srivenkateshwaraa
College of Engineering & Technology
(Approved by AICTE, New Delhi & Affiliated to Pondicherry University, Puducherry)
13-A, Pondy - Villupuram Main Road, Ariyur, Puducherry - 605 102.
ASPIRE TO EXCEL
ISO 21001

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

EC E20- CELLULAR MOBILE COMMUNICATION

IV YEAR/ VIII SEM

COURSE OBJECTIVE

- *To understand the fundamentals of cellular communications and acquire knowledge on mobility and its procedures involved in mobile communication*
- *To gain better understanding of GSM technology and its real time application*
- *To frame ideas on working of various protocols involved in wireless communication and anticipate the emerging technologies and its benefits.*

COURSE OUTCOME

On successful completion of the module you may able to:

- *Understand the fundamentals of cellular communications and design a wireless cellular system*
- *Implement real time applications using GSM technology*
- *Apply the concepts of various Wireless protocols and implement a cellular system using up-coming technologies*

UNIT-I

Introduction: The cellular concept – Frequency reuse – Interference and system capacity – Trunking and Grade of service – Improving coverage and capacity in cellular systems - Advanced Mobile Phone service - Global system for mobile communication - EIA/T IA IS-136 Digital cellular system - EIA/T IA IS-95 Digital cellular system - cordless telephony and low tier TCS - Third generation wireless system.

UNIT-II

Mobility Management: Handoff - Roaming management - Handoff detection – channel Assignment techniques - Radio link transfer IS-41 Network signaling – Intersystem handoff and Authentication - PACS Network Signaling - cellular digital packet data.

UNIT-III

GSM: GSM Network signaling - GSM Mobility management GSM short message service - International roaming for GSM - GSM operation, Administration and maintenance -Mobile number Mobile number portability‘s, VoIP service for mobile networks.

UNIT-IV

Wireless Application Protocol: WAP model - WAP Gateway - WAP Protocol, WAP UAProf and caching - Wireless bearer for WAP - WAP developer tool kits – Mobile station application execution environment.

UNIT-V

Special Topics: Third generation mobile services - Wireless local loop – Wireless enterprise networks - Bluetooth technology. **(12)**

Text Books:

1. Yi-Bing Lin and Imrichchlantae, ―Wireless and Mobile Network Architecture‖, John Wiley 2006.
2. T. S. Rappaport, ―Wireless and Mobile Communication‖, Pearson Education, 2008.

Reference Books:

1. Kauch Pahlavan and Prahant Krishna moorthy, ―Principles of Wireless Networks‖, PHI Learning, 2007

Web References:

1. www.etsi.org
2. www.globecommsystems.com/wireless

UNIT - 1

INTRODUCTION

The cellular Concept

Introduction

Communication is one of the integral parts of science that has always been a focus point for exchanging information among parties at locations physically apart. After its discovery, telephones have replaced the telegrams and letters. Similarly, the term `mobile' has completely revolutionized the communication by opening up innovative applications that are limited to one's imagination. Today, mobile communication has become the backbone of the society. All the mobile system technologies have improved the way of living. It's main plus point is that it has privileged a common mass of society. In this chapter, the evolution as well as the fundamental techniques of the mobile communication is discussed.

Evolution of Mobile Radio Communications

The first wireline telephone system was introduced in the year 1877. Mobile communication systems as early as 1934 were based on Amplitude Modulation (AM) schemes and only certain public organizations maintained such systems. With the demand for newer and better mobile radio communication systems during the World War II and the development of Frequency Modulation (FM) technique by Edwin Armstrong, the mobile radio communication systems began to witness many new changes. Mobile telephone was introduced in the year 1946. However, during its initial three and a half decades it found very less market penetration owing to high costs and numerous technological drawbacks. But with the development of the cellular concept in the 1960s at the Bell Laboratories, mobile communications began to be a promising field of expanse which could serve wider populations. Initially, mobile communication was restricted to certain official users and the cellular concept was never even dreamt of being made commercially available. Moreover, even the growth in the cellular networks was very slow.

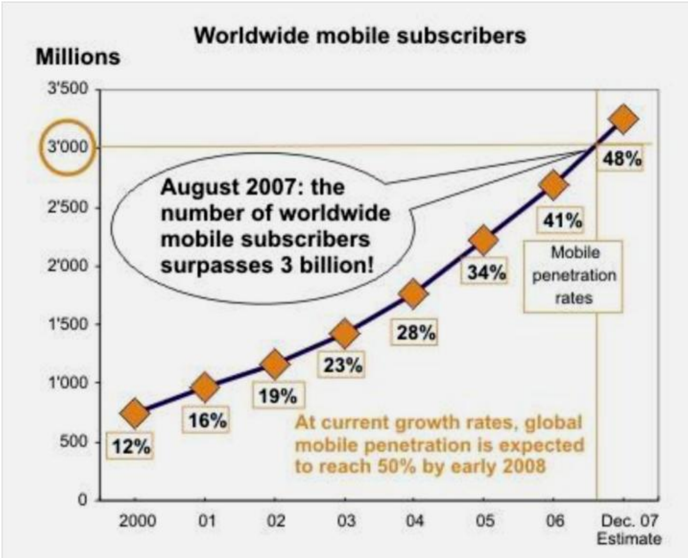

Figure 1.1.1 The worldwide mobile subscriber chart

However, with the development of newer and better technologies starting from the 1970s and with the mobile users now connected to the Public Switched Telephone Network (PSTN), there has been an astronomical growth in the cellular radio and the personal communication systems. Advanced Mobile Phone System (AMPS) was the first U.S. cellular telephone system and it was deployed in 1983. Wireless services have since then been experiencing a 50% per year growth rate. The number of cellular telephone users grew from 25000 in 1984 to around 3 billion in the year 2007 and the demand rate is increasing day by day. A schematic of the subscribers is shown in Fig. 1.1.1.

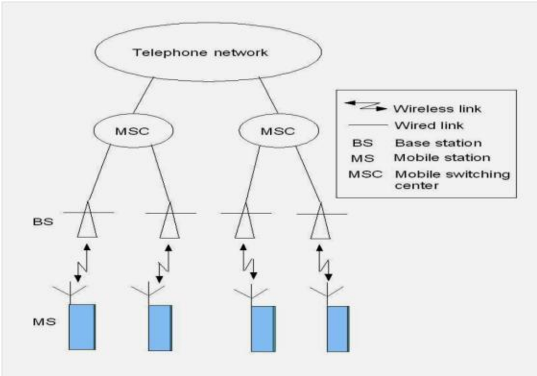

Figure 1.1.2: Basic mobile communication structure.

