management includes operations such as designation of set-up and voice channels, numbering the channels, and grouping voice channels into subsets.

The main objective of channel-assignment is to stabilize the fluctuations in the probability of call blockage over the entire coverage area of a cellular network over a period of time. The channel assignment does the allocation of specific channels to cell sites and mobile units. It can be done in two ways:

- **Short-term assignment, where one channel assignment per call ishandled by mobile telephone switching office (MTSO).**
- **Long-term assignment, where a fixed channel set consisting of one or more subsets are assigned to cell site on a long-term basis.**

Each channel consists of two frequency channel bandwidths (mobile transmit/uplink or reverse channel and cell-site transmit/downlink or forward channel) to allow duplex operation. These two channel bandwidths must be separated in frequency in order to avoid interference. The frequency separation between the uplink and downlink channels is termed as channel spacing (or) duplex spacing. In the present 800 MHz band cellular system, the separation between the mobile transmit and the cell- site transmit is specified as 45 MHz.

The total channels available are 832 in number. However, most mobile units and systems are still operating on 666 channels. The arrangement of 666 frequency channels in block A and block B systems, each containing 333 channels. Out of these 333 available channels in each system, 312 channels are used for voice communication and 21 channels are used for controlling the system. These 21 channels are called as control channels or set-up channels. Therefore, a total of 42 channels are used for controlling the system.

1.10.1 Fixed channel assignment

In FCA, each cell assigns its own frequency channel to the mobile subscribers within its cell. Channel assignment is primarily based on causing least co-channel and adjacent channel interference in the cellular system. The channel assignment for each voice call is determined by MTSO on a short- term basis. In a FCA, the set-up and voice channels are usually assigned to the cell site for relatively long periods. Channels in a channel set are usually 21 channels apart and must meet minimum frequency spacing requirements of a multi-channel transmitter combiner. Channels are usually

numbered in order of increasing frequency. Regardless of the number of channels in a channel set, the highest channel set is frequency adjacent to the lowest channel set.

The following are the advantages of FCA:

- **Fixed parameters (power, frequency) for transceivers.**
- **Good performance under uniform- and/or high-traffic loads as cells independently decide their channel allocation decisions.**
- **If each cell is allocated to a pre-determined set of voice channels then the call is *blocked* and all the channels are occupied.**

Borrowing strategy: A cell is allowed to borrow channels from neighbouring cell if all of its own channels are occupied. Mobile switching centre (MSC) supervises the borrowing procedure to ensure no disrupting calls or interference with any of the calls in progress in the donor cell.

1.10.2 Dynamic channel assignment

In dynamic channel assignment (DCA), the central common pool maintains all the available channels. Channels are assigned dynamically as new requests for radio resource (for a fresh originating call or handoff of existing call) arrive in the system. This also implies that when the use of assigned channel is completed, the channel currently in use is returned to the central pool.

In order to achieve optimum system capacity with limited frequency spectrum, many DCA schemes have been proposed to allocate the channels more efficiently. In a cellular system, a mobile subscriber moves from one cell to another and continuation of communication link is ensured with suitable handoff mechanism. This demands for additional and flexible radio resources utilization. However, because a limited frequency band is allocated for cellular communication, there is an upper limit to the maximum number of channels, thereby restricting the number of available channels that can be assigned to each cell. Another way is non-uniform FCA based on the amount of traffic expected to be served in different cells as per the statistical traffic data.

The following are the advantages of DCA:

- **No fixed channels are assigned to each cell.**
- **Out of the available channels, any channel can be assigned to any cellon need basis.**
- **The serving base station (BS) requests a channel from the MSC whenever a**
- **call request is made.**

1.11 Handoff in Cellular Systems

Handoff refers to a process of transferring an ongoing call or data session from one channel connected to the core network to another. The channel change due to handoff may be through a time slot, frequency band, code word, or combination of these for time- division multiple access (TDMA), frequency-division multiple access (FDMA), code- division multiple access (CDMA), or a hybrid scheme. Handoff is also called as 'Handover'.

Reasons for a Handoff to be conducted:

- **To avoid call termination when the phone is moving away from the area covered by one cell and entering the area covered by another cell.**
- **When the capacity for connecting new calls of a given cell is used up.**
- **When there is interference in the channels due to the different phones using the same channel in different cells.**
- **When the user behaviors change**

1.11.1 Types of Handoffs:-

Handoffs are classified into two categories – *hard and soft handoffs*, which are further divided among themselves.

Hard handoff:

A hard handoff is essentially a "*break before make*" connection. Here the link to the prior base station is terminated before or as the user is transferred to the new cell's base station. This means that the mobile is linked to no more than one base station at a given time. A hard handoff occurs when users experience an interruption during the handover process caused by frequency shifting. A hard handoff is perceived by network engineers as event during the call. These are intended to be instantaneous in order to minimize the disruption of the call. Hard handoff can be further divided as intra and inter-cell handoffs.

Intra and inter-cell handoffs: In intra-cell handoff the source and target are one and the same cell and only the used channel is changed during the handoff. The purpose of intra-cell handoff is to change a channel, which may be interfered, or fading with a new clearer or less fading channel. In inter-cell handoff the source and the target are different cells (even if they are on the same cell site). The purpose of the inter-cell handoff is to maintain the call as the subscriber is moving out of the area of the source cell and entering the area of the target cell

Soft handoff:

Soft handoff is also called as Mobile Directed Handoff as they are directed by the mobile telephones. Soft handoff is the ability to select between the instantaneous received signals from different base stations. Here the channel in the source cell is retained and used for a while in parallel with the channel in the target cell. In this the connection to the target is established before the connection to the source is broken, hence this is called *"make-before-break".* Soft handoffs can be classified as Multiways and softer handoffs.

- **Multiways and softer handoffs: A soft handoff which involves using connections to more than two cells is a multiways handoff. When a call is in a state of soft handoff the signal of the best of all used channels can be utilized for the call at a given moment or all the signals can be combined to produce a clear signal, this type is called softer handoff.**

1.11.2 Types of handoff protocols:

There are four basic types of handoff protocols which help in providing continuous and QOS-guaranteed service. Namely:

- **Network-controlled handoff (NCHO)**
- **Mobile-assisted handoff (MAHO)**
- **Soft handoff (SHO) and**
- **Mobile-controlled handoff (MCHO)**

NCHO is a centralized handoff protocol, in which the network makes handoff decision based on measurements of the signal quality of mobile station (MS) at a number of based stations (BS). Sometimes the network sets up a bridge connection between the old and new BSs and thus minimizes the duration of handoff. This type of handoff is not suitable for a rapidly changing environment and a high density of users due to the associated delay.

An MAHO protocol distributes the handoff decision process. The MS makes measurements, and the MSC makes decisions.

SHO is a "make before break" connection. SHO is often used in conjunction with MAHO. Rather than immediately terminating the connection between a MS and a BS, the connection to the old BS is not broken until a connection to the new BS is made.

In MCHO, the MS is completely in control of the handoff process. This type of hand off has a short reaction time and is suitable for microcellular systems. A MS keeps on measuring signal strength from all the surround base stations. If the MS find that there is a new BS who has a stronger signal than that of an old BS, it may consider to handoff from the old BS to the new BS given a certain signal threshold is reached.

1.12 Dropped Call Rates

- **The dropped call is defined as an established call which leaves the system before it is normally terminated**
- **The Dropped Call Rate (DCR) parameter represents what percentage of all established calls is dropped during a specified time period**
- **The DCR and voice quality are inversely proportional and high DCR may indicate coverage,**

handoff, or channels accessibility problems

Formula of Dropped Call Rate:

The general formula of dropped call rate *P in a whole system can be expressed as:*

$$P = 1 - \left[\sum_{n=0}^{N} \alpha_n X^n \right] = \sum_{n=0}^{N} \alpha_n \cdot P_n$$

1.13 Multiple Access schemes

In wireless communication systems, the subscriber needs to send information simultaneously from the mobile station to the base station while receiving information from the base station to the mobile station.There are several different ways to allow access to the channel. These include the following −

- **Frequency division multiple-access (FDMA)**
- **Time division multiple-access (TDMA)**
- **Code division multiple-access (CDMA)**
- **Space division multiple access (SDMA)**

1.13.1 Frequency Division Multiple Access (FDMA)

FDMA is the basic technology for advanced mobile phone services. The features of FDMA are as follows.

- **FDMA allots a different sub-band of frequency to each different user to access the network.**
- **If FDMA is not in use, the channel is left idle instead of allotting to the other users.**
- **FDMA is implemented in Narrowband systems and it is less complex than TDMA.**
- **Tight filtering is done here to reduce adjacent channel interference.**
- **The base station BS and mobile station MS, transmit and receive simultaneously and continuously in FDMA.**

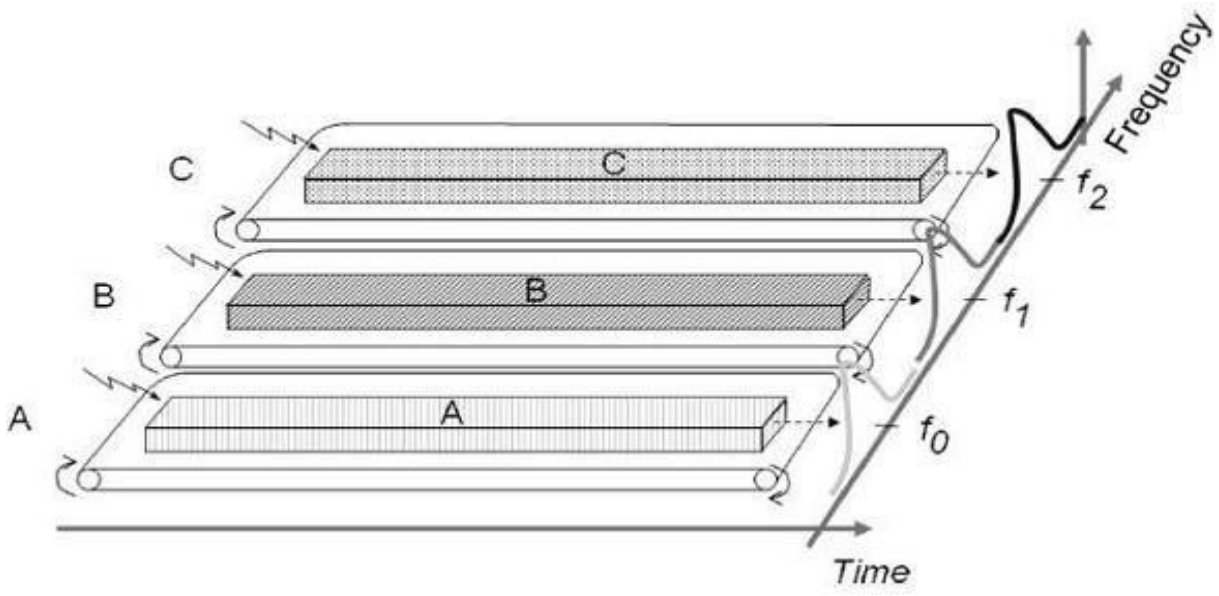


Figure 1.11 Frequency Division Multiple Access (FDMA)

1.13.2 Time Division Multiple Access (TDMA)

In the cases where continuous transmission is not required, there TDMA is used instead of FDMA. The features of TDMA include the following.

- **TDMA shares a single carrier frequency with several users where each users makes use of non- overlapping time slots.**
- **Data transmission in TDMA is not continuous, but occurs in bursts. Hence handsoff process is simpler.**
- **TDMA uses different time slots for transmission and reception thus duplexers are not required.**
- **TDMA has an advantage that is possible to allocate different numbers of time slots per frame to different users.**
- **Bandwidth can be supplied on demand to different users by concatenating or reassigning time slot based on priority.**

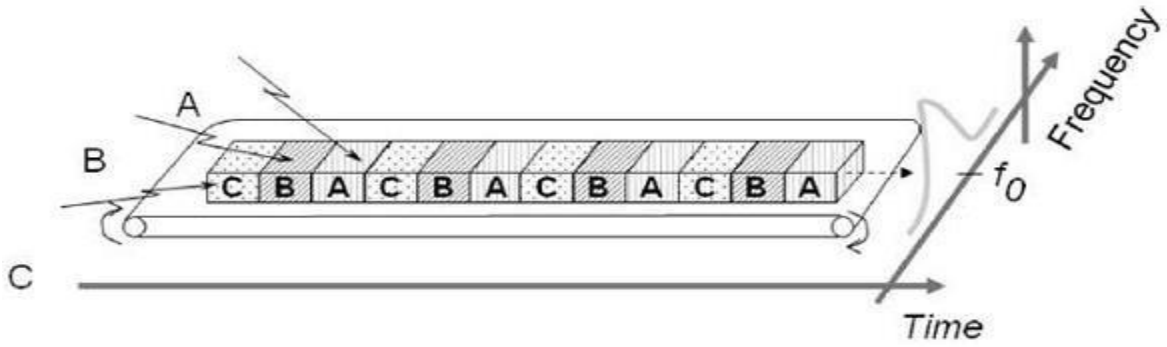


Figure 1.12 Time Division Multiple Access (TDMA)

1.13.3 Code Division Multiple Access (CDMA)

Code division multiple access technique is an example of multiple access where several transmitters use a single channel to send information simultaneously. Its features are as follows.

- **In CDMA every user uses the full available spectrum instead of getting allotted by separate frequency.**
- **CDMA is much recommended for voice and data communications.**
- **While multiple codes occupy the same channel in CDMA, the users having same code can communicate with each other.**
- **CDMA offers more air-space capacity than TDMA.**
- **The hands-off between base stations is very well handled CDMA.**

$$\text{Encodedsignal} = \text{Orginaldata} \times \text{chippingsequence}$$

- **1.13.4** Space Division Multiple Access (SDMA)

Space division multiple access or spatial division multiple access is a technique which is MIMO (multiple-input multiple-output) architecture and used mostly in wireless and satellite communication. It has the following features.

- **All users can communicate at the same time using the same channel.**
- **SDMA is completely free from interference.**
- **A single satellite can communicate with more satellites receivers of the same frequency.**
- **The directional spot-beam antennas are used and hence the base station in SDMA, can track a moving user.**
- **Controls the radiated energy for each user in space.**

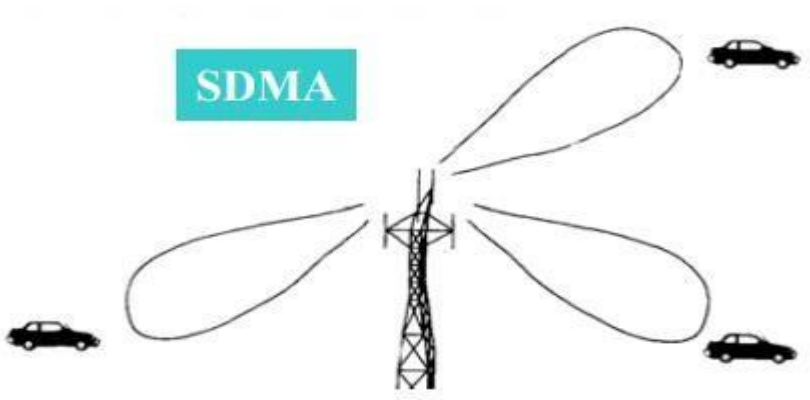


Figure 1.13 Space Division Multiple Access (SDMA)

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF ELECTRICAL AND ELECTRONICS

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

UNIT – II – Wireless Networks – SEC1614

II. Introduction

The wired version of LAN has gained wide popularity and large-scale deployment. The IEEE 802.3 standard has been revised and extended every few years. High-speed versions with transmission rate as high as 1000 Mbps are currently available. Until recently wireless version of LANs were not popular because of the following reasons:

- **High cost: Previously the equipment's cost more.**
- **Low data rate: Initially, the data rate supported by the WLAN is too less, so it supports only a few applications.**
- **Occupational safety concerns**
- **Licensing requirements**

Some of the advantages are mentioned below:

- **Availability of low-cost portable equipment's: Due to the technology enhancements, the equipment cost that are required for WLAN set-up have reduced a lot.**
- **Mobility: An increasing number of LAN users are becoming mobile. These mobile users require that they are connected to the network regardless of where they are because they want simultaneous access to the network. This makes the use of cables, or wired LANs, impractical if not impossible. Wireless LAN can provide users mobility, which is likely to increase productivity, user convenience and various service opportunities.**
- **Installation speed and simplicity: Wireless LANs are very easy to install. There is no requirement for wiring every workstation and every room. This ease of installation makes wireless LANs inherently flexible. If a workstation must be moved, it can be done easily and without additional wiring, cable drops or reconfiguration of the network.**
- **Installation flexibility: If a company moves to a new location, the wireless system is much easier to move than ripping up all of the cables that a wired system would have snaked throughout the building. This also provides portability. Wireless technology allows network to go anywhere wire cannot reach.**
- **Reduced cost of ownership: While the initial cost of wireless LAN can be higher than the cost**

of wired LAN hardware, it is envisaged that the overall installation expenses and life cycle costs can be significantly lower. Long-term cost-benefits are greater in dynamic environment requiring frequent moves and changes. Scalability: Wireless LAN can be configured in a variety of topologies to meet the users need and can be easily scaled to cover a large area with thousands of users roaming within it.

However, wireless LAN technology needs to overcome a number of inherent limitations and challenges. Some of the limitations and challenges are mentioned below:

- **Lower reliability due to susceptibility of radio transmission to noise and interference.**
- **Fluctuation of the strength of the received signal through multiple paths causing fading.**
- **Vulnerable to eavesdropping leading to security problem.**
- **Limited data rate because of the use of spread spectrum transmission techniques enforced to ISM band users.**

We shall introduce the wireless LAN technology based on IEEE 802.11 standard.

2.1 IEEE 802.11 Architecture

Each computer, mobile, portable or fixed, is referred to as a *station* in 802.11. The difference between a portable and mobile station is that a portable station moves from point to point but is only used at a fixed point. Mobile stations access the LAN during movement. Fundamental to the IEEE 802.11 architecture is the concept of Basic Service Set (BSS) or wireless LAN cell. A BSS is defined as a group of stations that coordinate their access to the medium under a given instance of medium access control. The geographic area covered by a BSS is known as the *Basic Service Area (BSA)*, which is very similar to a cell in a cellular communication network. All stations with in a BSA with tens of meters in diameter may communicate with each other directly. The 802.11 standard support the formation of two distinct types of BSSs: ad hoc network and Infrastructure BSS.

Two or more BSS's are interconnected using a *Distribution System or DS*. This concept of DS increases network coverage. Each BSS becomes a component of an extended, larger network. Entry to the DS is accomplished with the use of *Access Points (AP)*. An access point is a station, thus addressable. So data moves between the BSS and the DS with the help of these access points.

Creating large and complex networks using BSS's and DS's leads us to the next level of hierarchy, the *Extended Service Set or ESS*. The beauty of the ESS is the entire network looks like an independent basic service set to the Logical Link Control layer (LLC). This means that stations

within the ESS can communicate or even move between BSS's transparently to the LLC.

The first type of BSS is known as *ad hoc network*, which consists of a group of stations within the range of each other. As its name implies, ad hoc networks are temporary in nature, which are typically created and maintained as needed without prior administrative arrangement. Ad hoc networks can be formed anywhere spontaneously and can be disbanded after a limited period of time. A typical ad hoc network is shown in Figure below.

The second type of BSS is known as *infrastructure BSS (IBSS),* which is commonly used in practice. Here, several BSSs are interconnected by a distribution system to form an extended service set (ESS) as shown in Fig. (b). The BSSs are like cells in a cellular communications network. Each BSS is provided with an Access point (AP) that has station functionality and provides access to the distribution system. APs operate on a fixed channel and remain stationary like *base stations* in a cellular communication system. APs are located such that the BSSs they serve overlap slightly to provide continuous service to all the stations.