Present Day Mobile Communication

Since the time of wireless telegraphy, radio communication has been used extensively. Our society has been looking for acquiring mobility in communication since then. Initially the mobile communication was limited between one pair of users on single channel pair. The range of mobility was defined by the transmitter power, type of antenna used and the frequency of operation. With the increase in the number of users, accommodating them within the limited available frequency spectrum became a major problem.

To resolve this problem, the concept of cellular communication was evolved. The present day cellular communication uses a basic unit called cell. Each cell consists of small hexagonal area with a base station located at the center of the cell which communicates with the user. To accommodate multiple users Time Division multiple Access (TDMA), Code Division Multiple Access (CDMA), Frequency Division Multiple Access (FDMA) and their hybrids are used. Numerous mobile radio standards have been deployed at various places such as AMPS, PACS, GSM, NTT, PHS and IS-95, each utilizing different set of frequencies and allocating different number of users and channels.

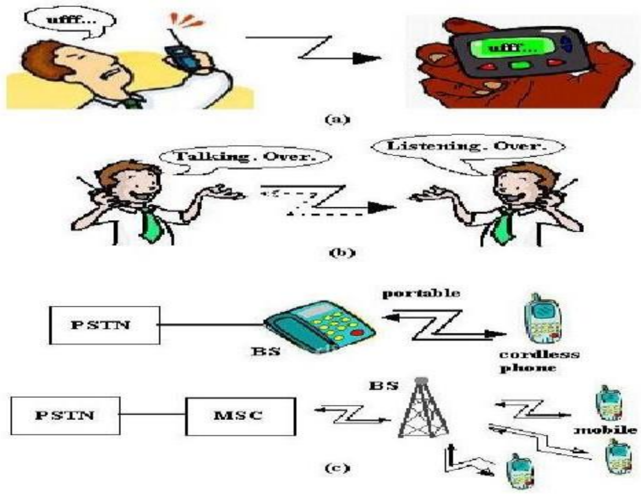

Figure 1.1.3: The basic radio transmission techniques: (a) simplex, (b) half duplex and (c) full duplex.

Fundamental Techniques

By definition, mobile radio terminal means any radio terminal that could be moved during its operation. Depending on the radio channel, there can be three different types of mobile communication. In general, however, a Mobile Station (MS) or subscriber unit communicates to a fixed Base Station (BS) which in turn communicates to the desired user at the other end. The MS consists of transceiver, control circuitry, duplexer and an antenna while the BS consists of transceiver and channel multiplexer along with antennas mounted on the tower. The BS are also linked to a power source for the transmission of the radio signals for communication and are connected to a fixed backbone network. Figure 1.1.2 shows a basic mobile communication with low power transmitters/receivers at the BS, the MS and also the Mobile Switching Center (MSC). The MSC is sometimes also called Mobile Telephone Switching Ofice (MTSO). The radio signals emitted by the BS decay as the signals travel away from it. A minimum amount of signal strength is needed in order to be detected by the mobile stations or mobile sets which are the hand-held personal units (portables) or those installed in the vehicles (mobiles). The region over which the signal strength lies above such a threshold value is known as the coverage area of a BS. The fixed backbone network is a wired network that links all the base stations and also the landline and other telephone networks through wires.

Radio Transmission Techniques

Based on the type of channels being utilized, mobile radio transmission systems may be classified as the following three categories which is also shown in Fig. 1.1.3

Simplex System: Simplex systems utilize simplex channels i.e., the communication is unidirectional. The first user can communicate with the second user. However, the second user cannot communicate with the first user. One example of such a system is a pager. Fig 1.1.3 (b)

Half Duplex System: Half duplex radio systems that use half duplex radio channels allow for non-simultaneous bidirectional communication. The first user can communicate with the second user but the second user can communicate to the first user only after the first user has finished his conversation. At a time, the user can only transmit or receive information. A walkie-talkie is an example of a half duplex system which uses `push to talk' and `release to listen' type of switches.

Full Duplex System: Full duplex systems allow two way simultaneous communications. Both the users can communicate to each other simultaneously. This can be done by providing two simultaneous but separate channels to both the users. This is possible by one of the two following methods. Frequency Division Duplexing (FDD): FDD supports two-way radio communication by using two distinct radio channels. One frequency channel is transmitted downstream from the BS to the MS (forward channel).

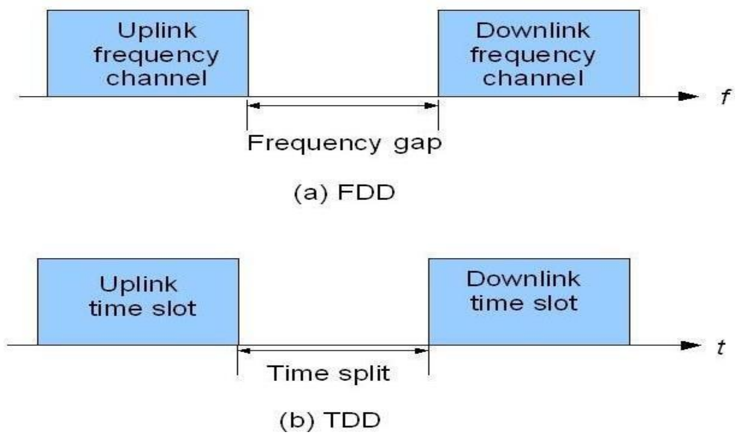

Figure 1.1.4: (a) Frequency division duplexing and (b) time division duplexing.

A second frequency is used in the upstream direction and supports transmission from the MS to the BS (reverse channel). Because of the pairing of frequencies, simultaneous transmission in both directions is possible. To mitigate self-interference between upstream and downstream transmissions, a minimum amount of frequency separation must be maintained between the frequency pair, as shown in Fig. 1.1.4. Time Division Duplexing (TDD): TDD uses a single frequency band to transmit signals in both the downstream and upstream directions. TDD operates by toggling transmission directions over a time interval. This toggling takes place very rapidly and is imperceptible to the user. A full duplex mobile system can further be subdivided into two categories: a single MS for a dedicated BS, and many MS for a single BS. Cordless telephone systems are full duplex communication systems that use radio to connect to a portable handset to a single dedicated BS, which is then connected to a dedicated telephone line with a specific telephone number on the Public Switched Telephone Network (PSTN). A mobile system, in general, on the other hand, is the example of the second category of a full duplex mobile system where many users connect among themselves via a single BS.