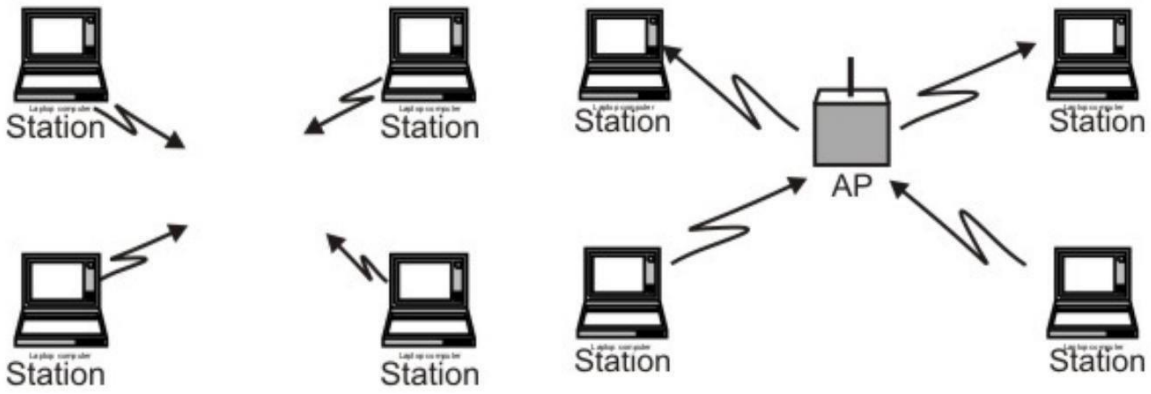


Figure 2.1 (a) Basic Service set (BSS), (b) Infrastructure BSS (ESS)

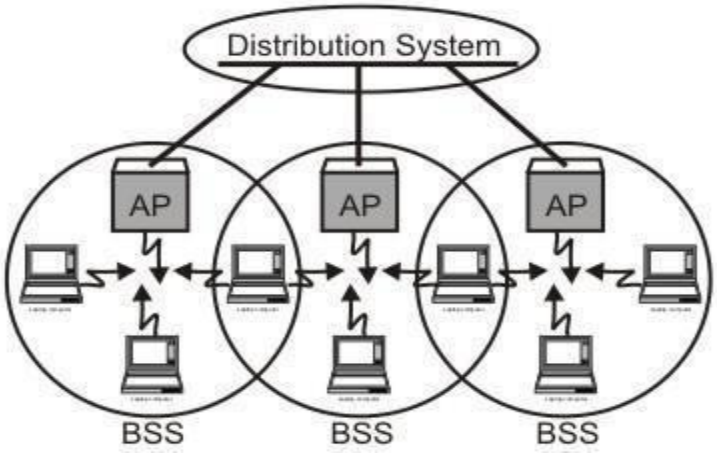


Figure 2.2 Extended service set (ESS)

An ESS can also provide gateway access for wireless users into a wired network. Each end station associates itself with one access point. Above Figure shows three BSSs interconnected through three APs to a distribution system. If station A associated with AP-1 wants to send a frame to another station associated with AP- 2, the first sends a frame to its access point (AP-1), which forwards the frame across the distribution system to the access point AP-2. AP-2 finally delivers it to the destination station.

The technique used for this purpose is known as *scanning*, which involves the following steps:

- **A station sends a *probe frame*.**
- **All APs within reach reply with a *probe response frame*.**
- **The station selects one of the access points, and sends the AP an *Association Request frame*.**
- **The AP replies with an *Association Response frame*.**

The above protocol is used when a station joins a network or when it wants to discontinue association with the existing AP because of weakened signal strength or some other reason. The discontinuation of association takes place whenever a station acquires a new AP and the new AP announces it in step 4 mentioned above. For example, assume that station B is moving away from the BSS of AP-1 towards the BSS of AP-2. As it moves closer to the BSS of AP-2, it sends probe frames, which is responded eventually by AP-2. As some of point of time station B prefers AP-2 over AP-1 and associates itself with the access point AP-2. The above mechanism is known as *active scanning*, as the node is actively searching for an access point. An access point also periodically sends Beacon frame that advertises the capabilities of the access point. In response, a station can associate to the AP simply by sending it an Association request frame. This is known as *passive scanning*.

2.1.1 Medium Access Control:

Most wired LANs products use Carrier Sense Multiple Access with Collision Detection (CSMA/CD) as the MAC protocol. Carrier Sense means that the station will listen before it transmits. If there is already someone transmitting, then the station waits and tries again later. If no one is transmitting then the station goes ahead and sends what it has. But when more than one station tries to transmit, the transmissions will collide and the information will be lost. This is where Collision Detection comes into play. The station will listen to ensure that its transmission made it to the destination without collisions. If a collision occurred then the stations wait and try again later. The time the station waits is determined by the back off algorithm. This technique works great for wired LANs but wireless topologies can create a problem for CSMA/CD. However, the wireless medium

presents some unique challenges not present in wired LANs that must be dealt with by

the MAC used for IEEE 802.11. Some of the challenges are:

- **The wireless LAN is prone to more interference and is less reliable.**
- **The wireless LAN is susceptible to unwanted interception leading to security problems.**
- **There are so called *hidden station* and *exposed station* problems.**

In the discussion of both the problem, we shall assume that all radio transmitters have fixed range. When the receiver is in the range of two active transmitters then the signal will be garbled. It is important to note that not all stations are in range of two transmitters.

2.1.2 The Hidden Station Problem

Consider a situation when A is transmitting to B, as depicted in the Fig. If C senses the media, it will not hear anything because it is out of range, and thus will falsely conclude that no transmission is going on and will start transmit to B. the transmission will interfere at B, wiping out the frame from A.

The problem of a station not been able to detect a potential competitor for the medium because the competitor is too far away is referred as *Hidden Station Problem.* As in the described scenario C act as a hidden station to A, this is also competing for the medium.

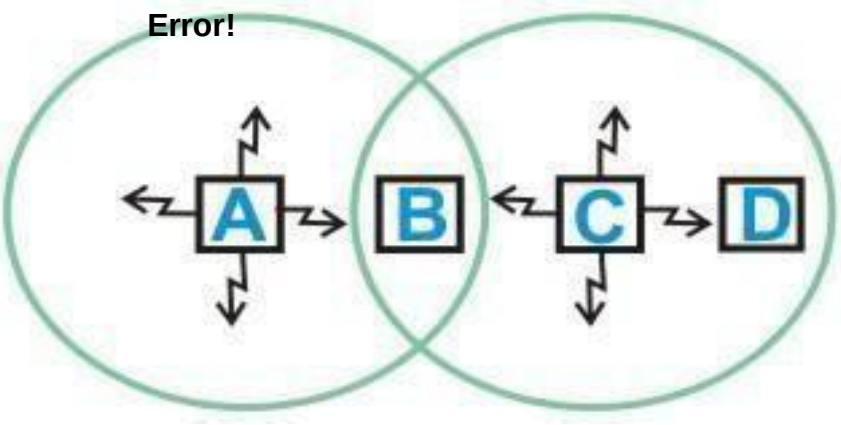


Figure 2.3 Hidden Station Problems

2.1.3 Exposed Station problem

Now consider a different situation where B is transmitting to A, and C sense the medium and detects the ongoing transmission between B and A. C falsely conclude that it can not transmit to D, when the fact is that such transmission would cause on problem. A transmission could cause a problem only when the destination is in zone between B and C. This problem is referred as *Exposed station Problem*. In this scenario as B is exposed to C, that's why C assumes it cannot transmit to D. So this problem is known as *Exposed station problem* (i.e. problem caused due to exposing of a station). The problem here is that before transmission, a station really wants to know that whether or not there is any activity around the receiver. CSMA merely tells whether or not there is any activity around the station sensing the carrier. Security

Wireless LANs are subjected to possible breaches from unwanted monitoring. To overcome this problem, IEEE 802.11 specifies an optional MAC layer security system known as *Wired Equivalent Privacy* (WEP). The objective is to provide a level of privacy to the wireless LAN similar to that enjoyed by wired Ethernets. It is achieved with the help of a 40-bit shared key authentication service. By default each BSS

supports up to four 40-bit keys that are shared by all the clients in the BSS. Keys unique to a pair of communicating clients and direction of transmission may also be used. Advanced Encryption Standard (AES) (802.11i) for authentication and encryption is recommended as a long-term solution.

2.1.4 Frame Control Field (in MAC header)

- **The protocol version field is 2 bits in length and will carry the version of the 802.11 standard. The initial value of 802.11 is 0; all other bit values are reserved.**
- **Type and subtype fields are 2 and 4 bits, respectively. They work together hierarchically to determine the function of the frame.**
- **The remaining 8 fields are all 1 bit in length.**
- **The To DS field is set to 1 if the frame is destined for the distribution system.**
- **From DS field is set to 1 when frames exit the distribution system. Note that frames which stay within their basic service set have both of these fields set to 0.**
- **The More Frag field is set to 1 if there is a following fragment of the current MSDU.**

- **Retry is set to 1 if this frame is a retransmission.**
- **Power Management field indicates if a station is in power save mode (set to 1) or active (set to 0).**
- **More data field is set to 1 if there is any MSDUs are buffered for that station.**
- **The WEP field is set to 1 if the information in the frame body was processed with the WEP algorithm.**
- **The Order field is set to 1 if the frames must be strictly ordered.**
- **The Duration/ID field is 2 bytes long. It contains the data on the duration value for each field and for control frames it carries the associated identity of the transmitting station.**
- **The address fields identify the basic service set, the destination address, the source address, and the receiver and transmitter addresses. Each address field is 6 bytes long.**
- **The sequence control field is 2 bytes and is split into 2 subfields, fragment number and sequence number.**
- **Fragment number is 4 bits and tells how many fragments the MSDU is broken into.**
- **The sequence number field is 12 bits that indicates the sequence number of the MSDU. The frame body is a variable length field from 0 - 2312. This is the payload.**

2.2 IEEE 802.16 STANDARD

WiMAX: The story of wireless LAN cannot be complete without the mention of WiMAX, which stands for Worldwide Interoperability for Microwave Access by the WiMAX Forum. The forum was formed in June 2001 to promote conformance and interoperability of the IEEE 802.16 standard, officially known as Wireless (Metropoliton Area Network) MAN. The Forum describes WiMAX as "a standards- based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL". It supports point to multi-point (PMP) broadband wireless access. WiMAX can deliver a maximum of 70 Mbit/s, over a maximum distance of 70 miles (112.6 kilometers). It has some similarities to DSL in this respect, where one can either have high bandwidth or long range, but not both simultaneously. The other feature to consider with WiMAX is that available bandwidth is shared between users in a given radio sector, so if there are many active users in a single sector, each will get reduced bandwidth.

2.2.1 802.16 Standards and Amendments

Although the original 802.16 standard along with amendments a, b, and c are now withdrawn, there are still many documents that are being used for defining and evolving the 802.16 standard. A summary of the major documents, including those that have been withdrawn is given below

STANDARD / AMENDMENT	COMMENTS
802.16	Now withdrawn. This is the basic 802.16 standard that was released in 2001. It provided for basic high data links at frequencies between 11 and 60 GHz.
802.16a	Now withdrawn. This amendment addressed certain spectrum issues and enabled the standard to be used at frequencies below the 11 GHz minimum of the original standard.
802.16b	Now withdrawn. It increased the spectrum that was specified to include frequencies between 5 and 6 GHz while also providing for Quality of Service aspects.
802.16c	Now withdrawn. This amendment to 802.16 provided a system profile for operating between 10 and 66 GHz and provided more details for operations within this range. The aim was to enable greater levels of interoperability.
802.16d (802.16-2004)	This amendment was also known as 802.16-2004 in view of the fact that it was released in 2004. It was a major revision of the 802.16 standard and upon its release, all previous documents were withdrawn. The standard / amendment provided a number of fixes and improvements to 802.16a including the use of 256 carrier OFDM. Profiles for compliance testing are also provided, and the standard was aligned with the ETSI HiperMAN standard to allow for global deployment. The standard only addressed fixed operation.
802.16e (802.16-2005)	This standard, also known as 802.16-2005 in view of its release date, provided for nomadic and mobile use. With lower data rates of 15 Mbps against to 70 Mbps of 802.16d, it enabled full nomadic and mobile use including handover.

STANDARD / AMENDMENT	COMMENTS
802.16f	Management information base
802.16g	Management plane procedures and services
802.16h	Improved coexistence mechanisms for license-exempt operation
802.16j	Multi-hop relay specification
802.16k	802.16 bridging
802.16m	Advanced air interface. This amendment is looking toth e future and it is anticipated it will provide data rates of 100 Mbps for mobile applications and 1 Gbps for fixed applications. It will allow cellular, macro and micro cell coverage, with currently there are no restrictions on the RF bandwidth although it is expected to be 20 MHz or more.

Table 2.1 Standards Comparsion

2.2.2 Summary of the IEEE 802.16 standards

In view of the fact that it is necessary for standards such as 802.16 to continually move forward, further amendments and documents will be issued as new development take place. Only by taking account of the way in which technology is moving and the new requirements for 802.16, can it keep pace with the needs of the users. One good example of a standard that has evolved is Ethernet. This standard has remained in use for many years, and will do so for many years to come. This has been achieved by simply upgrading the standard to keep pace with the needs of the users. In this way it has been the major networking standard for over 30 years. This too could be true for the IEEE 802.16 standard.

2.2.3 Comparison between 802.11/ WiFi and 802.16/WiMAX

WiMAX is similar to the wireless standard known as Wi-Fi, but on a much larger scale and at faster speeds. A nomadic version would keep WiMAX-enabled devices connected over large areas, much like today's cell phones. We can compare it with Wi-Fi based on the following factors.

IEEE Standards :

Wi-Fi is based on IEEE 802.11 standard whereas WiMAX is based on IEEE 802.16. However, both are IEEE standards.

Range :

Wi-Fi typically provides local network access for a few hundred feet with the speed of up to 54 Mbps, a single WiMAX antenna is expected to have a range of up to 40 miles with the speed of 70 Mbps or more. As such, WiMAX can bring the underlying Internet connection needed to service local Wi-Fi networks.

Scalability :

Wi-Fi is intended for LAN applications, users scale from one to tens with one subscriber for each CPE device. Fixed channel sizes (20MHz).

WiMAX is designed to efficiently support from one to hundreds of Consumer premises equipments (CPE)s, with unlimited subscribers behind each CPE. Flexible channel sizes from 1.5MHz to 20MHz.

Bit rate :

Wi-Fi works at 2.7 bps/Hz and can peak up to 54 Mbps in 20 MHz channel. WiMAX works at 5 bps/Hz and can peak up to 100 Mbps in a 20 MHz channel.

Quality of Service:

Wi-Fi does not guarantee any QoS but WiMax will provide your several level of QoS.

As such, WiMAX can bring the underlying Internet connection needed to service local Wi-Fi networks. Wi-Fi does not provide ubiquitous broadband while WiMAX does.

Feature	WiMax (802.16a)	Wi-Fi (802.11b)	Wi-Fi (802.11a/g)

Primary Application	Broadband Wireless Access	Wireless LAN	Wireless LAN
Frequency Band	Licensed/Unlicensed 2 G to 11 GHz	2.4 GHz ISM	2.4 GHz ISM (g) 5 GHz U-NII (a)
Channel Bandwidth	Adjustable	25 MHz	20 MHz
Half/Full Duplex	Full	Half	Half
Radio Technology	OFDM	Direct Sequence	OFDM
Bandwidth Efficiency	<=5 bps/Hz	<=0.44 bps/Hz	<=2.7 bps/Hz
Modulation	BPSK, QPSK,	QPSK	BPSK, QPSK, 16-, 64-QAM
FEC	Convolutional Code Reed-Solomon	None	Convolutional Code
Mobility	Mobile WiMax (802.16e)	In development	In development
Mesh	Yes	Vendor Proprietary	Vendor Proprietary
Access Protocol	Request/Grant	CSMA/CA	CSMA/CA

Table 2.2 Comparison of various IEEE Standards

2.3 WIRELESSES LOCAL LOOP:

A local loop connects a subscriber to the service provider's switch, this connection is usually a wire; typically copper wire. Advanced studies on the capabilities of copper wire as a transmission medium has made it possible to use the local loop to offer services other than the basic voice service. This technology known as digital subscriber line technology (DSL) utilizes the existing copper wires to provide high speed data services. Optical fibre is a better option particularly for its large bandwidth but cost restricts its use as a local loop.

Wireless local loop eliminates the need for wires as the subscriber's equipment is wirelessly connected to the provider's network. Wireless local loop (WLL) is a popular alternative as it has been deployed in both developed and developing nations because of its advantages. With an ever increasing demand to access the internet, the wireless local loop has evolved seeking to meet such demand.

Wireless local loop also known as radio local loop uses radio signals to complete

the last lap to the user's premises. Wireless local loop is particularly suited to remote locations providing access to provider's infrastructure and in areas where the terrain makes it impossible to lay cables. Wireless local loop offers a number of advantages over its wire line counterpart.

1) **Fast deployment**
2) **Low installation cost**
3) **Low maintenance cost**
4) **High system capacity**

There are several wireless local loop (WLL) technologies available, hence, the technology deployed for a particular area will depend on the population density and service needs of the users.

2.3.1 WIRELESS LOCAL LOOP SYSTEM ARCHITECTURE:

The wireless local loop architecture is shown in figure 2.4. The fixed subscriber unit (FSU) is an interface between subscriber's wired devices and wireless local loop network. The wired devices can be computers as well as telephones. The fixed subscriber performs channel coding and decoding, modulation and demodulation, and transmission/reception of signal via radio.

The base transceiver system (BTS) performs channel coding/decoding, modulation and demodulation as well as transmission and reception of signal via radio. The base transceiver system is also referred to as the radio port (RP). A base station controller (BSC) controls one or more base transceiver systems (BTSs) and provides an interface to the local exchange (switch) in the central office.

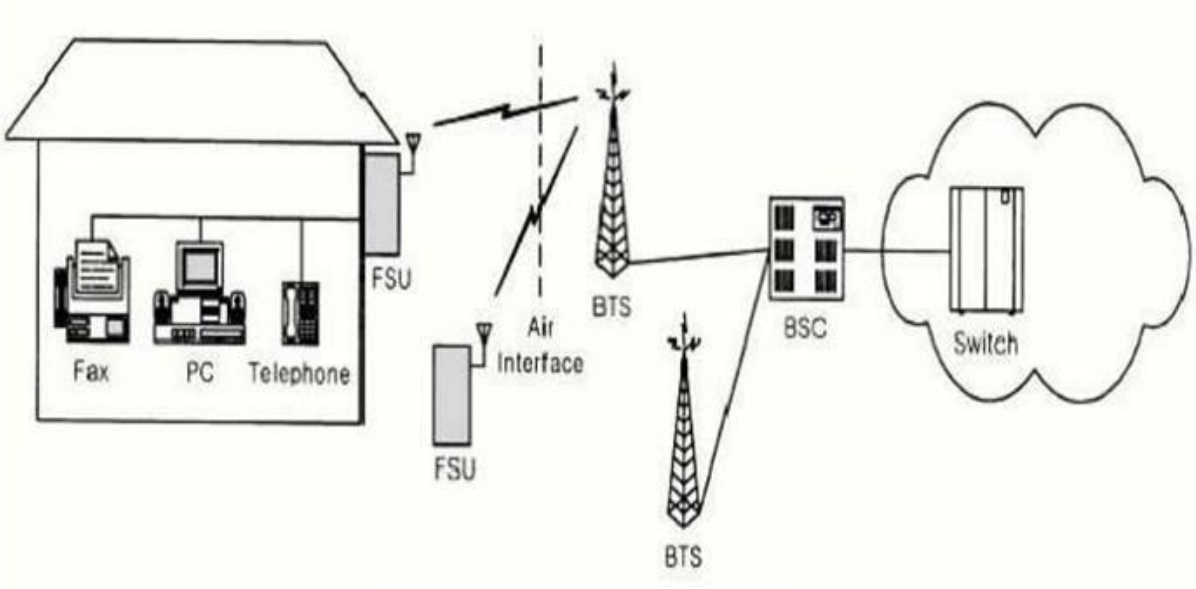


Figure 2.4 WLL Architecture

2.3.2 SUMMARY OF WIRELESS LOCAL LOOP SERVICES

It is developed for a digital cellular system with direct sequence (DS) CDMA technology, operating at 800MHz band. IS-95 based CDMA wireless local loop can support two rate sets. A code channel (traffic channel) operates at a maximum of 9.6 kbps with the rate set 1 or 14.4 kbps with rate set

2. IS-95B offers high speed data services through code aggregation. In IS-95B systems, multiple codes (up to eight codes) may be assigned to a connection. In CDMA systems pseudo-noise (PN) sequences are used for the different user signals with the same transmission bandwidth.

Wideband code division multiple access (W-CDMA) in comparison with narrowband CDMA systems (IS-95) use higher chip rate for direct sequence spread spectrum and, thus, spread its information into wider spectrum bandwidth (typically, equal to or over 5 MHz). Thus, data rate per code channel in W-CDMA can be higher than that in narrowband system. The wireless local loop standard defines several options for voice codecs: 64 kbps PCM, 32 kbps ADPCM, 16 kbps LD-CELP, and 8 kbps conjugate structure algebraic-code-excited linear prediction (CS-ACELP). CDMA based systems offer higher capacity and flexibility compared to other digital standards.

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF ELECTRICAL AND ELECTRONICS
DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

UNIT – III – MOBILE COMMUNICATION SYSTEMS – SEC1614

III GSM

3.1 GSM Architecture

GSM consists of many subsystems, such as the mobile station (MS), the base station sub system (BSS), the network and switching subsystem (NSS), and the operation subsystem (OSS).

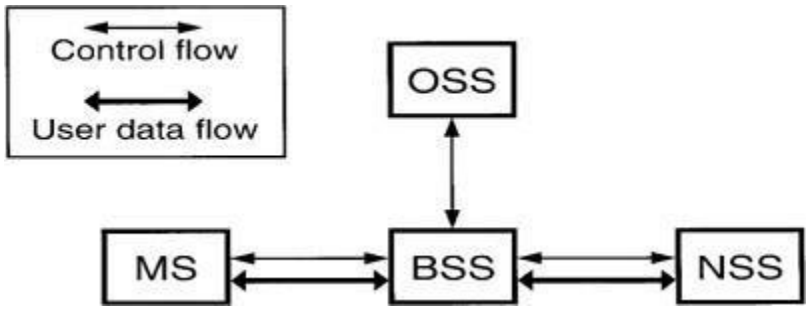


Fig 3.1 The external environment of BSS

3.1.1 The Mobile Station: The MS may be a stand-alone piece of equipment for certain services or support the connection of external terminals, such as the interface for a personal computer or fax. The MS includes mobile equipment (ME) and a subscriber identity module (SIM). ME does not need to be personally assigned to one subscriber. The SIM is a subscriber module which stores all the subscriber- related information. When a subscriber's SIM is inserted into the ME of an MS, that MS belongs to the subscriber, and the call is delivered to that MS. The ME is not associated with a called number it is linked to the SIM. In this case, any ME can be used by a subscriber when the SIM is inserted in the ME.

3.1.2 Base Station Subsystem:

The BSS connects to the MS through a radio interface and also connects to the NSS. The BSS consists of a base transceiver station (BTS) located at the antenna site and a base station controller (BSC) that may control several BTSs. The BTS consists of radio transmission and reception equipment similar to the ME in an MS.

A transcoder/rate adaption unit (TRAU) carries out encoding and speech decoding and rate adaptation for transmitting data. As a subpart of the BTS, the TRAU may be sited away from the BTS, usually at the MSC. In this case, the low transmission rate of speech code channels allows more compressed transmission between the BTS and the TRAU, which is sited at the MSC. GSM uses the open system interconnection (OSI). There are three common interfaces based on OSI (Fig. 3.1.): a common radio interface, called air interface, between the MS and BTS, an interface A between the MSC and BSC, and an A-bis interface between the BTS and BSC. With these common interfaces, the system operator can purchase the product of manufacturing company A to interface with the product of manufacturing company B. The difference between interface and protocol is that an interface represents the point of contact between two adjacent entities (equipment or systems) and a protocol provides information flows through the interface.

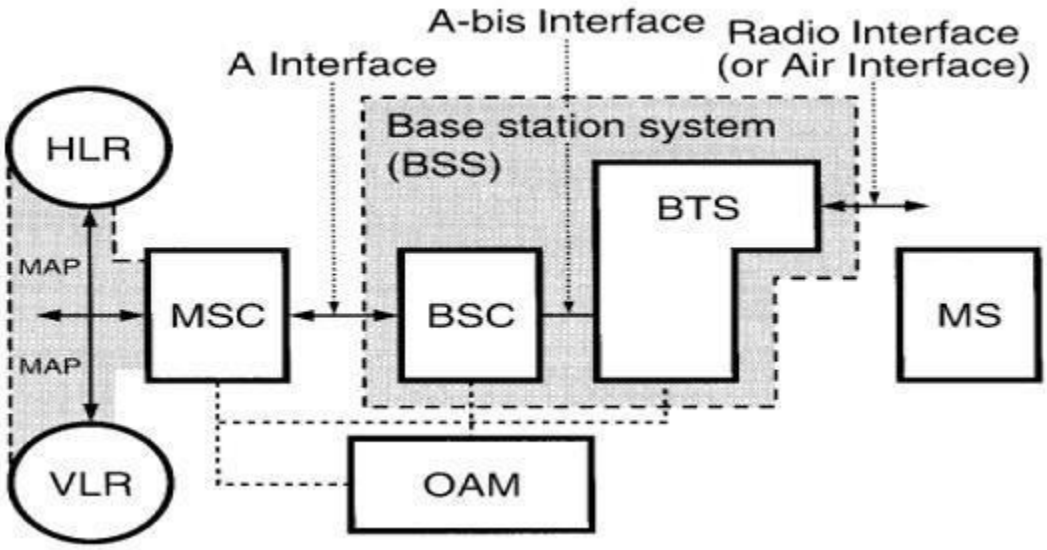


Fig 3.2 the functional architecture and principal interfaces

For example, the GSM radio interface is the transit point for information flow pertaining to several protocols.

3.2 Network and Switching Subsystem: **NSS (see Fig. 3.2.) in GSM uses an intelligent network (IN). The IN's attributes will be described later. A signaling NSS includes the main switching functions of GSM. NSS manages the communication between GSM users and other telecommunications users. NSS management consists of:**

3.2.1 Mobile service switching center (MSC): **Coordinates call set-up to and from GSM users. An MSC controls several BSCs.**

3.2.2 Interworking function (IWF): **A gateway for MSC to interface with external networks for communication with users outside GSM, such as packet-switched public data network (PSPDN) or circuit-switched public data network (CSPDN).The role of the IWF depends on the type of user data and the network to which it interfaces.**

3.2.3 Home location register (HLR): **Consists of a stand-alone computer without switching capabilities, a database which contains subscriber information, and information related to the subscriber's current location, but not the actual location of the subscriber. A subdivision of HLR is the authentication center (AUC). The AUC manages the security data for subscriber authentication. Another sub-division of HLR is the equipment identity register (EIR) which stores the data of mobile equipment (ME) or ME-related data.**

3.2.4 Visitor location register (VLR): **Links to one or more MSCs, temporarily storing subscription data currently served by its corresponding MSC, and holding more detailed data than the HLR.**

For example, the VLR holds more current subscriber location information than the location information at the HLR.

3.2.5 Gateway MSC (GMSC): **In order to set up a requested call, the call is initially routed to a gateway MSC, which finds the correct HLR by knowing the directory number of the GSM subscriber. The GMSC has an interface with the external network for gatewaying, and the network also operates the full Signaling System 7 (SS7) signaling between NSS machines.**

3.2.6 Signaling transfer point (STP): **Is an aspect of the NSS function as a stand-alone node or in the same equipment as the MSC. STP optimizes the cost of the signaling transport among MSC/VLR, GMSC, and HLR. As mentioned earlier, NSS uses an intelligent network. It separates the central data base (HLR) from the switches (MSC) and uses STP to transport signaling among MSC and HLR.**

3.3 Operation Subsystem: **There are three areas of OSS, as shown in Fig.3.4. (1) network operation and maintenance functions, (2) subscription management, including charging and billing, and (3)mobile equipment management. These tasks require interaction between some or all of the infrastructure equipment. OSS is implemented in any existing network.**

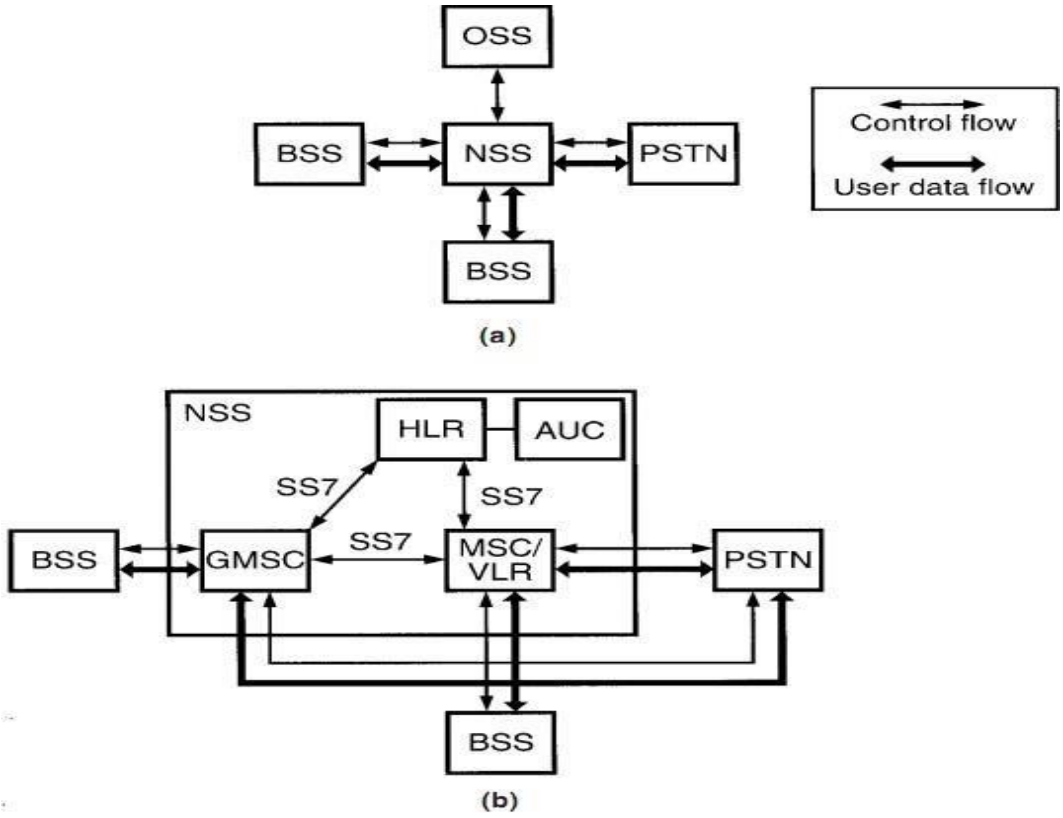


Fig.3.3. NSS and its environment (a) the external environment; (b) the internal structure

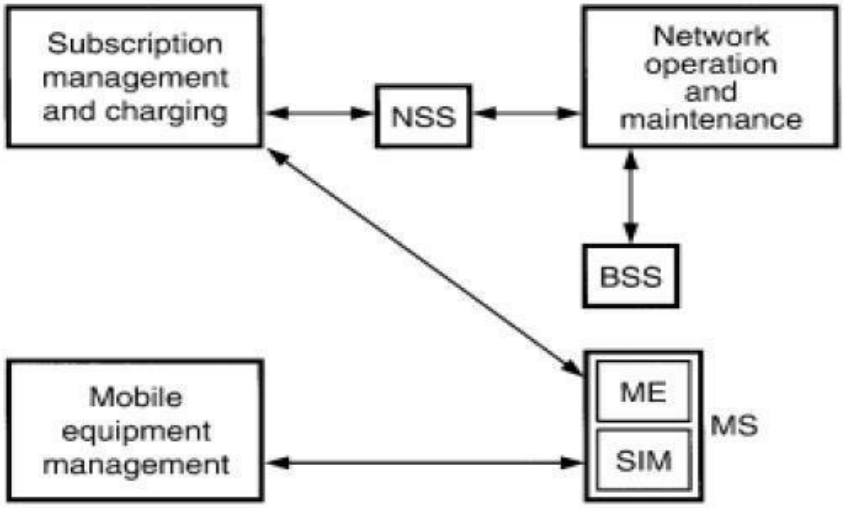


Fig.3.4. OSS organization

3.3.1GSM Channel Structure:

The services offered to users have four radio transmission modes, three data modes, and a speech mode. The radio transmission modes use the physical channels.

Physical Channels: There are three kinds of physical channels, also called traffic channels (TCHs):

1.TCH/F (full rate): Transmits a speech code of 13 kbps or three data-mode rates, 12, 6, and 3.6 kbps.

2.TCH/H (half rate): Transmits a speech code of 7 kbps or two data modes, 6 and 3.6 kbps.

3.TCH/8 (one-eighth rate): Used for low-rate signaling channels, common channels, and data channels.

3.3.2Logic channels:

1. Common channels: All the common channels are embedded in different traffic channels. They are grouped by the same cycle (51 × 8 BP), where BP stands for burst period (i.e., time slot), which is 577 µs.

2. Downlink common channels: There are five downlink unidirectional channels, shared or grouped by a TCH.

- **Frequency correction channel (FCCH) repeats once every 51×8 BPs; used to identify a beacon frequency.**
- **Synchronization channel (SCH) follows each FCCH slot by 8 BPs.**
- **Broadcast control channel (BCCH) is broadcast regularly in each cell and received by all the mobile stations in the idle mode.**
- **Paging and access grant channel (PAGCH) is used for the incoming call received at the mobile station. The access grant channel is answered from the base station and allocates a channel during the access procedure of setting up a call.**
- **Call broadcast channel (CBCH). Each cell broadcasts a short message for 2s from the network to the mobile station in idle mode. Half a downlink TCH/8 is used, and special CBCH design constraints exist because of the need for sending two channels (CBCH and BCCH) in parallel. The mobile station (MS) finds the FCCH burst, then looks for an SCH burst on the same frequency to achieve synchronization. The MS then receives BCCH on several time slots and selects a proper cell, remaining for a period in the idle mode.**

3. Uplink common channels: The random-access channel (RACH) is the only common uplink channel. RACH is the channel that the mobile station chooses to access the calls. There are two rates: RACH/F (full rate, one time slot every 8 BP), and RACH/H (half rate, using 23 time slots in the 51 × 8 BP cycle, where 8 BP cycle [i.e. a frame] is 4.615ms).

4. Signaling channels: All the signaling channels have chosen one of the physical channels and the logical channels names are based on their logical functions:

5. Slow Associated Control Channel (SACCH): A slow-rate TCH used for signaling transport and used for non urgent procedures, mainly handover decisions. It uses one-eighth rate. The TCH/F is always allocated with SACCH. This combined TCH and SACCH is denoted TACH/F. SACCH occupies 1 time slot (0.577 ms) in every 26 frames (4.615ms × 26). The time organization of a TACH/F is shown in Fig.3.5.

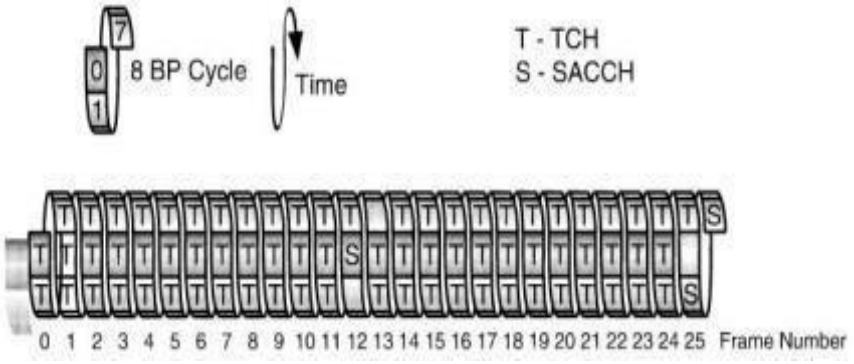


Fig.3.5. Time organization of TACH/F6.

6. Fast Associated Control Channel (FACCH): Indicates cell establishment, authenticates subscribers, or commands a handover.

7. Stand-alone Dedicated Control Channel (SDCCH): Occasionally the connection between a mobile station and the network is used solely for passing signaling information and not for calls. This connection may be at the user's demand or for other management operations such as updating the unit's location. It operates at a very low rate and uses a TCH/8 channel. Radio slots are allocated to users only when call penetration is needed. There are two modes, dedicated and idle. The mode used depends on the uplink and the downlink. In GSM terminology, the downlink is the signal transmitted from the base station to the mobile station, and the uplink is the signal transmitted in the opposite direction.

8. Voice/data channels: Each time slot of a voice channel contains 260 bits per block. The entire block contains 316 bits. Each time slot of a data channel contains 120 or 240 bits per block.

3.4 The different modes of GSM channel are as follows

1. **Channel mode: Because of the precious value of the radio spectrum, individual users cannot have their own TCH at all times.**
2. **Dedicated mode: Uses TCH during call establishment and uses SACCH to perform location updating in the dedicated mode. TCH and SACCH are dedicated channels for both**

uplink and downlink channels.

3. Idle mode: During non call activities, the five downlink channels are in the idle mode: FCCH; SCH; BCCH, which is broadcasting regularly; PAGCH and CBCH, which sends one message every 2 s. During idle mode, the mobile station listens to the common downlink channels, and also uses SDCCH (uplink channel) to register a mobile location associated with a particular base station to the network.

3.5 GSM Mobility Management

Mobility management is one of the major functions of a GSM or a UMTS network that allows mobile phones to work. The aim of mobility management is to track where the subscribers are, allowing calls, SMS and other mobile phone services to be delivered to them.

3.5.1 Location update procedure :

A GSM or UMTS network, like all cellular networks, is basically a radio network of individual cells, known as base stations. Each base station covers a small geographical area which is part of a uniquely identified location area. By integrating the coverage of each of these base stations, a cellular network provides a radio coverage over a much wider area. A group of base stations is named a location area, or a routing area.

The location update procedure allows a mobile device to inform the cellular network, whenever it moves from one location area to the next. Mobiles are responsible for detecting location area codes (LAC). When a mobile finds that the location area code is different from its last update, it performs another update by sending to the network, a location update request, together with its previous location, and its Temporary Mobile Subscriber Identity (TMSI).

The mobile also stores the current LAC in the SIM card, concatenating it to a list of recently used LACs. This is done to avoid unnecessary IMSI attachment procedures in case the mobile has been forced to switch off (by removing the battery, for example) without having a chance to notify the network with an IMSI detach and then switched on right after it has been turned off. Considering the fact that the mobile is still associated with the Mobile Switching Center/Visitor Location Register (MSC/VLR) of the current location area, there is no need for any kind of IMSI attachment procedures to be done.

3.5.2 TMSI:

The Temporary Mobile Subscriber Identity (TMSI) is the identity that is most commonly sent between the mobile and the network. TMSI is randomly assigned by the VLR to every mobile in the area, the moment it is switched on. The number is local to a location area, and so it has to be updated each time the mobile moves to a new geographical area.

The network can also change the TMSI of the mobile at any time. And it normally does so, in order to avoid the subscriber from being identified, and tracked by eavesdroppers on the radio interface. This makes it difficult to trace which mobile is which, except briefly, when the mobile is just switched on, or when the data in the mobile becomes invalid for one reason or another. At that point, the global "international mobile subscriber identity" (IMSI) must be sent to the network. The IMSI is sent as rarely as possible, to avoid it being identified and tracked.

3.5.3 Roaming:

Roaming is one of the fundamental mobility management procedures of all cellular networks. Roaming is defined as the ability for a cellular customer to automatically make and receive voice calls, send and receive data, or access other services, including home data services, when travelling outside the geographical coverage area of the home network, by means of using a visited network. This can be done by using a communication terminal or else just by using the subscriber identity in the visited network. Roaming is technically supported by a mobility management, authentication, authorization and billing procedures.