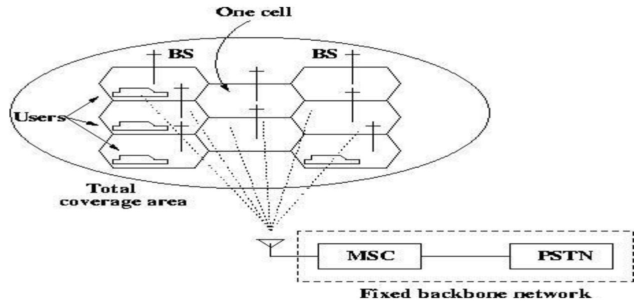

Figure 1.1.5: Basic Cellular Structure.

How a Mobile Call is Actually Made?

In order to know how a mobile call is made, we should first look into the basics of cellular concept and main operational channels involved in making a call. These are given below.

Cellular Concept

Cellular telephone systems must accommodate a large number of users over a large geographic area with limited frequency spectrum, i.e., with limited number of channels. If a single transmitter/ receiver is used with only a single base station, then sufficient amount of power may not be present at a huge distance from the BS. For a large geographic coverage area, a high powered transmitter therefore has to be used. But a high power radio transmitter causes harm to environment. Mobile communication thus calls for replacing the high power transmitters by low power transmitters by dividing the coverage area into small segments, called cells. Each cell uses a certain number of the available channels and a group of adjacent cells together use all the available channels. Such a group is called a cluster. This cluster can repeat itself and hence the same set of channels can be used again and again. Each cell has a low power transmitter with a coverage area equal to the area of the cell. This technique of substituting a single high powered transmitter by several low powered transmitters to support many users is the backbone of the cellular concept.

Operational Channels

- In each cell, there are four types of channels that take active part during a mobile call. These are: Forward Voice Channel (FVC): This channel is used for the voice transmission from the BS to the MS.
- Reverse Voice Channel (RVC): This is used for the voice transmission from the MS to the BS.
- Forward Control Channel (FCC): Control channels are generally used for controlling the activity of the call, i.e., they are used for setting up calls and to divert the call to unused voice channels. Hence these are also called setup channels. These channels transmit and receive call initiation and service request messages. The FCC is used for control signaling purpose from the BS to MS.
- Reverse Control Channel (RCC): This is used for the call control purpose from the MS to the BS. Control channels are usually monitored by mobiles.

Making a Call

When a mobile is idle, i.e., it is not experiencing the process of a call, then it searches all the FCCs to determine the one with the highest signal strength. The mobile then monitors this particular FCC. However, when the signal strength falls below a particular threshold that is insufficient for a call to take place, the mobile again searches all the FCCs for the one with the highest signal strength. For a particular country or continent, the control channels will be the same. So all mobiles in that country or continent will search among the same set of control channels. However, when mobile moves to a different country or continent, then the control channels for that particular location will be different and hence the mobile will not work. Each mobile has a mobile identification number (MIN). When a user wants to make a call, he sends a call request to the MSC on the reverse control channel. He also sends the MIN of the person to whom the call has to be made. The MSC then sends this MIN to all the base stations. The base station transmits this MIN and all the mobiles within the coverage area of that base station receive the MIN and match it with their own. If the MIN matches with a particular MS, that mobile sends an acknowledgment to the BS. The BS then informs the MSC that the mobile is within its coverage area. The MSC then instructs the base station to access specific unused voice channel pair. The base station then sends a message to the mobile to move to the particular channels and it also sends a signal to the mobile for ringing. In order to maintain the quality of the call, the MSC adjusts the transmitted power of the mobile which is usually expressed in dB or dBm. When a mobile moves from the coverage area of one base station to the coverage area of another base station i.e., from one cell to another cell, then the signal strength of the initial base station may not be sufficient to continue the call in progress. So the call has to be transferred to the other base station. This is called handoff. In such cases, in order to maintain the call, the MSC transfers the call to one of the unused voice channel of the new base station or it transfers the control of the current voice channels to the new base station.

1.1.5.3 Future Trends

Tremendous changes are occurring in the area of mobile radio communications, so much so that the mobile phone of yesterday is rapidly turning into a sophisticated mobile device capable of more applications than PCs were capable of only a few years ago. Rapid development of the Internet with its new services and applications has created fresh challenges for the further development of mobile communication systems. Further enhancements in modulation schemes will soon increase the Internet access rates on the mobile from current 1.8 Mbps to greater than 10 Mbps. Bluetooth is rapidly becoming a common feature in mobiles for local connections. The mobile communication has provided global connectivity to the people at a lower cost due to advances in the technology and also because of the growing competition among the service providers.

Frequency Reuse

What is a cell?

The power of the radio signals transmitted by the BS decay as the signals travel away from it. A minimum amount of signal strength (let us say, x dB) is needed in order to be detected by the MS or mobile sets which may the hand-held personal units or those installed in the vehicles. The region over which the signal strength lies above this threshold value x dB is known as the coverage area of a BS and it must be a circular region, considering the BS to be isotropic radiator. Such circle, which gives this actual radio coverage, is called the foot print of a cell (in reality, it is amorphous). It might so happen that either there may be an overlap between any two such side by side circles or there might be a gap between the coverage areas of two adjacent circles. This is shown in Figure 1.2.1. Such a circular geometry, therefore, cannot serve as a regular shape to describe cells. We need a regular shape for cellular design over a territory which can be served by 3 regular polygons, namely, equilateral triangle, square and regular hexagon,

which can cover the entire area without any overlap and gaps. Along with its regularity, a cell must be designed such that it is most reliable too, i.e., it supports even the weakest mobile with occurs at the edges of the cell. For any distance between the center and the farthest point in the cell from it, a regular hexagon covers the maximum area. Hence regular hexagonal geometry is used as the cells in mobile communication.