3.6 Location Related Databases

Two databases are used by Location Management to store MS location related data.

- **Visitor Location Register(VLR)**
- **Home Location Register(HLR)**

3.6.1 Visitor Location Register

A VLR contains a data record for each of the MS that are currently operating in its area. Each record contains a set of subscriber identity codes, related subscription information, and a Location Area Identity (LAI) code. This information is used by the MSC when handling calls to or from an MS in the area. When an MS moves from one area to another, the responsibility for its supervision passes from one VLR to another. A new data record is created by the VLR that

has adopted the MS, and the old record is deleted. Provided that aninter-working agreement exists between the network operators

concerned, data transaction can cross both network and national boundaries.

3.6.2 Home Location Register

The HLR contains information relevant to mobile subscribers who are fee-paying customers of the organization that operates the PLMN.

Subscription Information

The subscription information includes the IMSI and directory number allocated to the subscriber, the type of services provided and any related restrictions.

Location Information

The location information includes the address of the VLR in the area where the subscribers MS is currently located and the address of the associated MSC.

The location information enables incoming calls to be routed to the MS. The absence of this information indicates that the MS is inactive and cannot be reached.

When an MS moves from one VLR area to another, the location information in the HLR is updated with the new entry for the MS, using subscription data copied from the HLR. Provided that an inter- working agreement exists between the network operators, concerned data transactions can move across both network and national boundaries.

Types of Identification Numbers

During the performance of the location update procedure and the processing of a mobile call different types of numbers are used

- **Mobile Station ISDN Number(MSISDN)**
- **Mobile Subscriber Roaming Number(MSRN)**
- **International Mobile Subscriber**
- **Identity(IMSI) Temporary Mobile**
- **Subscriber Identity(TMSI) Local Mobile Station Identity(LMSI).**

3.7 GSM Handover

One of the key elements of a mobile phone or cellular telecommunications system, is that the system is split into many small cells to provide good frequency re-use and coverage. However

as the mobile moves out of one cell to another it must be possible to retain the connection. The process by which this occurs is known as handover or handoff. The term handover is more widely used within Europe, whereas handoff tends to be use more in North America. Either way, handover and handoff are the same process.

3.8 Requirements for GSM handover

The process of handover or handoff within any cellular system is of great importance. It is a critical process and if performed incorrectly handover can result in the loss of the call. Dropped calls are particularly annoying to users and if the number of dropped calls rises, customer dissatisfaction increases and they are likely to change to another network. Accordingly GSM handover was an area to which particular attention was paid when developing the standard.

3.9 Types of GSM handover

Within the GSM system there are four types of handover that can be performed for GSM only systems:

- ***Intra-BTS handover:*** **This form of GSM handover occurs if it is required to change the frequency or slot being used by a mobile because of interference, or other reasons. In this form of GSM handover, the mobile remains attached to the same base station transceiver, but changes the channel or slot.**
- ***Inter-BTS Intra BSC handover:*** **This for of GSM handover or GSM handoff occurs when the mobile moves out of the coverage area of one BTS but into another controlled by the same BSC. In this instance the BSC is able to perform the handover and it assigns a new channel and slot to the mobile, before releasing the old BTS from communicating with the mobile.**
- ***Inter-BSC handover:*** **When the mobile moves out of the range of cells controlled by one BSC, a more involved form of handover has to be performed, handing over not only from one BTS to another but one BSC to another. For this the handover is controlled by the MSC.**

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

3.10 GSM handover process

Although there are several forms of GSM handover as detailed above, as far as the mobile is concerned, they are effectively seen as very similar. There are a number of stages involved in undertaking a GSM handover from one cell or base station to another.

In GSM which uses TDMA techniques the transmitter only transmits for one slot in eight, and similarly the receiver only receives for one slot in eight. As a result the RF section of the mobile could be idle for 6 slots out of the total eight. This is not the case because during the slots in which it is not communicating with the BTS, it scans the other radio channels looking for beacon frequencies that may be stronger or more suitable. In addition to this, when the mobile communicates with a particular BTS, one of the responses it makes is to send out a list of the radio channels of the beacon frequencies of neighboring BTSs via the Broadcast Channel (BCCH).
The mobile scans these and reports back the quality of the link to the BTS. In this way the mobile assists in the handover decision and as a result this form of GSM handover is known as Mobile Assisted Hand Over (MAHO).

The network knows the quality of the link between the mobile and the BTS as well as the strength of local BTSs as reported back by the mobile. It also knows the availability of channels in the nearby cells. As a result it has all the information it needs to be able to make a decision about whether it needs to hand the mobile over from one BTS to another.

If the network decides that it is necessary for the mobile to hand over, it assigns a new channel and time slot to the mobile. It informs the BTS and the mobile of the change. The mobile then retunes during the period it is not transmitting or receiving, i.e. in an idle period.

A key element of the GSM handover is timing and synchronization. There are a number of possible scenarios that may occur dependent upon the level of synchronization.

3.11 GSM User Services:

GSM offers three basic types of services:

- **Telephony services or**
- **teleservices Data services or bearer services Supplementary services**

3.11.1Teleservices

The abilities of a Bearer Service are used by a Tele-service to transport data. These services are further transited in the following ways:

2.Voice Calls

The most basic Teleservice supported by GSM is telephony. This includes full-rate speech at 13 kbps and emergency calls, where the nearest emergency-service provider is notified by dialing three

digits.

3.Videotext and Facsmile

Another group of teleservices includes Videotext access, Teletex transmission, Facsmile alternate speech and Facsmile Group 3, Automatic Facsmile Group, 3 etc.

3.11.2 Short Text Messages

Short Messaging Service (SMS) service is a text messaging service that allows sending and receiving text messages on your GSM mobile phone. In addition to simple text messages, other text data including news, sports, financial, language, and location-based data can also be transmitted.

1.Bearer Services

Data services or Bearer Services are used through a GSM phone. to receive and send data is the essential building block leading to widespread mobile Internet access and mobile data transfer. GSM currently has a data transfer rate of 9.6k. New developments that will push up data transfer rates for GSM users are HSCSD (high speed circuit switched data) and GPRS (general packet radio service) are now available.

3.11.3 Supplementary Services

Supplementary services are additional services that are provided in addition to teleservices and bearer services. These services include caller identification, call forwarding, call waiting, multi-party conversations, and barring of outgoing (international) calls, among others. A brief description of supplementary services is given here:

- **Conferencing : It allows a mobile subscriber to establish a multiparty conversation, i.e., a simultaneous conversation between three or more subscribers to setup a conference call. This service is only applicable to normal telephony.**
- **Call Waiting : This service notifies a mobile subscriber of an incoming call during a conversation. The subscriber can answer, reject, or ignore the incoming call.**
- **Call Hold : This service allows a subscriber to put an incoming call on hold and resume after a while. The call hold service is applicable to normal telephony.**
- **Call Forwarding : Call Forwarding is used to divert calls from the original recipient to another number. It is normally set up by the subscriber himself. It can be used by the subscriber to divert calls from the Mobile Station when the subscriber is not available, and so to ensure that calls are not lost.**

- **Call Barring : Call Barring is useful to restrict certain types of outgoing calls such as ISD or stop incoming calls from undesired numbers. Call barring is a flexible service that enables the subscriber to conditionally bar calls.**
- **Number Identification : There are following supplementary services related to number identification:**
  - **Calling Line Identification Presentation : This service displays the telephone number of the calling party on your screen.**
  - **Calling Line Identification Restriction : A person not wishing their number to be presented to others subscribes to this service.**
  - **Connected Line Identification Presentation : This service is provided to give the calling party the telephone number of the person to whom they are connected. This service is useful in situations such as forwarding's where the number connected is not the number dialled.**
  - **Connected Line Identification Restriction : There are times when the person called does not wish to have their number presented and so they would subscribe to this person. Normally, this overrides the presentation service.**
  - **Malicious Call Identification : The malicious call identification service was provided to combat the spread of obscene or annoying calls. The victim should subscribe to this service, and then they could cause known malicious calls to be identified in the GSM network, using a simple command.**
- **Advice of Charge (AoC) : This service was designed to give the subscriber an indication of the cost of the services as they are used. Furthermore, those service providers who wish to offer rental services to subscribers without their own SIM can also utilize this service in a slightly different form. AoC for data calls is provided on the basis of time measurements.**
- **Closed User Groups (CUGs) : This service is meant for groups of subscribers who wish to call only each other and no one else.**
- **Unstructured supplementary services data (USSD) : This allows operator-defined individual services.**

3.12 GSM International mobile Roaming:

International mobile roaming is a service that allows mobile users to continue to use their mobile phone or other mobile device to make and receive voice calls and text messages, browse

the internet, and send and receive emails, while visiting another country. Roaming extends the coverage of the

home operator's retail voice and SMS services, allowing the mobile user to continue using their home operator phone number and data services within another country. The seamless extension of coverage is enabled by a wholesale roaming agreement between a mobile user's home operator and the visited mobile operator network. The roaming agreement addresses the technical and commercial components required to enable the service.

The most common international roaming services are:

Voice: Making and receiving calls to or from home country, visited country or a third country, while abroad

SMS: Sending and receiving text messages to or from home country, visited country or a third country, while abroad

Email: Reading and replying to emails while abroad

Mobile broadband: Using mobile devices or dongles to access the internet, including downloading images, MP3s, films and software, while abroad

Applications: Using mobile applications while abroad that require mobile data, such as location-based services and language translators. International mobile roaming is one of a wider range of communications services offered to mobile users while travelling abroad, which also include hotel services, Wi-Fi, national "travel" SIMs, and visited operator SIMs.

3.13 How mobile roaming works?

When a mobile user is abroad and turns their mobile device on, the mobile device attempts to communicate with a visited mobile network. The visited network picks up the connection from the user's mobile, recognizes whether Figure 3.7 the shows commercial and technical details for international mobile roaming. The diagram focuses on the international roaming wholesale and retail arrangements, for simplicity. The mobile user (Mobile User A) has an international roaming service with their home operator (Home Operator) and is automatically connected to a visited network (Visited Operator A) while roaming. Mobile User A is automatically granted access to Visited Operator A's network when arriving in the visited country by an exchange of a data between Home Operator and Visited Operator A, where Visited Operator A confirms Mobile User A is a roaming customer with Home Operator. As such, the wholesale roaming agreement between Visited Operator A and Home Operator specifies how this data is to be provided to the visited operator. Home Operator usually has wholesale roaming agreements with more than one operator in the same visited country, which in this case is Visited Operator A and a second network, Visited Operator B. As a result, Mobile User A can call home using either visited operator networks, both

of which use international transit services to carry

the call back to Mobile User A's home country. Mobile User A pays a retail price to Home Operator for the roaming service and does not pay Visited Operator A. Provided Mobile User B is not also roaming; they will not incur any extra charges to receive a call from, or to make calls to Mobile User A.Visited Operator A sends transferred account procedure (TAP) files to a clearing house which forwards them to the Home Operator. TAP files are used for billing of calls while roaming. Home Operator can then pay Visited Operator A the wholesale charges as per call volumes in the TAP file and rates in the wholesale roaming agreement. It is registered with its system, and attempts to identify the user's home network. If there is a roaming agreement between the home network and one of the mobile networks in the visited country, the call is routed by the visited network towards an international transit network (Figure 3.6). The international transit network carrier is responsible for the call delivery to the destination network. Once this is done, the destination network will connect the call.

The visited network also requests service information from the home network about the user, such as whether the phone being used is lost or stolen, and whether the mobile device is authorized for international use. If the phone is authorized for use, the visited network creates a temporary subscriber record for the device and the home network updates its subscriber record on where the device is located so if a call is made to the phone it can be appropriately routed.

Fig 3.6 overview of international roaming technology and operations

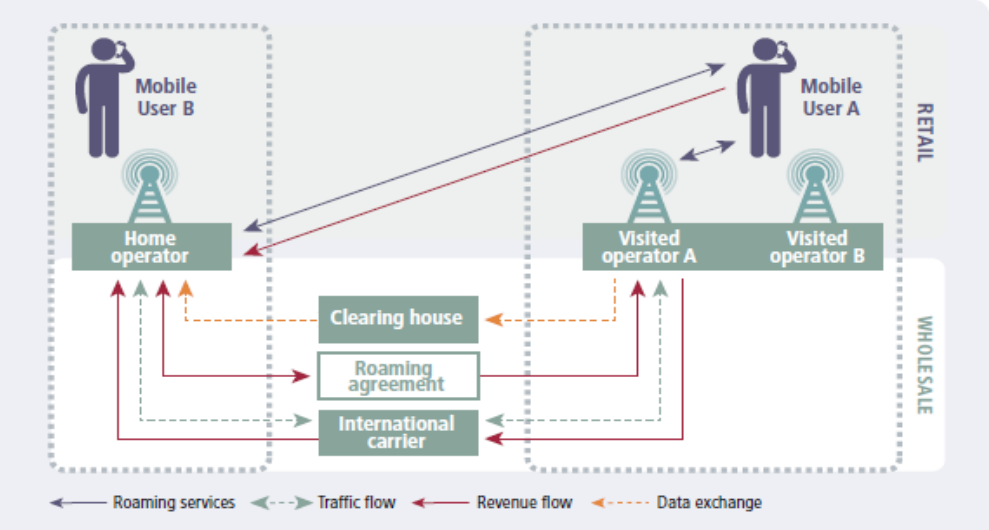


Fig 3.7 commercial link required for international mobile roaming

3.14 GSM Security:

- **GSM is the most secured cellular telecommunications system available today. GSM has its security methods standardized. GSM maintains end-to-end security by retaining the confidentiality of calls and anonymity of the GSM subscriber.**
- **Temporary identification numbers are assigned to the subscriber's number to maintain the privacy of the user. The privacy of the communication is maintained by applying encryption algorithms and frequency hopping that can be enabled using digital systems and signalling.**
- **This chapter gives an outline of the security measures implemented for GSM**
- **subscribers. Mobile StationAuthentication**
- **The GSM network authenticates the identity of the subscriber through the use of a challenge-response mechanism. A 128-bit Random Number (RAND) is sent to the MS. The MS computes the 32-bit Signed Response (SRES) based on the encryption of the RAND with the authentication algorithm (A3) using the individual subscriber authentication key (Ki). Upon receiving the SRES from the subscriber, the GSM network repeats the calculation to verify the identity of the subscriber.**
- **The individual subscriber authentication key (Ki) is never transmitted over the radio channel, as it is present in the subscriber's SIM, as well as the AUC, HLR, and VLR**

databases. If the received SRES agrees with the calculated value, the MS has been successfully authenticated and may continue. If the values do not match, the connection is terminated and an authentication failure is indicated to the MS.

- **The calculation of the signed response is processed within the SIM. It provides enhanced security, as confidential subscriber information such as the IMSI or the individual subscriber authentication key (Ki) is never released from the SIM during the authentication process.**
- **SignallingandDataConfidentiality**
- **The SIM contains the ciphering key generating algorithm (A8) that is used to produce the 64-bit ciphering key (Kc). This key is computed by applying the same random number (RAND) used in the authentication process to ciphering key generating algorithm (A8) with the individual subscriber authentication key (Ki).**
- **GSM provides an additional level of security by having a way to change the ciphering key, making the system more resistant to eavesdropping. The ciphering key may be changed at regular intervals as required. As in case of the authentication process, the computation of the ciphering key (Kc) takes place internally within the SIM. Therefore, sensitive information such as the individual subscriber authentication key (Ki) is never revealed by the SIM.**
- **Encrypted voice and data communications between the MS and the network is accomplished by using the ciphering algorithm A5. Encrypted communication is initiated by a ciphering mode request command from the GSM network. Upon receipt of this command, the mobile station begins encryption and decryption of data using the ciphering algorithm (A5) and the ciphering key (Kc).**
- **Subscriber IdentityConfidentiality**
- **To ensure subscriber identity confidentiality, the Temporary Mobile Subscriber Identity (TMSI) is used. Once the authentication and encryption procedures are done, the TMSI is sent to the mobile station. After the receipt, the mobile station responds. The TMSI is valid in the location area in which it was issued. For communications outside the location area, the Location Area Identification (LAI) is necessary in addition to the TMSI.**

3.15 GSM Billing:

GSM service providers are doing billing based on the services they are providing to their customers. All the parameters are simple enough to charge a customer for the provided services. This chapter provides an overview of the frequently used billing techniques and parameters applied to charge a GSM subscriber.

Telephony Service

These services can be charged on per call basis. The call initiator has to pay the charges, and the incoming calls are nowadays free. A customer can be charged based on different parameters such as:

- **International call or long distance call.**
- **Local call.**
- **Call made during peak hours.**
- **Call made during night time.**
- **Discounted call during weekends. Call per minute or per second.**
- **Many more other criteria can be designed by a service provider to charge their customers.**

SMSService

Most of the service providers charge their customer's SMS services based on the number of text messages sent. There are other prime SMS services available where service providers charge more than normal SMS charge. These services are being availed in collaboration of Television Networks or Radio Networks to demand SMS from the audiences. Most of the time, the charges are paid by the SMS sender but for some services like stocks and share prices, mobile banking facilities, and leisure booking services, etc. the recipient of the SMS has to pay for the service.

GPRS Services

Using GPRS service, you can browse, play games on the Internet, and download movies. So a service provider will charge you based on the data uploaded as well as data downloaded on your mobile phone. These charges will be based on per Kilo Byte data downloaded/uploaded.

Additional parameter could be a QoS provided to you. If you want to watch a movie, then a low QoS may work because some data loss may be acceptable, but if you are downloading a zip file, then a single byte loss will corrupt your complete downloaded file. Another parameter could be peak and off peak time to download a data file or to browse the Internet.

Supplementary Services

Most of the supplementary services are being provided based on monthly rental or absolutely free. For example, call waiting, call forwarding, calling number identification, and call on hold are available at zero cost.

Call barring is a service, which service providers use just to recover their dues, etc., otherwise this service is not being used by any subscriber.

Call conferencing service is a form of simple telephone call where the customers are charged for multiple calls made at a time. No service provider charges extra charge for this service.

Closed User Group (CUG) is very popular and is mainly being used to give special discounts to the users if they are making calls to a particular defined group of subscribers.

3.16 General Packet Radio System (GPRS):

General Packet Radio System is also known as GPRS is a third-generation step toward internet access. GPRS is also known as GSM-IP that is a Global-System Mobile Communications Internet Protocol as it keeps the users of this system online, allows to make voice calls, and access internet on-the-go. Even Time-Division Multiple Access (TDMA) users benefit from this system as it provides packet radio access.

GPRS also permits the network operators to execute an Internet Protocol (IP) based core architecture for integrated voice and data applications that will continue to be used and expanded for 3G services.

GPRS supersedes the wired connections, as this system has simplified access to the packet data networks like the internet. The packet radio principle is employed by GPRS to transport user data packets in a structure way between GSM mobile stations and external packet data networks. These packets can be directly routed to the packet switched networks from the GPRS mobile stations.

Key Features

Following three key features describe wireless packet data:

- **The always online feature - Removes the dial-up process, making applications only one click**

away.

- **An upgrade to existing systems - Operators do not have to replace their equipment; rather, GPRS is added on top of the existing infrastructure.**
- **An integral part of future 3G systems - GPRS is the packet data core network for 3G systems EDGE and WCDMA.**

3.17 Goals of GPRS

GPRS is the first step toward an end-to-end wireless infrastructure and has the following goals:

- **Open architecture**
- **Consistent IP services**
- **Same infrastructure for different air interfaces**
- **Integrated telephony and Internet infrastructure**
- **Leverage industry investment in IP**
- **Service innovation independent of infrastructure**

3.18 GPRS – Architecture:

GPRS architecture works on the same procedure like GSM network, but, has additional entities that allow packet data transmission. This data network overlaps a second-generation GSM network providing packet data transport at the rates from 9.6 to 171 kbps. Along with the packet data transport the GSM network accommodates multiple users to share the same air interface resources concurrently.