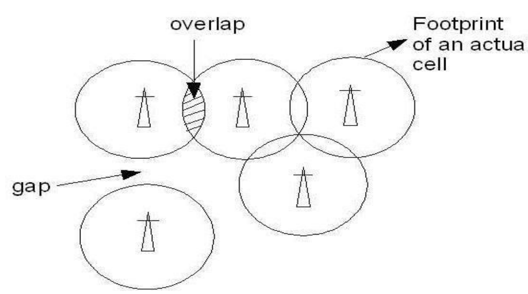

Figure 1.2.1: Footprint of cells showing the overlaps and gaps.

Frequency Reuse

Frequency reuse, or, frequency planning, is a technique of reusing frequencies and channels within a communication system to improve capacity and spectral efficiency. Frequency reuse is one of the fundamental concepts on which commercial wireless systems are based that involve the partitioning of an RF radiating area into cells. The increased capacity in a commercial wireless network, compared with a network with a single transmitter, comes from the fact that the same radio frequency can be reused in a different area for a completely different transmission.

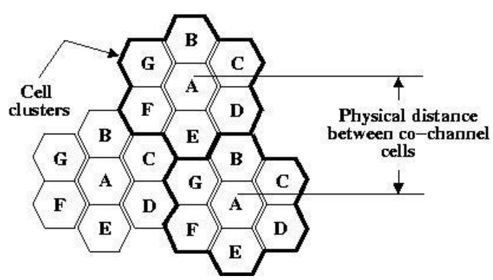

Figure 1.2.2: Frequency reuse technique of a cellular system.

Frequency reuse in mobile cellular systems means that frequencies allocated to the service are reused in a regular pattern of cells, each covered by one base station. The repeating regular pattern of cells is called cluster. Since each cell is designed to use radio frequencies only within its boundaries, the same frequencies can be reused in other cells not far away without interference, in another cluster. Such cells are called `co-channel' cells. The reuse of frequencies enables a cellular system to handle a huge number of calls with a limited number of channels. Figure 1.2.2 shows a frequency planning with cluster size of 7, showing the co-channels cells in different clusters by the same letter. The closest distance between the co-channel cells (in different clusters) is determined by the choice of the cluster size and the layout of the cell cluster. Consider a cellular system with S duplex channels available for use and let N be the number of cells in a cluster. If each cell is allotted K duplex channels with all being allotted unique and disjoint channel groups we have S = KN under normal circumstances. Now, if the cluster are repeated M times within the total area, the total number of duplex channels, or, the total number of users in the system would be T = MS = KMN. Clearly, if K and N remain constant, then

$$T \ \alpha \ M \qquad (1.2.1)$$

and, if T and K remain constant, then

$$N \ \frac{\alpha}{M} \qquad (1.2.2)$$

Hence the capacity gain achieved is directly proportional to the number of times a cluster is repeated, as shown in (1.2.1), as well as, for a fixed cell size, small N decreases the size of the cluster with in turn results in the increase of the number of clusters (1.2.2) and hence the capacity. However for small N, co-channel cells are located much closer and hence more interference. The value of N is determined by calculating the amount of interference that can be tolerated for a sufficient quality communication. Hence the smallest N having interference below the tolerated limit is used. However, the cluster size N cannot take on any value and is given only by the following equation

$$N = i^2 + ij + j^2 \quad i \geq 0, \ j \geq 0 \qquad (1.2.3)$$

Where i and j are integer numbers.

Interference and system capacity

Susceptibility and interference problems associated with mobile communications equipment are because of the problem of time congestion within the electromagnetic spectrum. It is the limiting factor in the performance of cellular systems. This interference can occur from clash with another mobile in the same cell or because of a call in the adjacent cell. There can be interference between the base stations operating at same frequency band or any other non-cellular system's energy leaking inadvertently into the frequency band of the cellular system. If there is an interference in the voice channels, cross talk is heard will appear as noise between the users. The interference in the control channels leads to missed and error calls because of digital signaling. Interference is more severe in urban areas because of the greater RF noise and greater density of mobiles and base stations. The interference can be divided into 2 parts: co-channel interference and adjacent channel interference.

Co-channel interference (CCI)

For the efficient use of available spectrum, it is necessary to reuse frequency bandwidth over relatively small geographical areas. However, increasing frequency reuse also increases interference, which decreases system capacity and service quality.

The cells where the same set of frequencies is used are call co-channel cells. Co-channel interference is the cross talk between two different radio transmitters using the same radio frequency as is the case with the co-channel cells. The reasons of CCI can be because of either adverse weather conditions or poor frequency planning or overly crowded radio spectrum. If the cell size and the power transmitted at the base stations are same then CCI will become independent of the transmitted power and will depend on radius of the cell (R) and the distance between the interfering co-channel cells (D). If D/R ratio is increased, then the effective distance between the co-channel cells will increase and interference will decrease. The parameter Q is called the frequency reuse ratio and is related to the cluster size. For hexagonal geometry

$$Q = \frac{D}{R} = \sqrt{3N} \qquad (1.3.1.1)$$

From the above equation, small of `Q' means small value of cluster size `N' and increase in cellular capacity. But large `Q' leads to decrease in system capacity but increase in transmission quality. Choosing the options is very careful for the selection of `N', the proof of which is given in the first section. The Signal to Interference Ratio (SIR) for a mobile receiver which monitors the forward channel can be calculated as

$$\frac{S}{I} = \frac{S}{\sum_{i=1}^{i_0} I_i} \qquad (1.3.1.2)$$

Where i_0 is the number of co-channel interfering cells, S is the desired signal power from the baseband station and I_i is the interference power caused by the i-th interfering co-channel base station. In order to solve this equation from power calculations, we need to look into the signal power characteristics. The average power in the mobile radio channel decays as a power law of the distance of separation between transmitter and receiver. The expression for the received power P_r at a distance d can be approximately calculated as

$$P_r = P_0 \left(\frac{d}{d_0}\right)^{-n} \qquad (1.3.1.3)$$

and in the dB expression as

$$P_r(dB) = P_0(dB) - 10n\log\left(\frac{d}{d_0}\right) \qquad (1.3.1.4)$$

Where P_0 is the power received at a close-in reference point in the far field region at a small distance do from the transmitting antenna and `n' is the path loss exponent. Let us calculate the SIR for this system. If D_i is the distance of the i-th interferer from the mobile, the received power at a given mobile due to i-th interfering cell is proportional to $(Di)^{-n}$ (the value of 'n' varies between 2 and 4 in urban cellular systems).

Let us take that the path loss exponent is same throughout the coverage area and the transmitted power be same, then SIR can be approximated as

$$\frac{S}{I} = \frac{R^{-n}}{\sum_{i=1}^{i_0} D_i^{-n}} \qquad (1.3.1.5)$$

Where the mobile is assumed to be located at R distance from the cell center. If we consider only the first layer of interfering cells and we assume that the interfering base stations are equidistant from the reference base station and the distance between the cell centers is 'D' then the above equation can be converted as

$$\frac{S}{I} = \frac{(D/R)^n}{i_0} = \frac{(\sqrt{3N})^n}{i_0} \qquad (1.3.1.6)$$

Which is an approximate measure of the SIR. Subjective tests performed on AMPS cellular system which uses FM and 30 kHz channels show that sufficient voice quality can be obtained by SIR being greater than or equal to 18 dB. If we take n=4, the value of 'N' can be calculated as 6.49. Therefore minimum N is 7. The above equations are based on hexagonal geometry and the distances from the closest interfering cells can vary if different frequency reuse plans are used.

We can go for a more approximate calculation for co-channel SIR. This is the example of a 7 cell reuse case. The mobile is at a distance of D-R from 2 closest interfering cells and approximately D+R/2, D, D-R/2 and D+R distance from other interfering cells in the first tier. Taking n = 4 in the above equation, SIR can be approximately calculated as

$$\frac{S}{I} = \frac{R^{-4}}{2(D-R)^{-4}+(D+R)^{-4}+(D)^{-4}+(D+\frac{R}{2})^{-4}+(D-\frac{R}{2})^{-4}} \qquad (1.3.1.7)$$

Which can be rewritten in terms frequency reuse ratio Q as

$$\frac{S}{I} = \frac{1}{2(Q-1)^{-4}+(Q+1)^{-4}+(Q)^{-4}+(Q+\frac{1}{2})^{-4}+(q-\frac{1}{2})^{-4}} \qquad (1.3.1.8)$$

Using the value of N equal to 7 (this means Q = 4.6), the above expression yields that worst case SIR is 53.70 (17.3 dB). This shows that for a 7 cell reuse case the worst case SIR is slightly less than 18 dB. The worst case is when the mobile is at the corner of the cell i.e., on a vertex as shown in the Figure 1.3.1.1. Therefore N = 12 cluster size should be used. But this reduces the capacity by 7/12 times. Therefore, co-channel interference controls link performance, which in a way controls frequency reuse plan and the overall capacity of the cellular system. The effect of co-channel interference can be minimized by optimizing the frequency assignments of the base stations and their transmit powers. Tilting the base-station antenna to limit the spread of the signals in the system can also be done.

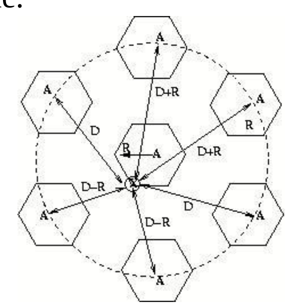

Figure 1.3.1.1: First tier of co-channel interfering cells

Adjacent Channel Interference (ACI)

This is a different type of interference which is caused by adjacent channels i.e. channels in adjacent cells. It is the signal impairment which occurs to one frequency due to presence of another signal on a nearby frequency. This occurs when imperfect receiver filters allow nearby frequencies to leak into the passband. This problem is enhanced if the adjacent channel user is transmitting in a close range compared to the subscriber's receiver while the receiver attempts to receive a base station on the channel. This is called near-far effect. The more adjacent channels are packed into the channel block, the higher the spectral efficiency, provided that the performance degradation can be tolerated in the system link budget. This effect can also occur if a mobile close to a base station transmits on a channel close to one being used by a weak mobile.

This problem might occur if the base station has problem in discriminating the mobile user from the "bleed over" caused by the close adjacent channel mobile. Adjacent channel interference occurs more frequently in small cell clusters and heavily used cells. If the frequency separation between the channels is kept large this interference can be reduced to some extent. Thus assignment of channels is given such that they do not form a contiguous band of frequencies within a particular cell and frequency separation is maximized. Efficient assignment strategies are very much important in making the interference as less as possible. If the frequency factor is small then distance between the adjacent channels cannot put the interference level within tolerance limits. If a mobile is 10 times close to the base station than
Other mobile and has energy spill out of its passband, then SIR for weak mobile is approximately

$$\frac{S}{I} = 1^{-}0^{n} \qquad (1.3.2.1)$$

Which can be easily found from the earlier SIR expressions. If n = 4, then SIR is -52 dB. Perfect base station filters are needed when close-in and distant users share the same cell. Practically, each base station receiver is preceded by a high Q cavity filter in order to remove adjacent channel interference. Power control is also very much important for the prolonging of the battery life for the subscriber unit but also reduces reverse channel SIR in the system. Power control is done such that each mobile transmits the lowest power required to maintain a good quality link on the reverse channel.

Trunking and Grade of service

Cellular systems use the concept of trunking to accommodate a large number of users in a limited radio spectrum. It was found that a central office associated with say, 10,000 telephones requires about 50 million connections to connect every possible pair of users. However, a worst case maximum of 5000 connections need to be made among these telephones at any given instant of time, as against the possible 50 million connections. In fact, only a few hundreds of lines are needed owing to the relatively short duration of a call. This indicates that the resources are shared so that the number of lines is much smaller than the number of possible connections. A line that connects switching offices and that is shared among users on an as-needed basis is called a trunk.

The fact that the number of trunks needed to make connections between offices is much smaller than the maximum number that could be used suggests that at times there might not be sufficient facilities to allow a call to be completed. A call that cannot be completed owing to a lack of resources is said to be blocked. So one important to be answered in mobile cellular systems is: How many channels per cell are needed in a cellular telephone system to ensure a reasonably low probability that a call will be blocked? In a trunked radio system, a channel is allotted on per call basis. The performance of a radio system can be estimated in a way by looking at how efficiently the calls are getting connected and also how they are being maintained at handoffs. Some of the important factors to take into consideration are

(i) Arrival statistics, (ii)Service statistics, (iii) Number of servers/channels.