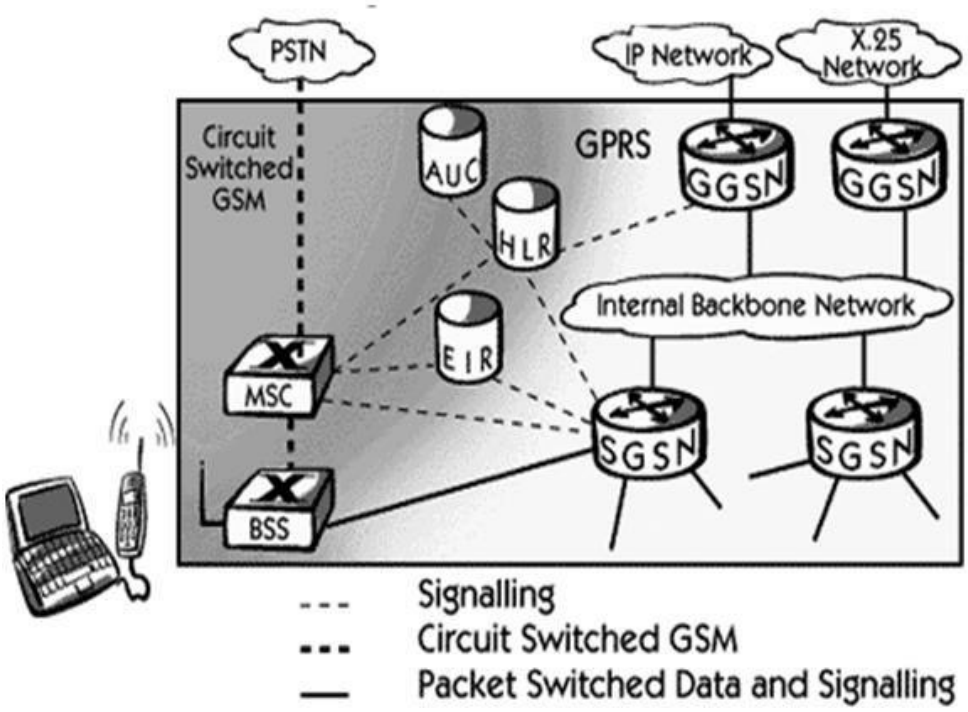


Fig 3.8 GPRS Architecture Block Diagram

3.18.1 GPRS Mobile Stations:

New Mobile Stations (MS) are required to use GPRS services because existing GSM phones do not handle the enhanced air interface or packet data. A variety of MS can exist, including a high-speed version of current phones to support high-speed data access, a new PDA device with an embedded GSM phone, and PC cards for laptop computers. These mobile stations are backward compatible for making voice calls using GSM.

3.18.2 GPRS Base Station Subsystem:

Each BSC requires the installation of one or more Packet Control Units (PCUs) and a software upgrade. The PCU provides a physical and logical data interface to the Base Station Subsystem (BSS) for packet data traffic. The BTS can also require a software upgrade but typically does not require hardware enhancements.

When either voice or data traffic is originated at the subscriber mobile, it is transported over the air interface to the BTS, and from the BTS to the BSC in the same way as a standard GSM call. However, at the output of the BSC, the traffic is separated; voice is sent to the Mobile Switching Center (MSC) per standard GSM, and data is sent to a new device called the SGSN via the PCU over a Frame Relay interface.

3.18.3 GPRS Support Nodes:

Following two new components, called Gateway GPRS Support Nodes (GSNs) and, Serving GPRS Support Node (SGSN) are added:

Gateway GPRS Support Node (GGSN)

The Gateway GPRS Support Node acts as an interface and a router to external networks. It contains routing information for GPRS mobiles, which is used to tunnel packets through the IP based internal backbone to the correct Serving GPRS Support Node. The GGSN also collects charging information connected to the use of the external data networks and can act as a packet filter for incoming traffic.

Serving GPRS Support Node (SGSN)

The Serving GPRS Support Node is responsible for authentication of GPRS mobiles, registration of mobiles in the network, mobility management, and collecting information on charging for the use of the air interface.

Internal Backbone:

The internal backbone is an IP based network used to carry packets between different GSNs. Tunnelling is used between SGSNs and GGSNs, so the internal backbone does not need any information about domains outside the GPRS network. Signalling from a GSN to a MSC, HLR or EIR is done using SS7.

Routing Area:

GPRS introduces the concept of a Routing Area. This concept is similar to Location Area in GSM, except that it generally contains fewer cells. Because routing areas are smaller than location areas, less radio resources are used while broadcasting a page message.

3.18.4 GPRS Mobility Management:

The management of GPRS mobility in the network ensures the continuity of packet services when a given subscriber moves from one GPRS LA to another. This implies that the network must know the identifier of the GPRS LA indicating where the MS is located.

The GMM functions enable the network infrastructure to keep track of subscribers' locations within the PLMN or within another PLMN. The SGSN, which is the serving node of an MS, handles the mobility context management related to it. This context contains information such as the IMSI, the P_TMSI, the RAI, and the CI. This mobility context management is also stored at the MS side, in the SIM card. All GPRS mobility procedures require a TBF connection at the RLC/MAC layer between the MS and the PCU.

3.19 GPRS Procedure:

3.19.1 GPRS Attach Procedure:

When an MS needs to signal its presence to the network in order to access to GPRS services, it performs an IMSI attach procedure for GPRS services. During this procedure a MM context is created between the MS and the SGSN.

There are two types of GPRS attach procedures:

1. ***Normal GPRS attach.*** **This procedure is used by the MS to be IMSI attached for GPRS services only.**
2. ***Combined attach procedure.*** **This procedure is used by a class A or class B MS to be IMSI attached for GPRS and non-GPRS services in a cell that supports GPRS in network operation mode I.**

Note that by default, the IMSI-attach procedure is referred to as the *attach procedure for circuit- switched services.* The IMSI-attach procedure for GPRS services is also called the *GPRS-attach procedure.*

Normal GPRS Attach

Figure 3.9 describes a GPRS-attach procedure. In this scenario, the MS signals itself to the network by sending it its old P-TMSI identifier associated with the old RAI identifier. When the SGSN receives this information, it analyzes the RAI identifier in order to determine the associated SGSN. If there is an SGSN change, the new SGSN must contact the old SGSN from its RAI identifier in order to retrieve the MS identity. Authentication functions may be performed; they are mandatory if no MM context information related to the MS, such as IMSI, P-TMSI, CI, and RA exists anywhere in the network. Then the new SGSN informs the HLR of SGSN change, and location information in the HLR database is updated via the MAP protocol on SS7 signaling. If the HLR receives an indication from an SGSN different from the one stored in its table for a GPRS subscriber, it requests the old SGSN to remove GPRS data related to this subscriber, and then transmits this data to the new SGSN.

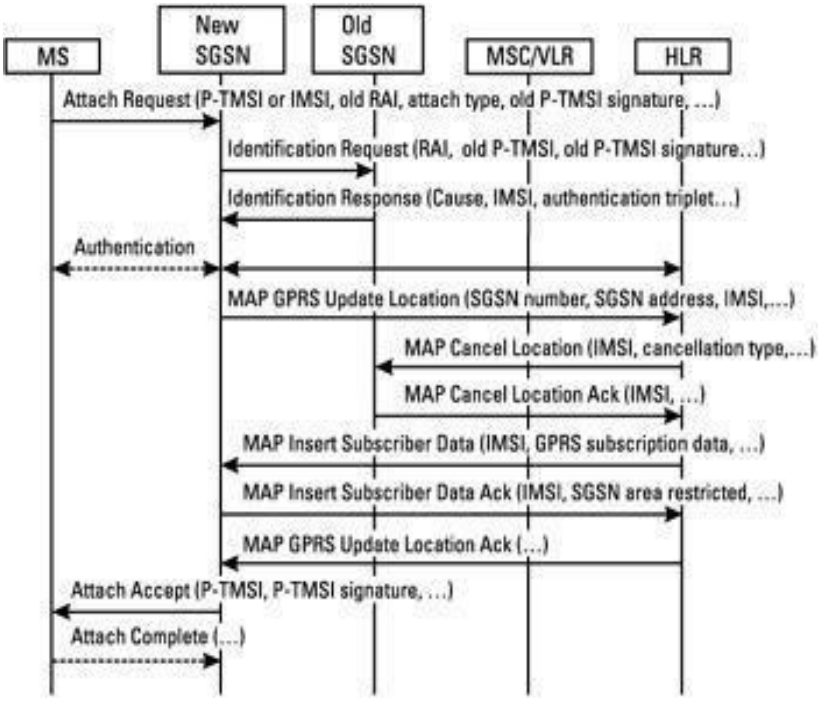


Fig 3.9 GPRS-attach procedure

3.19.2GPRS Detach Process:

When an MS does not need to access GPRS services anymore, an IMSI-detach procedure is initiated, either by the MS or by the SGSN. During this procedure, the MM context between the MS and the SGSN is removed.

There are two types of GPRS-detach procedures:

1. ***Normal GPRS detach.*** **This procedure is used to IMSI detach only for GPRS services.**
2. ***Combined detach procedure.*** **This procedure is used to IMSI detach a class A or B MS for GPRS or non-GPRS services in a cell that supports GPRS in network operation mode I.**

This procedure is initiated either by the MS or by the network

MS-Initiated Detach Procedure

MS-Initiated Normal *GPRS Detach* When a GPRS MS wishes to be IMSI detached for GPRS services, it initiates a GPRS-detach procedure to the SGSN. The procedure is ended upon the receipt of the DETACH *MS-Initiated Normal GPRS Detach* When a GPRS MS wishes to be IMSI detached for GPRS services, it initiates a GPRS-detach procedure to the SGSN. The

procedure is ended upon the receipt of the DETACH ACCEPT message by the MS, as illustrated in Figure 3.10

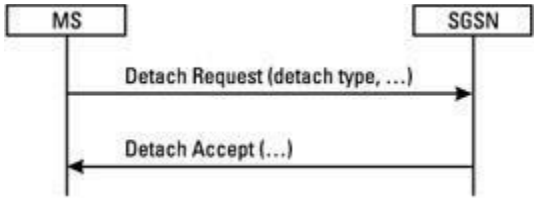


Figure 3.10: Normal GPRS detach initiated by MS.

MS-Initiated Combined GPRS Detach :When an MS both IMSI and GPRS attached wishes to perform a GPRS detach in a cell that supports GPRS in network operation mode I, it initiates a combined detach procedure to the SGSN. The latter sends an explicit request to the MSC/VLR to deactivate the association between SGSN and MSC/VLR in order that circuit-switched incoming calls are no longer routed to SGSN. Figure 3.11 illustrates this scenario. The same scenario is used for an MS both IMSI and GPRS attached wishing to be IMSI detached or both IMSI and GPRS detached in network operation mode I.

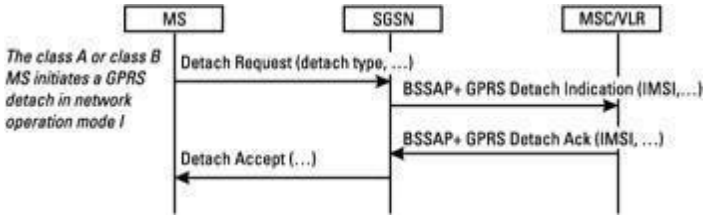


Fig 3.11: Combined GPRS detach initiated by an MS in network operation mode I.

3.19.3 Network-Initiated Detach Procedure

Network-Initiated Normal GPRS Detach **When an SGSN wishes to IMSI detach a given MS for GPRS services, it initiates a GPRS-detach procedure. The procedure is ended upon the receipt of DETACH ACCEPT message by the SGSN, as illustrated in Figure 3.12. The network may request the MS to perform a reattach in the case of a network failure condition.**

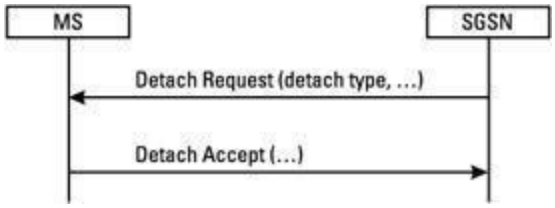


Figure 3.12: Normal GPRS detach initiated by an SGSN.

Network-Initiated Combined GPRS Detach When an SGSN wishes to IMSI detach a class A or B MS for GPRS or non-GPRS services, it notifies the relevant MS of a GPRS detach. It also sends an explicit request to MSC/VLR to deactivate the association between SGSN and MSC/VLR. Circuit-switched incoming calls are no longer routed to SGSN. Figure 3.13 illustrates this scenario.

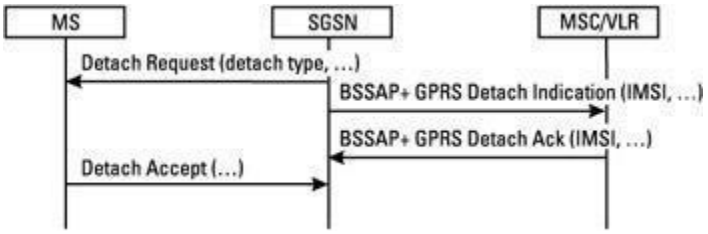


Figure 3.13: GPRS detach initiated by SGSN in network operation mode I.

An HLR may initiate a GPRS detach for operator purposes in order to remove the subscriber's MM and PDP contexts at the SGSN. The HLR sends a CANCEL LOCATION message in order to delete the subscriber's MM and PDP contexts from the SGSN. This latter then notifies the relevant MS of a GPRS detach. If the MS is both IMSI and GPRS attached, the SGSN sends an explicit request to the MSC/VLR to deactivate the association between the SGSN and the MSC/VLR. Figure 3.14 illustrates this scenario.

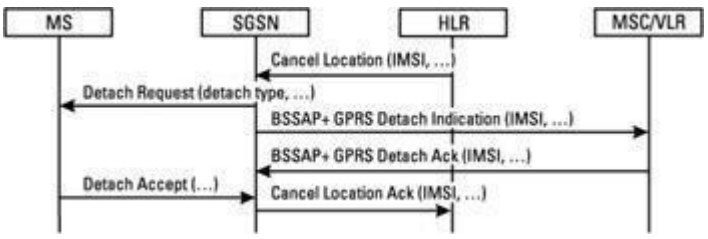


Figure 3.14: Combined GPRS detach initiated by HLR.

3.20 Location Procedures

A location procedure is always initiated by the MS. Under normal circumstances, a location change occurs when the MS decides to camp on a new cell for better radio conditions. If an MS in GMM READY state camps in a new cell within its current RA, it needs to perform a cell update procedure in order to receive directly downlink PDUs from the network without being paged. If the MS camps in a new cell belonging to a new RA, it needs to perform an RA update procedure in order to update MM context information between the MS and the SGSN.

Cell Update

When a GPRS MS in GMM READY state detects a new cell within its current RA, it performs a cell update procedure by sending any LLC frame containing its identity. Figure 3.15illustrates the cell update notification.

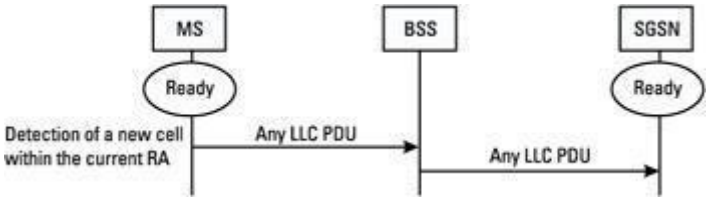


Figure 3.15: Cell update.

RA Update Procedure

An RA update procedure is performed when a GPRS MS has detected a new RA. This procedure is always initiated by the MS. There are four types of RA update procedures:

1. ***Normal RA update,* performed by a class C MS or by a class A or B MS in a cell that supports GPRS in network operation mode II or III upon detection of a new RA;**
2. ***Periodic RA,* performed by any GPRS MS upon expiry of a timer;**
3. ***Combined RA and LA update,* performed by a class A or B MS in a cell that supports GPRS in network operation mode I upon detection of a new LA;**

4. ***Combined RA and IMSI attach,*** **performed by a class A or B MS in a cell that supports GPRS in network operation mode 1 in order to be IMSI attached for non-GPRS services when the MS is already IMSI attached for GPRS services.**

Normal RA Update

Intra-SGSN HA Update During an RA update procedure, the MS signals itself to the SGSN by sending its old P-TMSI signature associated with the RAI identifier from its old RA. The SGSN has the necessary information about the MS if the SGSN also handles the old RA.

In the case of an intra-SGSN change, the SGSN validates the presence of the MS in the new RA by returning to it a ROUTING AREA UPDATE ACCEPT message. If the SGSN allocates a new P-TMSI identifier, it is acknowledged by the MS. This procedure is called intra-SGSN RA update since the SGSN does not need to contact an old SGSN, GGSN, and HLR. Figure 3.16 illustrates an intra-SGSN RA update procedure.

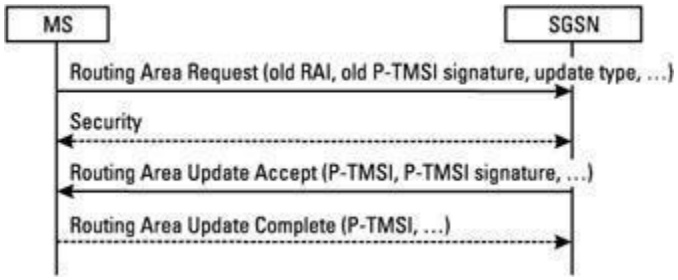


Figure 3.16: Intra-SGSN RA update.

Note that a periodic RA update is always an intra-SGSN RA update procedure.

Inter-SGSN RA Update When the SGSN detects that the old RA sent by the MS is handled by another SGSN, the SGSN has no information about this MS. In this case, the SGSN needs to contact the old SGSN, the GGSN, and the HLR in order to retrieve information and update the routing information. This procedure is called an inter-SGSN RA update procedure. Thus the new SGSN is able to contact the old SGSN from the RAI identifier in order to retrieve MM and PDP context information related to the MS identified in the old SGSN by its old P-TMSI. If the old signature does not match the one saved in the old SGSN, the new SGSN performs an MS authentication procedure. If the old SGSN has saved in its buffer some packets addressed to the MS, it forwards the packets toward the new SGSN.

When the new SGSN has retrieved MM and PDP context information, it updates the data related to the new SGSN in the GGSN. The new SGSN then updates location information

in the

HLR database via the MAP protocol using the SS7 network. If the HLR receives an indication from an SGSN different from the one saved in its table for a GPRS subscriber, it requests the old SGSN to remove GPRS data related to this subscriber. It then transmits this data to the new SGSN. As shown in Figure 3.17 when the new SGSN receives an RA update confirmation in the HLR database, it transmits the RA update confirmation to the MS with its new P-TMSI identifier and the receive N-PDU number. This message contains the acknowledgment of N-PDUs successfully transferred by the MS before the start of the update procedure. The RA update procedure ends as soon as the MS acknowledges its new P-TMSI identifier.

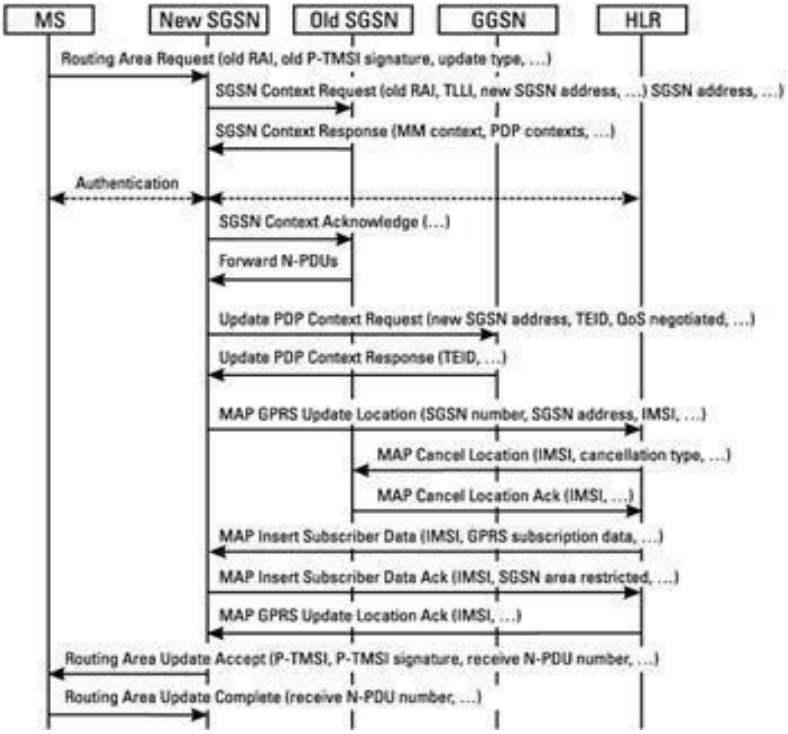


Figure 3.17: Inter-SGSN RA update.