Let us now consider the following assumptions for a buffer less system handling 'L' users as shown in Figure 1.4.1:

a) The number of users L is large when compared to 1.
b) Arrival statistics is Poisson distributed with a mean parameter λ.
c) Duration of a call is exponentially distributed with a mean rate $\mu 1$.
d) Residence time of each user is exponentially distributed with a rate parameter $\mu 2$.
e) The channel holding rate therefore is exponentially distributed with a parameter $\mu = \mu 1 + \mu 2$.
f) There is a total of 'J' number of channels ($J \leq L$).

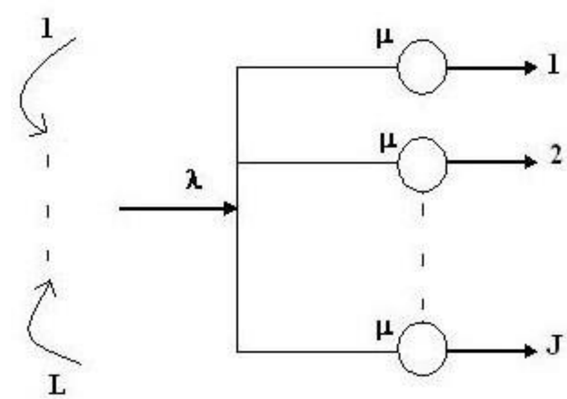

Figure 1.4.1: The buffer less J-channel trunked radio system.

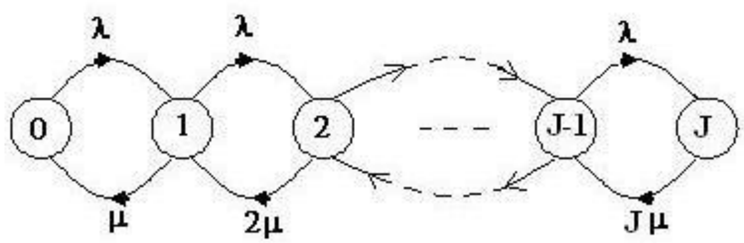

Figure 1.4.2: Discrete-time Markov chain for the M/M/J/J trunked radio system.

To analyze such a system, let us recapitulate a queuing system in brief. Consider an M/M/m/m system which is an m-server loss system. The name M/M/m/m reflects standard queuing theory nomenclature whereby:

(i) The first letter indicates the nature of arrival process (e.g. M stands for memory less which here means a Poisson process).

(ii) The second letter indicates the nature of probability distribution of service times.(e.g M stands for exponential distribution). In all cases, successive inter arrival times and service times are assumed to be statistically independent of each other.

(iii) The third letter indicates the number of servers.

(iv) The last letter indicates that if an arrival finds all 'm' users to be busy, then it will not enter the system and is lost.

In view of the above, the buffer less system as shown in Figure 1.4.1 can be modeled as M/M/J/J system and the discrete-time Markov chain of this system is shown in Figure 1.4.2.

Trunking mainly exploits the statistical behavior of users so that a fixed number of channels can be used to accommodate a large, random user community. As the number of telephone lines decrease, it becomes more likely that all channels are busy for a particular user. As a result, the call gets rejected and in some systems, a queue may be used to hold the caller's request until a channel becomes available. In the telephone system context the term Grade of Service (GoS) is used to mean the probability that a user's request for service will be blocked because a required facility, such as a trunk or a cellular channel, is not available. For example, a GoS of 2 % implies that on the average a user might not be successful in placing a call on 2 out of every 100 attempts. In practice the blocking frequency varies with time. One would expect far more call attempts during business hours than during the middle of the night. Telephone operating companies maintain usage records and can identify a "busy hour", that is, the hour of the day during which there is the greatest demand for service. Typically, telephone systems are engineered to provide a specified grade of service during a specified busy hour. User calling can be modeled statistically by two parameters: the average number of call requests per unit time λ_{user} and the average holding time H. The parameter λ_{user} is also called the average arrival rate, referring to the rate at which calls from a single user arrive. The average holding time is the average duration of a call.
The product:

$$A_{user} = \lambda_{user} H \tag{1.4.1}$$

that is, the product of the average arrival rate and the average holding time is called the offered traffic intensity or offered load. This quantity represents the average traffic that a user provides to the system. Offered traffic intensity is a quantity that is traditionally measured in Erlangs. One Erlang represents the amount of traffic intensity carried by a channel that is completely occupied. For example, a channel that is occupied for thirty minutes during an hour carries 0.5 Erlang of traffic. Call arrivals or requests for service are modeled as a Poisson random process. It is based on the assumption that there is a large pool of users who do not cooperate in deciding when to place calls. Holding times are very well predicted using an exponential probability distribution. This implies that calls of long duration are much less frequent than short calls. If the traffic intensity offered by a single user is Auser, then the traffic intensity offered by N users is $A = NA_{user}$. The purpose of the statistical model is to relate the offered traffic intensity A, the grade of service P_b, and the number of channels or trunks C needed to maintain the desired grade of service. Two models are widely used in traffic engineering to represent what happens when a call is blocked. The blocked calls cleared model assumes that when a channel or trunk is not available to service an arriving call, the call is cleared from the system.

The second model is known as blocked calls delayed. In this model a call that cannot be serviced is placed on a queue and will be serviced when a channel or trunk becomes available. Use of the blocked-calls-cleared statistical model leads to the Erlang B formula that relates offered traffic intensity A, grade of service P_b, and number of channels K. The Erlang B formula is:

$$P_b = \frac{A^K/K!}{\sum_{n=0}^{K} A^n/n!} \tag{1.4.2}$$

When the blocked-calls-delayed model is used, the "grade of service" refers to the probability that a call will be delayed. In this case the statistical model leads to the Erlang C formula,

$$P[delay] = \frac{A^K/[(K-A)(K-1)]!}{A/[(K-A)(K-1)]! + \sum_{n=0}^{K} A^n/n!} \tag{1.4.3}$$

Improving Coverage and capacity in cellular systems

The Key Trade Off

Previously, we have seen that the frequency reuse technique in cellular systems allows for almost boundless expansion of geographical area and the number of mobile system users who could be accommodated. In designing a cellular layout, the two parameters which are of great significance are the cell radius R and the cluster size N, and we have also seen that co-channel cell distance $D = \sqrt{3N}R$. In the following, a brief description of the design trade-off is given, in which the above two parameters play a crucial role.

The cell radius governs both the geographical area covered by a cell and also the number of subscribers who can be serviced, given the subscriber density. It is easy to see that the cell radius must be as large as possible. This is because, every cell requires an investment in a tower, land on which the tower is placed, and radio transmission equipment and so a large cell size minimizes the cost per subscriber. Eventually, the cell radius is determined by the requirement that adequate signal to noise ratio be maintained over the coverage area. The SNR is determined by several factors such as the antenna height, transmitter power, receiver noise figure etc. Given a cell radius R and a cluster size N, the geographic area covered by a cluster is

$$A_{cluster} = NA_{cell} = N3\sqrt{3}R^2/2 \tag{1.5.1.1}$$

If the total serviced area is A_{total}, then the number of clusters M that could be accommodated is given by

$$M = A_{total}/A_{cluster} = A_{total}/(N3\sqrt{3}R^2/2) \tag{1.5.1.2}$$

Note that all of the available channels N, are reused in every cluster. Hence, to make the maximum number of channels available to subscribers, the number of clusters M should be large, which, by Equation (1.5.1.2), shows that the cell radius should be small.

However, cell radius is determined by a trade-off: R should be as large as possible to minimize the cost of the installation per subscriber, but R should be as small as possible to maximize the number of customers that the system can accommodate. Now, if the cell radius R is fixed, then the number of clusters could be maximized by minimizing the size of a cluster N. We have seen earlier that the size of a cluster depends on the frequency reuse ratio Q. Hence, in determining the value of N, another trade-off is encountered in that N must be small to accommodate large number of subscribers, but should be sufficiently large so as to minimize the interference effects.

Now, we focus on the issues regarding system expansion. The history of cellular phones has been characterized by a rapid growth and expansion in cell subscribers. Though a cellular system can be expanded by simply adding cells to the geographical area, the way in which user density can be increased is also important to look at. This is because it is not always possible to counter the increasing demand for cellular systems just by increasing the geographical coverage area due to the limitations in obtaining new land with suitable requirements. We discuss here two methods for dealing with an increasing subscriber density: Cell Splitting and Sectoring. The other method, microcell zone concept can treat as enhancing the QoS in a cellular system. The basic idea of adopting the cellular approach is to allow space for the growth of mobile users.

When a new system is deployed, the demand for it is fairly low and users are assumed to be uniformly distributed over the service area. However, as new users subscribe to the cellular service, the demand for channels may begin to exceed the capacity of some base stations. As discussed previously, the number of channels available to customers (equivalently, the channel density per square kilometer) could be increased by decreasing the cluster size. However, once a system has been initially deployed, a system-wide reduction in cluster size may not be necessary since user density does not grow uniformly in all parts of the geographical area. It might be that an increase in channel density is required only in specific parts of the system to support an increased demand in those areas. Cell-splitting is a technique which has the capability to add new smaller cells in specific areas of the system

Cell-Splitting

Cell Splitting is based on the cell radius reduction and minimizes the need to modify the existing cell parameters. Cell splitting involves the process of sub-dividing a congested cell into smaller cells, each with its own base station and a corresponding reduction in antenna size and transmitting power. This increases the capacity of a cellular system since it increases the number of times that channels are reused. Since the new cells have smaller radii than the existing cells, inserting these smaller cells, known as microcells, between the already existing cells results in an increase of capacity due to the additional number of channels per unit area. There are few challenges in increasing the capacity by reducing the cell radius. Clearly, if cells are small, there would have to be more of them and so additional base stations will be needed in the system. The challenge in this case is to introduce the new base stations without the need to move the already existing base station towers. The other challenge is to meet the generally increasing demand that may vary quite rapidly between geographical areas of the system. For instance, a city may have highly populated areas and so the demand must be supported by cells with the smallest radius. The radius of cells will generally increase as we move from urban to sub urban areas, because the user density decreases on moving towards sub-urban areas. The key factor is to add as minimum number of smaller cells as possible

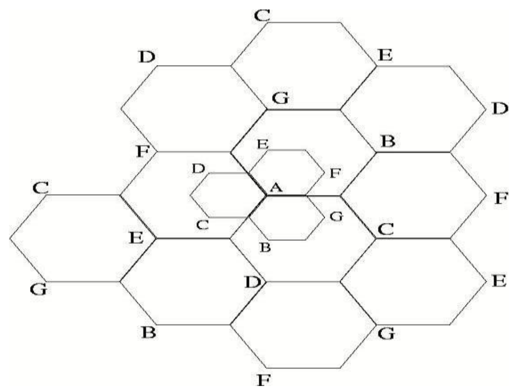

Figure 1.5.2.1: Splitting of congested seven-cell clusters.

wherever an increase in demand occurs. The gradual addition of the smaller cells implies that, at least for a time, the cellular system operates with cells of more than one size. Figure

shows a cellular layout with seven-cell clusters. Consider that the cells in the center of the diagram are becoming congested, and cell A in the center has reached its maximum capacity. Figure also shows how the smaller cells are being superimposed on the original layout. The new smaller cells have half the cell radius of the original cells. At half the radius, the new cells will have one-fourth of the area and will consequently need to support one-fourth the number of subscribers. Notice that one of the new smaller cells lies in the center of each of the larger cells. If we assume that base stations are located in the cell centers, this allows the original base stations to be maintained even in the new system layout. However, new base stations will have to be added for new cells that do not lie in the center of the larger cells. The organization of cells into clusters is independent of the cell radius, so that the cluster size can be the same in the small-cell layout as it was in the large-cell layout. Also the signal-to-interference ratio is determined by cluster size and not by cell radius. Consequently, if the cluster size is maintained, the signal-to-interference ratio will be the same after cell splitting as it was before. If the entire system is replaced with new half-radius cells, and the cluster size is maintained, the number of channels per cell will be exactly as it was before, and the number of subscribers per cell will have been reduced.

When the cell radius is reduced by a factor, it is also desirable to reduce the transmitted power. The transmit power of the new cells with radius half that of the old cells can be found by examining the received power PR at the new and old cell boundaries and setting them equal. This is necessary to maintain the same frequency re-use plan in the new cell layout as well. Assume that PT1 and PT2 are the transmit powers of the larger and smaller base stations respectively. Then, assuming a path loss index n=4, we have power received at old cell boundary = PT1=R4 and the power received at new cell boundary = PT2=(R=2)4. On equating the two received powers, we get PT2 = PT1 / 16. In other words, the transmit power must be reduced by 12 dB in order to maintain the same S/I with the new system lay-out. At the\ beginning of this channel splitting process, there would be fewer channels in the smaller power groups. As the demand increases, more and more channels need to be accommodated and hence the splitting process continues until all the larger cells have been replaced by the smaller cells, at which point splitting is complete within the region and the entire system is rescaled to have a smaller radius per cell. If a cellular layout is replaced entirety by a new layout with a smaller cell radius, the signal-to-interference ratio will not change, provided the cluster size does not change.