3.21 Combined RA and LA Update:

During a combined RA and LA update procedure in a cell that supports GPRS in network operation mode I, the new SGSN (in case of SGSN change) retrieves MM and PDP context information related to the MS from the old SGSN. The new SGSN sends its address to the GGSN, updates routing information in the HLR via the MAP protocol, and retrieves data related to the GPRS subscriber from the HLR. The new SGSN transmits an LA update request via the Gs interface.

If the LA change involves a new MSC/VLR entity, the new MSC/VLR updates the location information in the HLR via the MAP protocol. When the HLR receives a notification from an MSC/VLR different from the one saved in its table, it requests the old MSC/VLR to remove data related to the GPRS subscriber and then transmits this data to the new MSC/VLR data. When the new SGSN receives the LA update confirmation from the new MSC/VLR with the allocation of a new TMSI identifier value, it transmits the confirmation of the combined RA and LA update message toward the MS.

The new SGSN allocates a new P-TMSI identifier for packet services and also returns the receive N-PDU number, containing the acknowledgment of N- PDUs successfully transferred by the MS before the start of the combined procedure. The combined RA and LA update procedure ends as soon as the MS acknowledges its new TMSI and P-TMSI identifiers. Figure 3.18 illustrates the combined RA and LA update procedure. Note that the combined RA and IMSI attach scenario generates the same message exchange between the MS, SGSN, GGSN, MSC/VLR, and HLR
entities as the combined RA and LA update scenario.

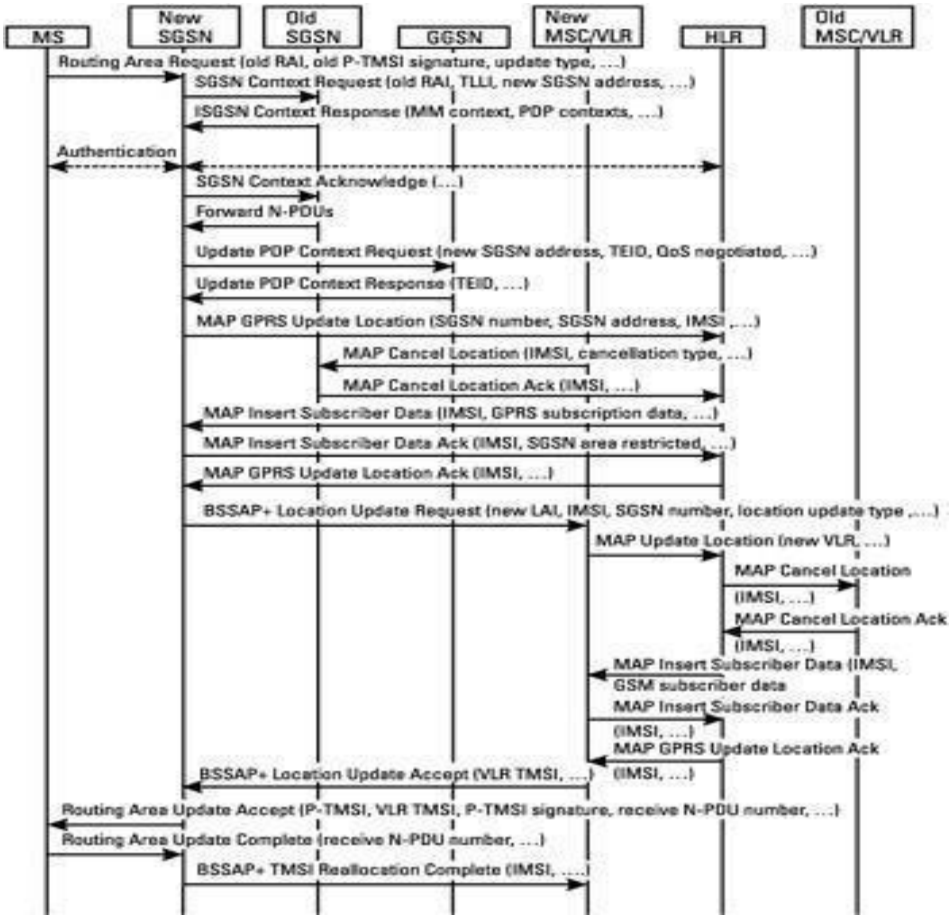


Figure 3.18: Combined RA and LA update procedure.

.

3.22 PDP Context Procedure:

PDP stands for Packet Data Protocol as shown in fig 3.19. The PDP addresses are network layer addresses (Open Standards Interconnect [OSI] model Layer 3). GPRS systems support both X2.5 and IP network layer protocols. Therefore, PDP addresses can be X.25, IP, or both. Each PDP address is anchored at a Gateway GPRS Support Node (GGSN), as shown in figure below. All packet data traffic sent from the public packet data network for the PDP address goes through the gateway (GGSN).

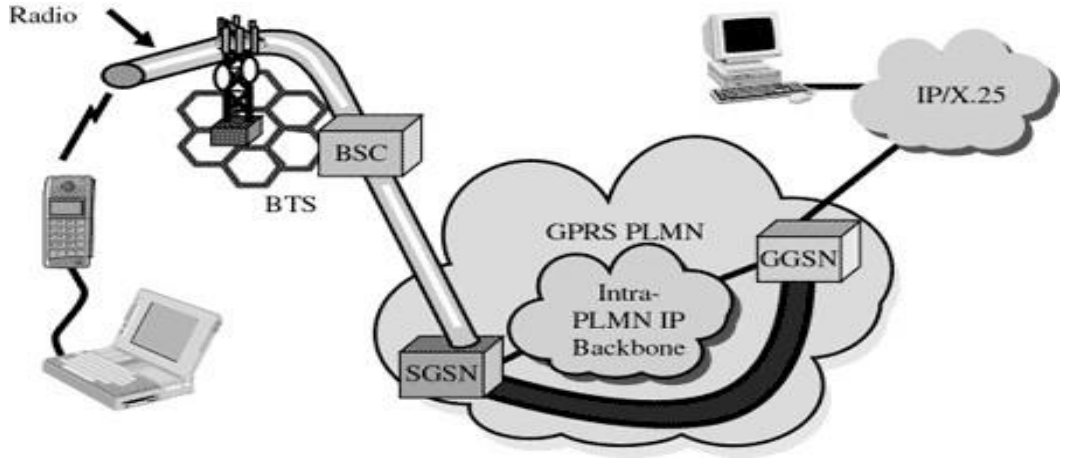


Fig 3.19 Packet Data Protocol

The public packet data network is only concerned that the address belongs to a specific GGSN. The GGSN hides the mobility of the station from the rest of the packet data network and from computers connected to the public packet data network. Statically assigned PDP addresses are usually anchored at a GGSN in the subscriber's home network. Conversely, dynamically assigned PDP addresses can be anchored either in the subscriber's home network or the network that the user is visiting. When a MS is already attached to a SGSN and it is about to transfer data, it must activate a PDP address. Activating a PDP address establishes an association between the current SGSN of mobile device and the GGSN that anchors the PDP address.

The record kept by the SGSN and the GGSN regarding this association is called the PDP context. It is important to understand the difference between a MS attaching to a SGSN and a MS activating a PDP address. A single MS attaches to only one SGSN, however, it may have multiple PDP addresses that are all active at the same time. Each of the addresses may be anchored to a different GGSN. If packets arrive from the public packet data network at a GGSN for a specific PDP address and the GGSN does not have an active PDP context corresponding to that address, it may simply discard the packets. Conversely, the GGSN may attempt to activate a PDP context with a MS if the address is statically assigned to a particular mobile device.

3.23 GPRS Billing:

As packet data is introduced into mobile systems, the question of how to bill for the services arises. Always online and paying by the minute does not sound all that appealing. Here, we describe the possibilities but it totally depends on different service providers, how they want to charge their customers.

The SGSN and GGSN register all possible aspects of a GPRS user's behavior and generate billing information accordingly. This information is gathered in so-called

Charging Data Records (CDR) and is delivered to a billing gateway.

The GPRS service charging can be based on the following parameters:

- **Volume - The amount of bytes transferred, i.e., downloaded and uploaded.**
- **Duration - The duration of a PDP context session.**
- **Time - Date, time of day, and day of the week (enabling lower tariffs at offpeak hours).**
- **Final destination - A subscriber could be charged for access to the specific network, such as through a proxy server.**
- **Location - The current location of the subscriber.**
- **Quality of Service - Pay more for higher network priority.**
- **SMS - The SGSN will produce specific CDRs for SMS.**
- **Served IMSI/subscriber - Different subscriber classes (different tariffs for frequent users, businesses, or private users).**
- **Reverse charging - The receiving subscriber is not charged for the received data; instead, the sending party is charged.**
- **Free of charge - Specified data to be free of charge.**
- **Flat rate - A fixed monthly fee.**
- **Bearer service - Charging based on different bearer services (for an operator who has several networks, such as GSM900 and GSM1800, and who wants to promote usage of one of the networks). Or, perhaps the bearer service would be good for areas where it would be cheaper for the operator to offer services from a wireless LAN rather than from the GSM network.**

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF ELECTRICAL AND ELECTRONICS

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

UNIT IV-MOBILE NETWORK AND TRANSPORT LAYERS-SEC1614

UNIT-IV

4.1.Mobile IP:

It is a correspondence convention (made by expanding Internet Protocol, IP) that permits the clients to move starting with one system then onto the next with a similar IP address. It guarantees that the correspondence will proceed without client's meetings or associations being dropped.

- **Mobile Node (MN):**
  It is the hand-held communication device that the user caries e.g. Cell phone.
- **Home Network:**
  It is a network to which the mobile node originally belongs to as per its assigned IP address (home address).
- **Home Agent (HA):**
  It is a router in home network to which the mobile node was originally connected
- **Home Address:**
  It is the permanent IP address assigned to the mobile node (within its home network).
- **Foreign Network:**
  It is the current network to which the mobile node is visiting (away from its home network).
- **Foreign Agent (FA):**
  It is a router in foreign network to which mobile node is currently connected. The packets from the home agent are sent to the foreign agent which delivers it to the mobile node.
- **Correspondent Node (CN):**
  It is a device on the internet communicating to the mobile node.
- **Care of Address (COA):**
  It is the temporary address used by a mobile node while it is moving away from its home network.

4.1.1. Working:

Correspondent node sends the data to the mobile node. Data packets

contains correspondent node's address (Source) and home address (Destination). Packets reaches to the home agent. But now mobile node is not in the home network, it has moved into the foreign network. Foreign agent sends the care-of-address to the home agent to which all the packets should be sent. Now, a tunnel will be established between the home agent and the foreign agent by the process of tunneling.

Tunneling - establishes a virtual pipe for the packets available between a tunnel entry and an endpoint. It is the process of sending a packet via a tunnel and it is achieved by a mechanism called encapsulation. Now, home agent encapsulates the data packets into new packets in which the source address is the home address and destination is the care-of-address and sends it through the tunnel to the foreign agent. Foreign agent, on other side of the tunnel receives the data packets, decapsulates them and sends them to the mobile node. Mobile node in response to the data packets received, sends a reply in response to foreign agent. Foreign agent directly sends the reply to the correspondent node.

4.1.2.Key Mechanisms in Mobile IP:

1. **Agent Discovery:**

   Agents advertise their presence by periodically broadcasting their agent advertisement messages. The mobile node receiving the agent advertisement messages observes whether the message is from its own home agent and determines whether it is in the home network or foreign network.

2. **Agent Registration:**

   Mobile node after discovering the foreign agent, sends registration request (RREQ) to the foreign agent. Foreign agent in turn, sends the registration request to the home agent with the care-of-address. Home agent sends registration reply (RREP) to the foreign agent. Then it forwards the registration reply to the mobile node and completes the process of registration.

3. **Tunneling**

   It establishes a virtual pipe for the packets available between a tunnel entry and

an end point. It is the process of sending a packet via a tunnel and it is achieved by a mechanism called encapsulation. It takes place to forward an IP datagram from the home agent to the care-of-address. Whenever home agent receives a packet from correspondent node, it encapsulates the packet with source address as home address and destination ascare-of-address.

4.2.Route Optimization:

The route optimization adds a conceptual data structure, the binding cache, to the correspondent node. The binding cache contains bindings for mobile node's home address and its current care-of-address. Every time the home agent receives a IP datagram that is destined to a mobile node currently away from the home network, it sends a binding update to the correspondent node to update the information in the correspondent node's binding cache. After this the correspondent node can directly tunnel packets to the mobile node.

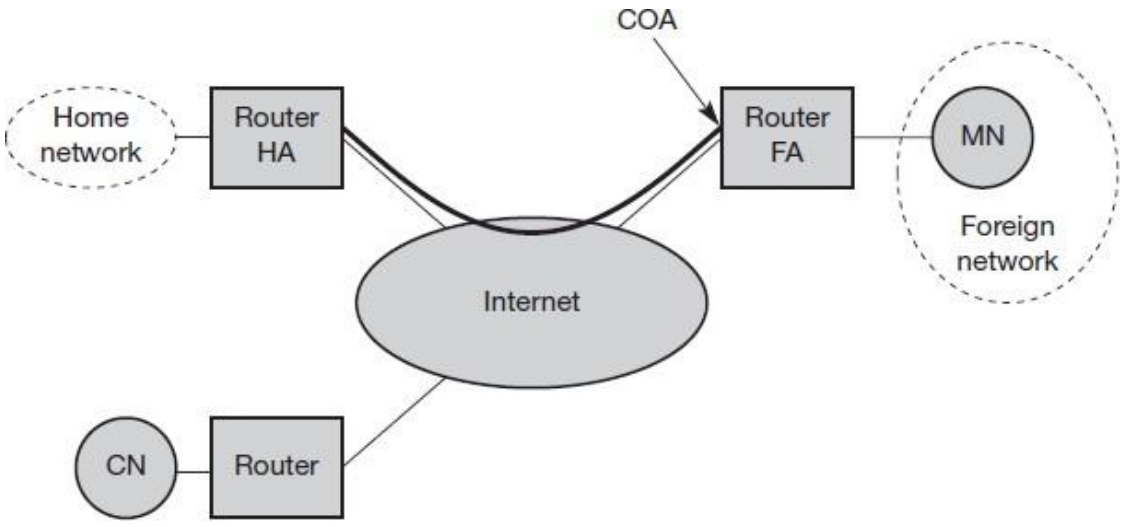


Figure 4.1 Mobile IP

4.3.Dynamic host configuration protocol

The dynamic host configuration protocol is used to simplify the installation and maintenance of networked computers. If a node is connected to a network, DHCP provides full system integration into the network, like addresses of a DNS server ,the default router, subnet mask, domain name, & IP address. DHCP is based on a client-server model as shown in Figure 4.2 given below. DHCP clients send a request to a server for which the server responds. A client sends requests using MAC broadcasts to reach all other devices connected in the network.

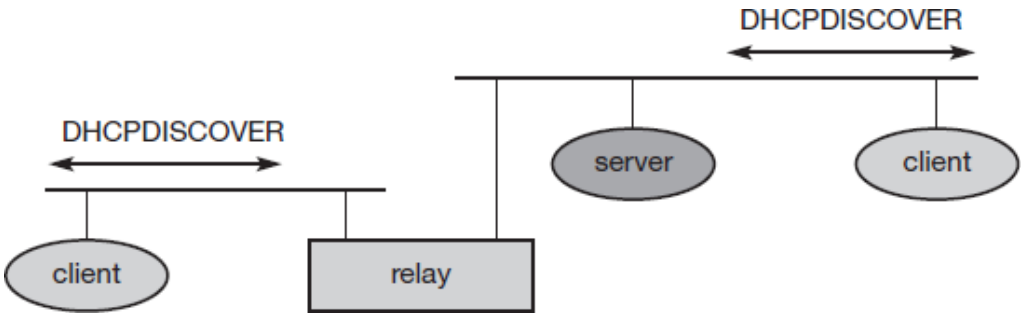


Figure 4.2 Basic DHCP Configurations

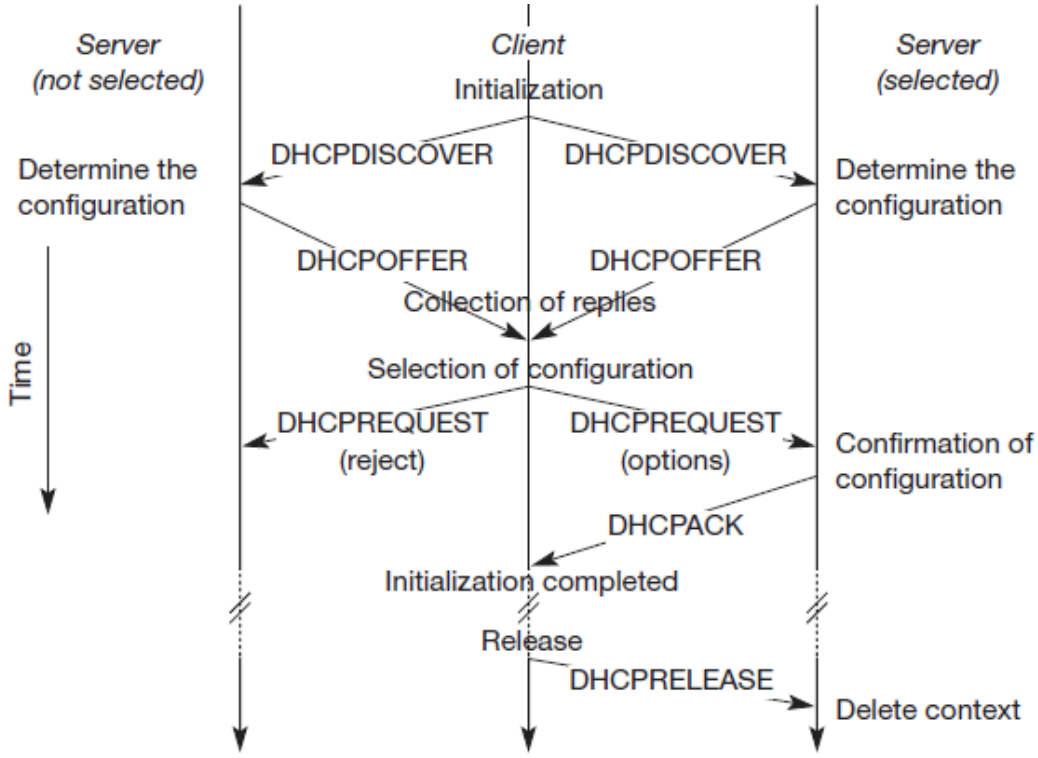


Figure 4.3 Client initialization

DHCP client initialization is shown in figure 4.3.It has one client and two servers. The client broadcasts a DHCPDISCOVER .In the figure shown above , two servers receive this broadcast and determine the configuration they can offer to the client. Servers reply to the client's request with DHCPOFFER and offer a list of configuration parameters. The client can now choose one of the configurations offered. The client in turn replies to the servers, accepting one of the configurations and rejecting the others using DHCPREQUEST. If a server receives a DHCPREQUEST with a rejection, it can free the reserved configuration for other possible clients. The server with the configuration accepted by the client now confirms the configuration with DHCPACK. This completes the initialization phase. If a client leaves a subnet, it should release the configuration received by the server using DHCPRELEASE. Now the server can free the context stored for the client and offer the configuration again. The configuration a client gets from a server is only leased for a certain amount of time, it has to be reconfirmed from time to time.

4.4.MOBILE ADHOC Routing:

***Pro-active routing protocols:**

It is also Called as table-driven routing protocols. Each mobile node maintains a separate routing table which contains the information of the routes to all the possible destination mobile nodes.

***Reactive routing protocols:**

Also known as on-demand routing protocol. The route is discovered only when it is required. The process of route discovery occurs by flooding the route request packets throughout the mobile network. It consists of two major phases namely, route discovery and route maintenance.

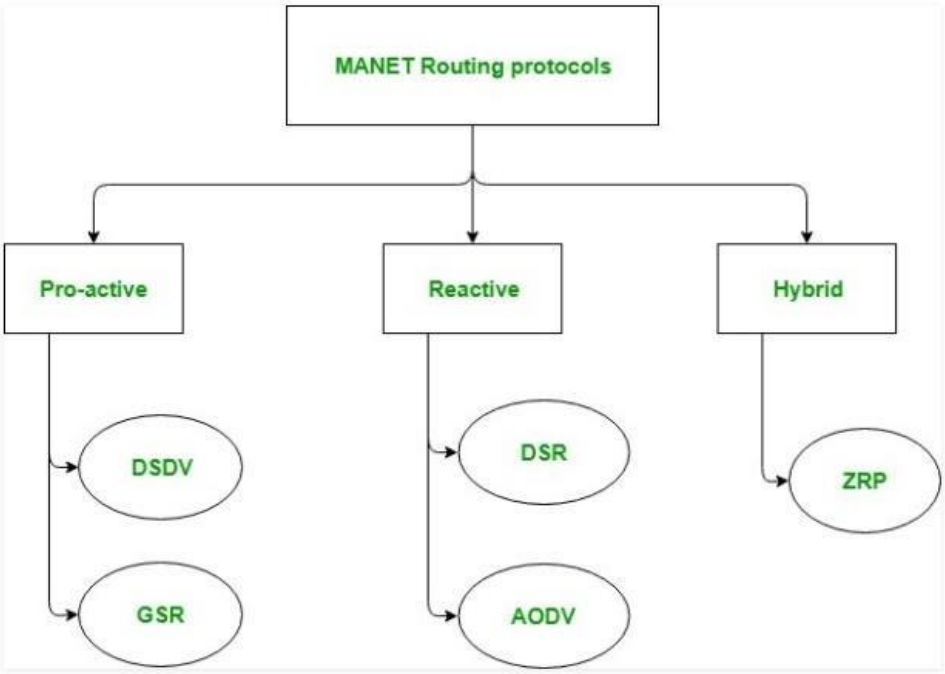


Figure 4.4 Adhoc routing protocols

***Hybrid routing protocol:**

Have the advantages of both, reactive and pro-active routing protocols. These protocols are adaptive in nature and adapts according to the zone and position of the source and destination mobile nodes. One of the most popular hybrid routing protocol is Zone Routing Protocol (ZRP).

4.5.Distance Sequence Distance Vector(DSDV):

- **Distance Sequence Distance Vector (DSDV) routing is an enhancement to distance vector routing for ad-hoc networks.**
- **Distance Vector Routing is used as routing information protocol (RIP) in wired networks.**
- **It performs extremely poorly with certain network changes due to the count-to-infinity problem.**
- **Each node exchanges its neighbor table periodically with its neighbors**
- **Changes at one node in the network propagate slowly through the network (step-by-step with every exchange).**

4.5.1.DSDV adds two things to AODV algorithm.

Sequence Numbers :-

- **Each routing advertisement comes with a sequence number. Within ad-hoc networks advertisements may propagate along many paths.**
- **Sequence numbers help to apply the advertisements in correct order.**
- **This avoids the loops that are likely with the unchanged distance vector algorithm.**

Damping :-

- **Transient changes in topology that are of short duration should not destabilize the routing mechanism.**
- **Advertisements containing changes in the topology currently stored.**
- **A node waits with dissemination if these changes are probably unstable. Waiting time depends in the time between the first the first and the best announcement of a path to a certain destination.**

4.6. DYNAMIC SOURCE ROUTING (DSR):

Dynamic Source Routing (DSR) divides the task of routing into two separate problems

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 currently no known route.**
2. **Route Maintenance:-If a node is continuously sending packets via a route it has to make sure that the route is held upright. As soon as a node detects problems with the current route it has to find an alternative.**

Algorithm:- The basic algorithm for route discovery each route request could contain a counter.

- **Every node rebroadcasting the request increments the counter by one.**
- **Knowing the maximum network diameter nodes can drop a request if the counter reaches this number.**
- **A node can cache path fragments from recent requests.**
- **These fragments can now be used to answer other route requests much faster.**
- **A node can also update this cache from packet headers while forwarding other packet**
- **If a node over heads transmission from other nodes it can also use this information for shortening routes**
- **After a route has been discovered it has to be maintained for as long as the node sends packets along this route. Depending on layer two mechanisms different approaches can betaken**
- **If the link layer uses an acknowledgement the node can interpret this acknowledgement as an intactroute.**
- **If possible the node could also listen to the next node forwarding the packet so getting a passive acknowledgement.**
- **A node could request an explicit acknowledgement.**

4.7. Zone routing protocol (ZRP):

This protocols uses a combination of proactive and reactive routing protocols: • proactive: in the neighborhood of r hops, reactive: outside this zone.

The protocol operates as follows:

- **if the destination is within the zone, the source sends packets directly;**
- **if not, the destination sends Route Request to peripheral nodes;**
- **if any peripheral node, has the destination in its zone it replies with Route Reply;**
- **if not, peripheral nodes sends Route Request to their peripheral nodes and so on;**
- **if multiple Route Reply are received the best is chosen based on somemetric.**

If the broken link is detected:

- **intermediate node repairs the link locally bypassing it (proactive routing);**
- **end nodes are informed;**
- **sub-optimal pass but very quick procedure;**
- **after several local reconfiguration, the source initiates global pass finding to find optimal.**

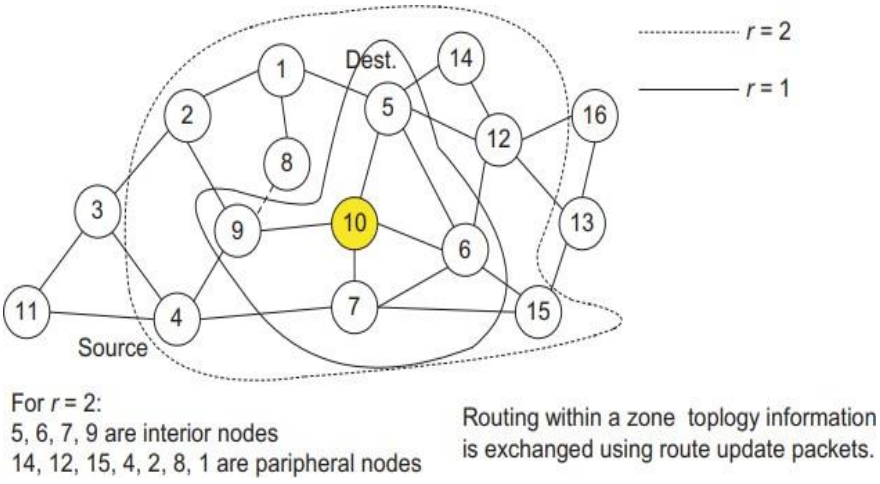


Figure 4.5 ZRP routing protocols

4.8 Transmission Control Protocol

4.8.1.Indirect TCP or I-TCP:

Segments a TCP connection into a fixed and a wireless part

- **Wireless Part a Mobile Host connected via a wireless link and a Access Point to the Wired ,Internet where the correspondent node resides.**
- **Standard TCP is used between the fixed computer and the Access Point.**

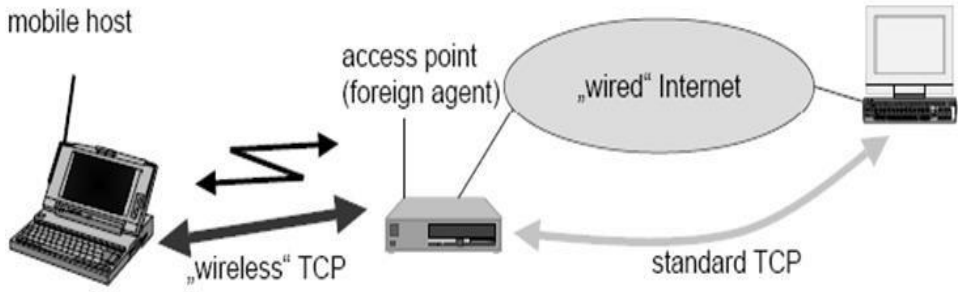


Figure 4.6 TCP Architecture

Between the Access Point and the Mobile host a special TCP adapted to wireless links .Segmenting the connection between Mobile Host and Correspondent Host is at the foreign agent of mobile IP. The foreign agent controls the mobility of the mobile host and can also handover the connection to the next foreign agent when the mobile host moves on.

The Correspondent Host in the fixed network does not notice the wireless link or the segmentation of the connection. The Foreign agent acts as a proxy and relays all data in both directions. If the Correspondent host send a packet the Foreign agent acknowledges this packet and tries to forward the packet to the Mobile Host. If the MH receives the packet it acknowledges the packet. This acknowledgement is used by the Mobile Host If a packet is lost on the wireless link due to a transmission error the correspondent host would not notice this. The foreign agent tries to retransmit this packet locally to maintain reliable data transport.

4.8.2.Snooping TCP

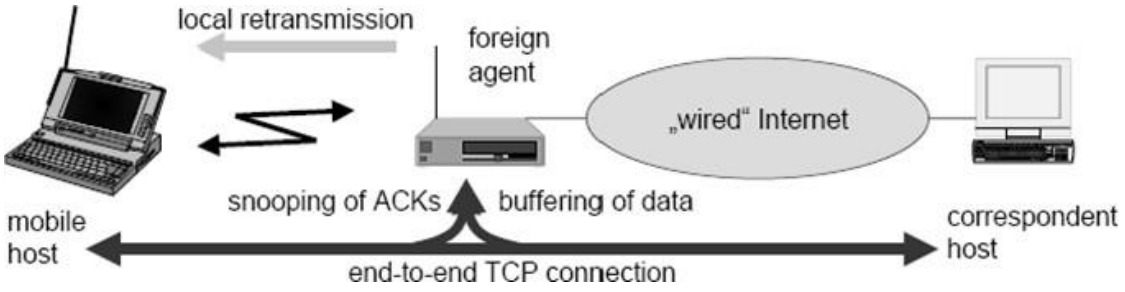


Figure 4.7 Snooping TCP

The foreign agent buffers all packets with Destination mobile host. Additionally 'snoops' the packet flow in both directions to recognize acknowledgements. The reason for buffering the packets toward the mobile node is to enable the foreign agent to perform a local transmission in case of packet loss on the wireless link. The foreign agent buffers every packet until it receives an acknowledgement from the mobile host. If the foreign agent does not receive an acknowledgement from the mobile host within a certain amount of time either the packet or the acknowledgement has been lost. Alternatively the foreign agent could receive a duplicate ACK which also shows the loss of a packet.Now the foreign agent Retransmits the packet directly from the buffer. Performing a much faster retransmission compared to the correspondent host. The time out for acknowledgements can be much shorter because it reflects only the delay of one hop plus processing time. To remain transparent the foreign agent must not acknowledge data to the correspondent host. The correspondent host believe that the mobile host had received the data would violate the end-to end semantic in case of a foreign agent failure.

The foreign agent can filter the duplicate acknowledgements to avoid unnecessary retransmissions of data from the correspondent host. If the foreign agent now crashes the time-out of the correspondent host still works and triggers a retransmission. The foreign agent may discard duplicates of packets already retransmitted locally and acknowledged by the mobile host. This avoids unnecessary traffic on the wireless link,

Advantages:

- **The end-to-end TCP semantic is preserved. No matter that the foreign agent crashes.**
- **The correspondent host does not need to be changed.**
- **Most of the enhancements are in the foreign agent.**
- **Supporting only the foreign stream from the correspondent host to the mobile host does not even require changes in the mobile host.**
- **It does not need a handover of state as soon as the mobile host moves to another foreign agent.**
- **It does not matter if the next foreign agent uses the enhancement or not. If not the approach automatically falls back to the standard solution.**

Disadvantages:

- **Snooping TCP does not isolate the behavior of the wireless link as well asI-TCP.**
- **Using negative acknowledgements between the foreign agent and the mobile host assumes additional mechanisms on the mobile host.**
- **All efforts for snooping and buffering data may be useless if certain encryption schemes are applied.**
- **Using IP encapsulation security payload the TCP protocol header will be encrypted -> snooping the sequence number will no longer work.**

4.8.3.Mobile TCP

The M-TCP (Mobile TCP) approach has the same goals as Indirect TCP & Snooping TCP,

- **To prevent the sender window from shrinking if bit errors or disconnection but not congestion cause current problems.**
- **M-TCP splits the TCP connection into 2 parts,**
- **An unmodified TCP is used on the standard host-supervisory host(SH)connection. While an optimized TCP is used on the SH_MH connection. The supervisory host is responsible for exchanging data between both parts similar to the**
- **proxy in I-TCP.**

- **The M-TCP approach assumes a relatively low bit error rate on the wireless link. Therefore it does not perform caching / retransmission of data via the SH.**
- **If a packet is lost on the wireless link it has to be retransmitted by the original sender. This maintains the TCP end-to-end semantics.**
- **The SH monitors all packets sent to the MH and ACKs returned from the MH**
- **If the SH does not receive an ACK for some time, it assumes that the MH is disconnected.**
- **It then chokes the sender by setting the sender's window size to0.**
- **Setting the window size = 0 ---> forces the sender to go into persistent mode.**
- **As soon as the SH detects connectivity again it reopens the window of the sender to the old value.**
- **The sender can continue sending at full speed. This mechanism does not require changes to the sender's TCP.**
- **The wireless side uses an adapted TCP that can recover from packet loss much**
- **faster.**
- **This modified TCP does not uses low start thus M-TCP needs a Bandwidth**
- **Manager to implement fair sharing over the wireless link.**

Advantages:

- **It maintains the TCP end-to-end semantics. The SH does not send any ACK itself but forwards the ACKs from the MH.**
- **If the MH is disconnected it**

➢ **Avoids useless retransmissions slow starter.**

➢ **Breaking connections by simply shrinking the sender's window to zero.**

Disadvantages:

- **The SH does not act as proxy as in I-TCP packet loss on the wireless link due to bit errors is propagated to the sender.**
- **M-TCP assumes a low bit error rate which is not always a valid assumption.**

4.8.4.Fast Retransmit / Fast Recovery

- **The mechanisms of fast recovery / fast retransmit a host can use after receiving duplicate acknowledgements thus concluding a packet without congestion.**

- **Retransmit behavior on mobile host & correspondent host.As soon as the mobile host registers at a new foreign agent using mobile IP it starts sending duplicated acknowledgements to correspondent hosts.**

- **The proposal is to send three duplicates. This forces the correspondent host to go into fast retransmit mode and not to slow start**

  The correspondent host continues to send with the same rate it did before the mobile host moved to another foreign agent.

- **As the mobile host may also go into slow start after moving to a new foreign agent this approach additionally puts the mobile host into fast retransmit.**
- **The mobile host retransmits all unacknowledged packets using the current congestion window size without going into slow start.**

Advantages:

- **This approach is simple**
- **Only minor changes in the mobile hosts software already result in a performance increase.**
- **No foreign agent or correspondent host has to be changed.**

Disadvantages:

- **This scheme is the insufficient isolation of packet losses.**
- **Forcing fast retransmission increases the efficiency but retransmitted packets still have to cross the whole network between correspondent host and mobile host.**
- **If the handover from one foreign agent to another takes a longer time, the correspondent host will have already started retransmission.**

4.8.5.Transmission / Time-Out Freezing

The approach so far can handle short interruptions of the connection either due to

- **Handover &**

- **Transmission errors on the wireless link**

Some were designed for longer interruptions of transmission.

- **The MAC layers has already noticed connection problems before the connection is actually interrupted from a TCP point of view. Additionally MAC layer knows the reason for the interruption is not caused congestion.**
- **TCP can now stop sending and freezes the current state of its congestion window and further timers.**
- **If the MAC layers notices the upcoming interruption early enough both the mobile and correspondent host can be informed.**
- **With a fast interruption of the wireless link additional mechanisms in the access point needed to inform the correspondent host of the reason for interruption.**
- **Otherwise the correspondent host goes into the slow start assuming congestion and finally breaks the connection.**
- **As soon as the MAC layer detects connectivity again it signals TCP that it can resume operation at exactly the same point where it had been forced to stop.**
- **Advantages:**
- **This approach offers a way to resume TCP connections even after longer interruptions of the connection.**
- **It is independent of any other TCP mechanisms such as acknowledgements or sequence numbers so it can be used together with encrypted data.**
- **Disadvantages:**
- **The software on the mobile host has to be changed to be more effective the correspondent host cannot remain unchanged.**
- **All mechanisms rely on the capability of the MAC layer to detect future interruptions. Freezing state of TCP does not help in case of some encryption schemes that use time- dependent random numbers.**
- **These schemes need resynchronization after interruption.**

4.8.6.Selective Retransmission

- **A very useful extension of TCP is the use of selective retransmission**
- **TCP acknowledgements are cumulative they acknowledge in-order receipt of packets up to a certain packet.**
- **If a single packet is lost the sender has to retransmit everything starting from the lost packet - Go-Back-n Retransmission.**
- **This obviously wastes bandwidth not just in the case of a mobile network but for any network.**
- **TCP can indirectly request a selective retransmission ofpackets.**
- **The receiver can acknowledge single packets not only trains of in-sequence packets.**
- **The sender can now determine precisely which packet is needed and can retransmit it.**

Advantage:

- **A sender retransmits only the lost packets.**
- **This lower bandwidth requirements and is extremely helpful in slow wireless links.**
- **The gain in efficiency is not restricted to wireless links and mobile environments.**
- **Using selective retransmission is also beneficial in all other networks.**

Disadvantage

- **While memory sizes and CPU performance permanently increase the bandwidth of the air interface remains almost the same.**
- **The higher complexity is no real disadvantage any longer as it was in the early days of TCP.**
- **More complex software on the receiver side because now more buffer is necessary to resequence data and to wait for gaps to be filled.**

Transaction-Oriented TCP

- **If the application requires reliable transport of the packets it may use TCP. Using TCP requires packets over the wireless link.**
- **TCP uses a three-way handshake to establish the connection.**
- **At least one additional packet is usually needed for transmission of the request&**

- **Requires three more packets to close the connection via a three-way handshake.**
- **Assuming connections with a lot of traffic or with a long duration this overhead is minimal.**

Advantage & Disadvantages:

- **For certain applications is the reduction in the overhead which standard TCP is not the original TCP anymore so it requires changes in the mobile host and all the correspondent hosts.**

This is a major disadvantage.

- **An additional scheme that can be used to reduce TCP overhead is header compression.**
- **Using tunneling schemes as in mobile IPtogether with TCP header remain unchanged for every packet.**
- **Header compression experiences difficulties when error rates are high due to the loss of the common context between sender and receiver.**

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF ELECTRICAL AND ELECTRONICS

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

UNIT – V - APPLICATION LAYER – SEC1614

V. APPLICATION LAYER

5.1 Wireless Application Protocol (WAP)

- **WAP is an application protocol is used to access services and information.**
- **The basic aim of WAP is to deliver Internet content and enhanced services to mobile devices and users (mobile phones, PDAs) independence from wireless network standards**

5.2 WAP - scope of standardization

- **Browser - "micro browser", similar to existing, well-known browsers in the Internet**
- **Script language - similar to Java script, adapted to the mobile environment**
- **WTA/WTAI -Wireless Telephony Application (Interface): access to all telephone functions**
- **Content formats -e.g., business cards (vCard), calendar events (vCalender)**
- **Protocol layers - transport layer, security layer, session layer etc.**
- **A WAP handset communicates to the origin server through the mobile network.**
- **The origin server is standard HTTP server /web server**

5.3 The WAP Architecture

i) **The user selects an option on their mobile device that has a URL with WML content assigned to it.**

ii) **The phone sends the URL request via the phone network to a WAP gateway, using the Binary encoded WAP protocol.**

iii) **The gateway translates this WAP request into a conventional HTTP request for the specified URL, and sends it on to the Internet.**

iv) **The appropriate Web server picks up the HTTP request.**

v) **The server processes the request, just as it would be any other request. If the**

URL refers to a static WML file, the server delivers it. If a CGI script is requested, it is processed and the content returned as usual.

vi) **The Web server adds the HTTP header to the WML content and returns it to the gateway.**

vii) **The WAP gateway compiles the WML into binary form.**

viii) **The gateway then sends the WML response back to the phone.**

ix) **The phone receives the WML via the WAP protocol.**

x) **The micro-browser processes the WML and displays the content on the screen.**

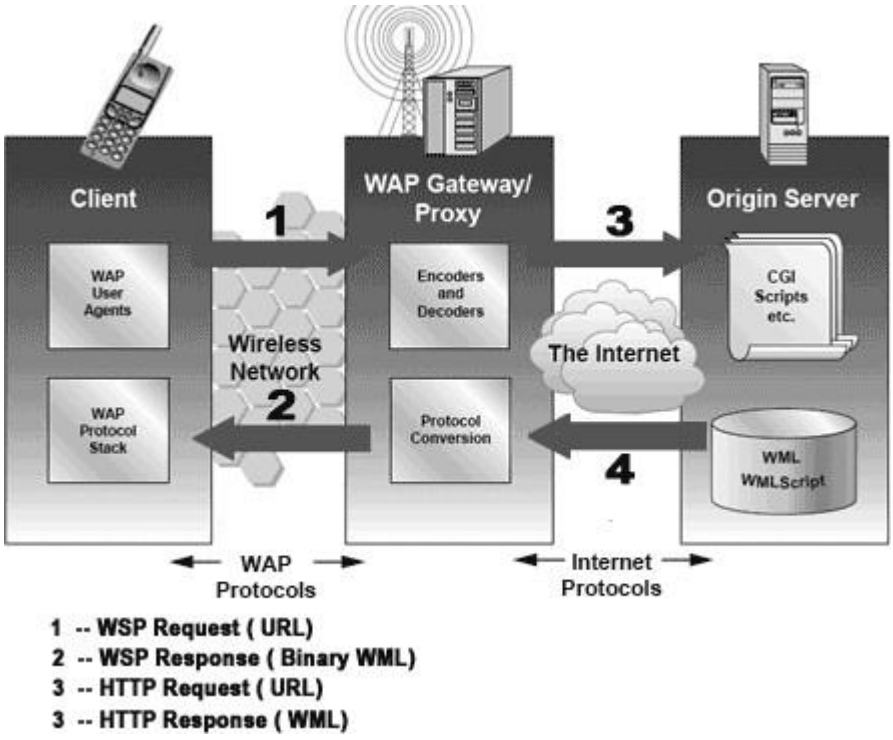


Figure 5.1 WAP Architecture

WAP specifies architecture based on layers that follow the OSI model fairly closely. The WAP model, orstack as it is commonly known, is illustrated below in Figure.

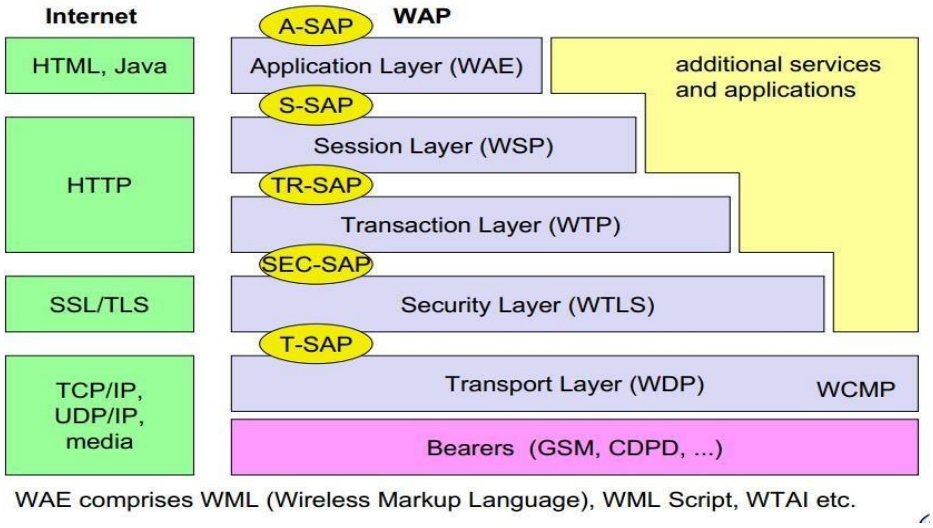


Figure 5.2 WAP Layers

5.4 WAP Protocol stack:

1. **Application Layer:**

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

2. **Session Layer:**

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

3. **Transaction Layer:**

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

4. **Security Layer:**

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

5. **Transport Layer:**

   This layer contains *Wireless Datagram Protocol*. It presents consistent data format to higher layers of WAP protocol stack.

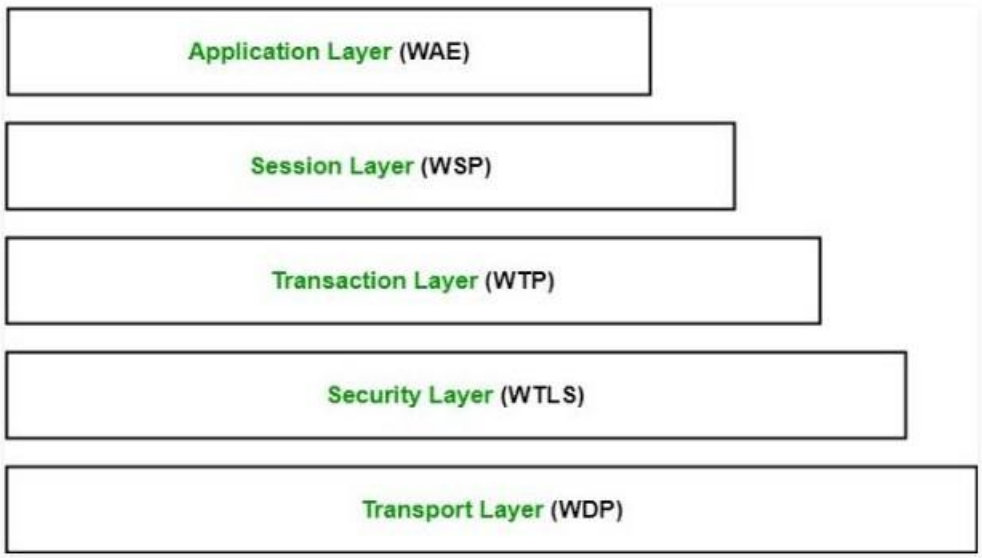


Figure 5.3 WAP Stack

5.5 Wireless Markup language (WML)

WML follows a deck and card metaphor. A WML document is made up of multiple cards. Cards can be grouped together into a deck. A WML deck is similar to an HTML page, in that it is identified by a URL and is the unit of content transmission. A user navigates with the WML browser through a series of WML cards, reviews the contents, enters requested data, makes choices etc. The WML browser fetches decks as required from origin servers. Either these decks can be static files on the server or they can be dynamically generated.

WML includes several basic features:

- **Text and images: WML gives, as do other mark-up languages, hints how text and images can be presented to a user. However, the exact presentation of data to a user is up to the user agent running on the handheld device. WML only provides a set of mark-up elements, such as emphasis elements (bold, italic, etc.) for text, or tab columns for tabbing alignment.**
- **User interaction: WML supports different elements for user input. Examples are: text entry controls for text or password entry, option selections or controls for task invocation. Again, the user agent is free to choose how these inputs are implemented. They could be bound to, e.g., physical keys, soft keys, or voice input.**

Navigation: As with HTML browsers, WML offers a history mechanism with navigation through the browsing history, hyperlinks and other inter card navigation elements.

- **Context management: WML allows for saving the state between different decks without server interaction, i.e., variable state can last longer than a single deck, and so state can be shared across different decks. Cards can have parameters defined by using this state without access to the server over the narrow-band wireless channel.**

5.5.1 WML Script

WML Script complements to WML and provides a general scripting capability in the WAP architecture (WAP Forum, 2000h). While all WML content is static (after loading on the client)
WML Script offers several capabilities not supported by WML:

(1) Validity check of user input: before user input is sent to a server, WML Script can check the validity and save bandwidth and latency in case of an error. Otherwise, the server has to perform all the checks, which always includes at least one round trip if problems occur.

(2) Access to device facilities: WML Script offers functions to access hardware components and software functions of the device. On a phone a user could, e.g., make a phone call, access the address book, or send a message via the message service of the mobile phone.

(3) Local user interaction: Without introducing round-trip delays, WML Script can directly and locally interact with a user, show messages or prompt for input. Only, for example, the result of several interactions could be transmitted to a server.

WML Script is event-based, i.e., a script may be invoked in response to certain user or environment events. WML Script also has full access to the state model of WML, i.e., WML Script can set and read WML variables.

Here is a simple example for some lines of WML Script: the function pizza_test accepts one value as input. The local variable tatse is initialized to the string "unknown". Then the script checks if the input parameter pizza_type has the value "Mar". If this is the case, taste is set to "well... ", otherwise the script checks if the pizza_type is "Vul". If this is the case, taste is set to "quite hot".

Finally, the current value of taste is returned as the value of the function pizza_test.

```
function
pizza_test(pizza_type) {
var taste = "unknown";
if (pizza_type =
"Mar") { taste =
"well... ";
}
else {
if (pizza_type =
"Vul") { taste =
"quite hot";
};
};
return taste;
};
```

5.5.2 Wireless telephony application (WTA)

WTA is a collection of telephony specific extensions for call and feature control mechanisms, merging data networks and voice networks. It is an Extension of basic WAE application model with following features

(a) network model for interaction

- **client requests to server**

- **event signaling: server can push content to the client**

(b) Event handling

- **table indicating how to react on certain events from the network**
- **client may now be able to handle unknown events**

5.5.3 Wireless telephony application interface (WTAI) includes:

- **Call control**
- **Network text messaging**
- **Phone book interface**
- **Event processing**

5.6 Wireless telephony application architecture:

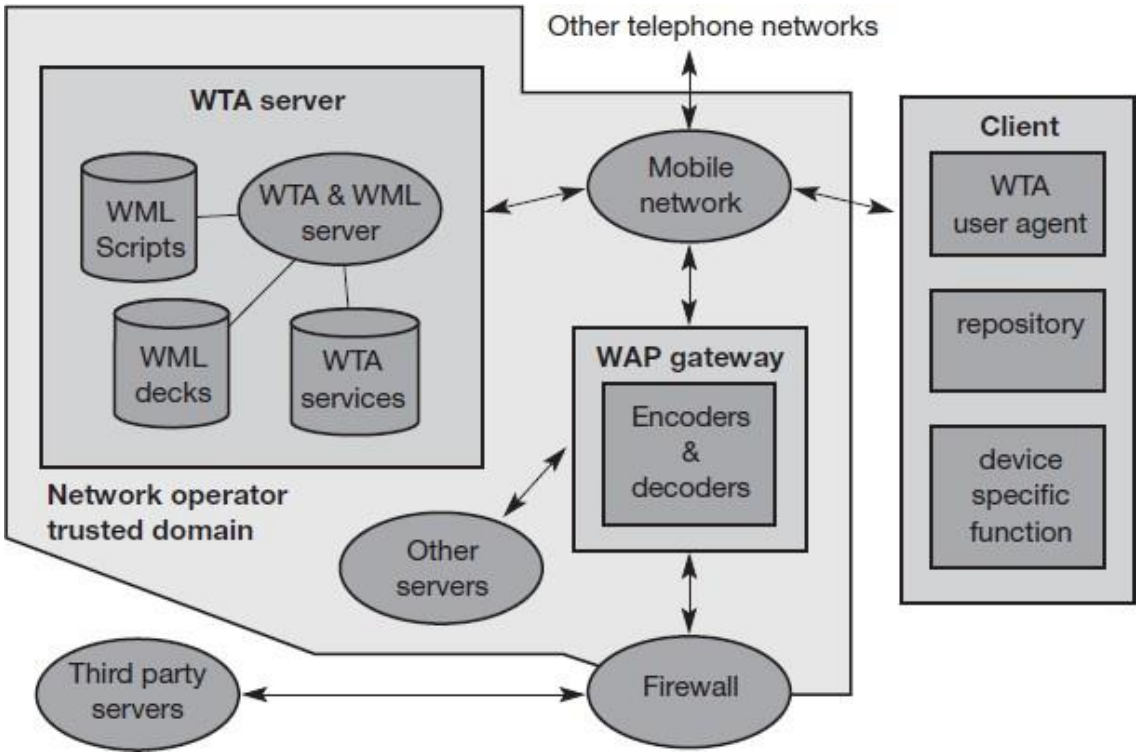


Figure 5.4 WTA Architecture

- **The client is connected via a mobile network with a WTA server, other telephone networks and a WAP gateway.**

- **A WML user agent running on the client is not shown here.**
- **The client may have voice and data connections over the network.**
- **Other origin servers can be connected via the WAP gateway.**

5.6.1 WTA Security Model:

In the WTA security model, any entity may become a WTA Service Provider by being approved for access to a trusted gateway. Access control of the trusted gateway by the WTA servers should be enforced using existing secure solutions. In order to provide security to WTA, a WAP gateway may control the access between the WTA user-agent and the WTA server. The WAP gateway should verify that the providers of WTA pull/push content are authorized.

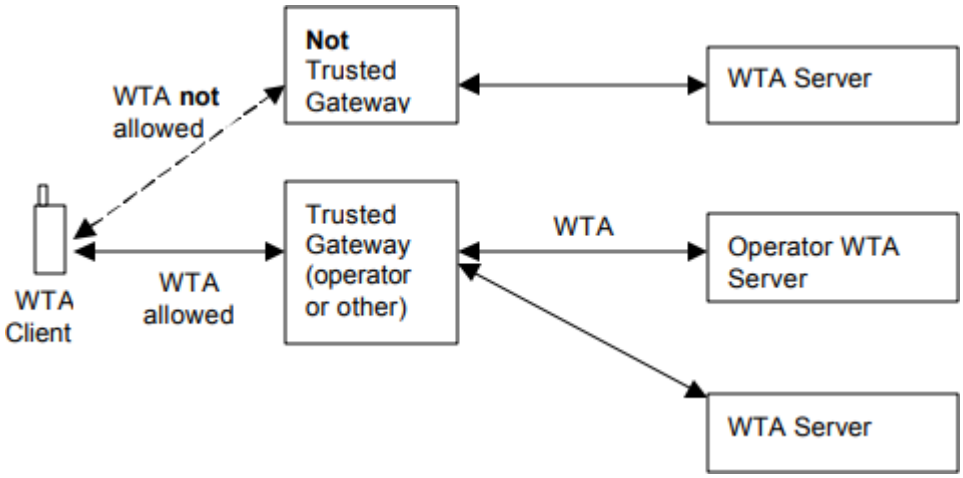


Figure 5.5 WTA Security Model

WTA Security

5.6.2 I-mode

The i-mode service was introduced in Japan by the mobile network operator NTT DoCoMo in 1999. While other network operators in Japan .NTT DoCoMo decided to use its own system which is based on the web protocols and content formats known from the www. Example services offered by i- mode are e-mail, web access (with certain restrictions), and picture exchange. The system soon became a big success with more than 30 million users only three years after its introduction. In comparison to i-mode, WAP was often cited as a failure, and operators outside Japan took over i- mode to participate in the

success.

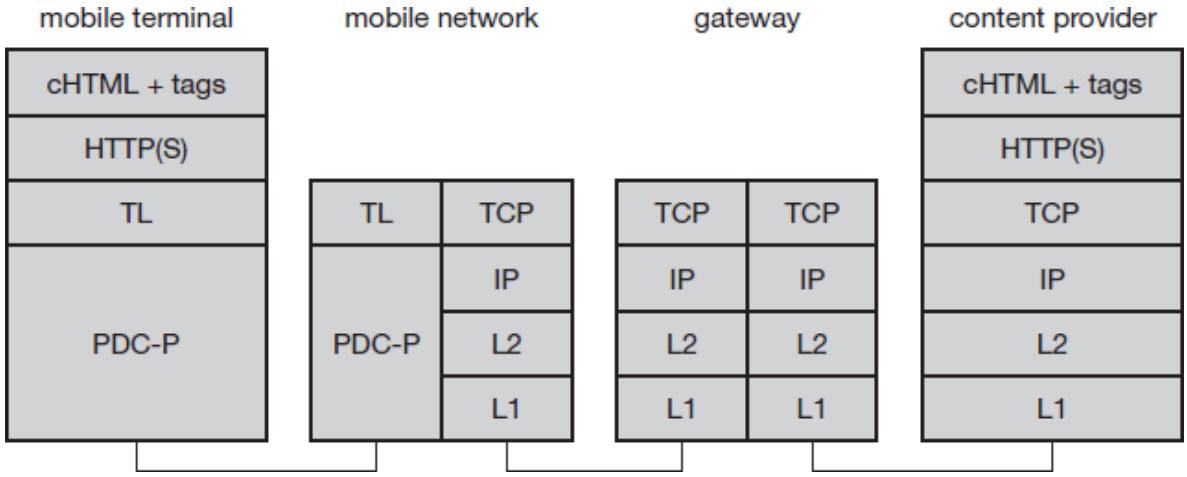


Figure 5.6 I-Mode Protocol Stack

The packet oriented PDC-P provides the bearer service between the mobile terminal and the operator's network. Typical data rates are 9.6 kbit/s, while enhanced versions offer 28.8 kbit/s. On top of the bearer service, i-mode uses a special connection oriented transport layer protocol with stop-and- go flow control, ARQ, push services (ARIB standard RCR STD27X). Within the operator's network and between the operator's gateway and a content provider, i-mode uses standard Internet protocols (TCP/IP over different layer 1 and layer 2 protocols). On top of the transport services, i-mode uses HTTP (with or without security if supported by the handset) as known from the www. i-mode applications can use an e-mail service or display pages described in compact HTML

5.6.3 SyncML

A set of protocols and a markup language for synchronization of data in mobile scenarios is provided by the SyncML framework (SyncML, 2002). The SyncML initiative is supported by companies like Ericsson, IBM, Motorola, Nokia, Openwave, Panasonic, Starfish, and Symbian. SyncML provides vendor independent mechanisms not only for synchronization of data, but also for the administration of devices and applications. The WAP 2.0 framework, which is described in the next section, chose SyncML as a synchronization mechanism.

The synchronization protocol may run over HTTP, WSP, or the object exchange

protocol OBEX. However, many more protocols such as SMTP or TCP/IP could be used. SyncML does not make many assumptions about the data structures. Each set of data must have a unique identifier. Clients and servers can use their individual identifiers for data sets. However, servers have to know the mapping between the identifiers. Clients and servers have to log changes and must be able to exchange these logs.

The messages exchanged for synchronization are based on XML. Tags have been specified to

<add>, <copy>, <delete>, and <replace> data sets. Operations can be made <atomic> (i.e., either all or no change operations may be applied) or applied in a certain <sequence>. If a conflict occurs (e.g., the same data set has been changed on the client and the server) SyncML does not specify a conflict resolution strategy. Instead, several recommendations for conflict resolution are given. Data sets can be mixed, the client may override server changes (or vice versa), a duplicate of the data set can be generated, or a failure of synchronization is signalled.

TEXT / REFERENCE BOOKS

1. Jochen Schiller, "Mobile Communications", Second Edition, Pearson Education, 2003.

2. William Stallings, "Wireless Communications and Networks", Pearson Education, 2002.

3. Yi-Bing Lin, Imrich Chlamtac, "Wireless and Mobile Network Architectures", John Wiley and sons, 2001