Some special care must be taken, however, to avoid co-channel interference when both large and small cell radii coexist. It turns out that the only way to avoid interference between the large-cell and small-cell systems is to assign entirely different sets of channels to the two systems. So, when two sizes of cells co-exist in a system, channels in the old cell must be broken down into two groups, one that corresponds to larger cell reuse requirements and the other which corresponds to the smaller cell reuse requirements. The larger cell is usually dedicated to high speed users as in the umbrella cell approach so as to minimize the number of hand-offs.

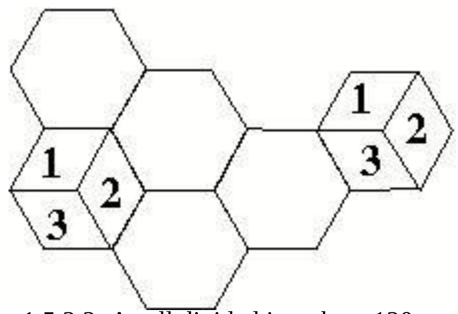

Figure 1.5.2.2: A cell divided into three 120o sectors.

signal-to-noise ratio over 90% of the coverage area. Although a 12-cell cluster size provided more than adequate co-channel separation to meet a requirement for a 17 dB signal-to-interference ratio in an interference-limited environment, it did not provide adequate frequency reuse to service an explosively growing customer base. The system planners reasoned that a subsequent shift to a 7-cell cluster size would provide an adequate number of channels. It was estimated that a 7-cell cluster size should provide an adequate 18.7 dB signal-to-interference ratio. The margin, however, is slim, and the 17 dB signal-to-interference ratio requirement could not be met over 90 % of the coverage area.

Sectoring

Sectoring is basically a technique which can increase the SIR without necessitating an increase in the cluster size. Till now, it has been assumed that the base station is located in the center of a cell and radiates uniformly in all the directions behaving as an omni-directional antenna. However it has been found that the co-channel interference in a cellular system may be decreased by replacing a single Omni-directional antenna at the base station by several directional antennas, each radiating within a specified sector. In the Figure 3.8, a cell is shown which has been split into three 120^o sectors. The base station feeds three 120o directional antennas, each of which radiates into one of the three sectors. The channel set serving this cell has also been divided, so that each sector is assigned one-third of the available number cell of channels. This technique for reducing co-channel interference wherein by using suit-able directional antennas, a given cell would receive interference and transmit with a fraction of available co-channel cells is called 'sectoring'. In a seven-cell-cluster layout with 120o sectored cells, it can be easily understood that the mobile units in a particular sector of the center cell will receive co-channel interference from only two of the first-tier co-channel base stations, rather than from all six. Likewise, the base station in the center cell will receive co-channel interference from mobile units in only two of the co-channel cells.

Hence the signal to interference ratio is now modified to

$$\frac{S}{I} = \frac{(\sqrt{3N})^n}{2} \qquad (1.5.3.1)$$

Where the denominator has been reduced from 6 to 2 to account for the reduced number of interfering sources. Now, the signal to interference ratio for a seven-cell cluster layout using 120^o sectored antennas can be found from equation (1.5.3.3) to be 23.4 dB which is a significant improvement over the Omni-directional case where the worst-case S/I is found to be 17 dB (assuming a path-loss exponent, n=4). Some cellular systems divide the cells into 60o sectors. Similar analysis can be performed on them as well. It is easy to see that the shaded region in the center receives interference from just one first-tier cell and hence the signal to interference ratio can be obtained suitably as

$$\frac{S}{I} = \frac{(\sqrt{3N})^n}{1} = \frac{(\sqrt{(3)(7)})^4}{1} = \quad 26.4dB. \quad (1.5.3.2)$$

Since the SIR exceeds 15 dB, one can try reducing the cluster size from seven to four. Now, the SIR for this reduced cluster size layout can be found to be

$$\frac{S}{I} = \frac{(\sqrt{3N})^n}{1} = \frac{(\sqrt{(3)(4)})^4}{1} = \quad 21.6dB. \quad (1.5.3.3)$$

The S/I ratio is still above the requirement and so a further reduction in the cell cluster size is possible. For a 3-cell cluster layout, there are two interfering sources and hence the S/I ratio is found to be

$$\frac{S}{I} = \frac{(\sqrt{3N})^n}{1} = \frac{(\sqrt{33})^4}{2} = \quad 16.07dB. \qquad (1.5.3.4)$$

This is just above the adequate S/I ratio and further reduction in cluster size is not possible. So, a 3-cluster cell layout could be used for meeting the growth requirements. Thus, when the cluster size is reduced from 7 to 3, the total number of channels increased by a factor of 7/3. The calculations in the above example are actually an idealization for several reasons. Firstly, practical antennas have side lobes and cannot be used to focus a transmitted beam into a perfect 120^o sector or 60^o sector. Due to this, additional interference will be introduced. Next, it is also a cause of concern that a given number of channels are not able to support as many subscribers when the pool of channels is divided into small groups. This is due to a reduction in Trunking Efficiency, a term which will be explained later on. Because sectoring involves using more than one antenna per base station, the available channels in the cell are divided and dedicated to a specific antenna. This breaks the available set of channels into smaller sets, thus reducing the trunking efficiency. Moreover, dividing a cell into sectors requires that a call in progress will have to be handed off (that is, assigned a new channel) when a mobile unit travels into a new sector. This increases the complexity of the system and also the load on the mobile switching center/base station.

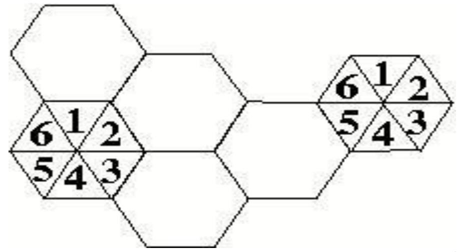

Figure 1.5.3.1: A seven-cell cluster with 60^o sectors.

Microcell Zone Concept

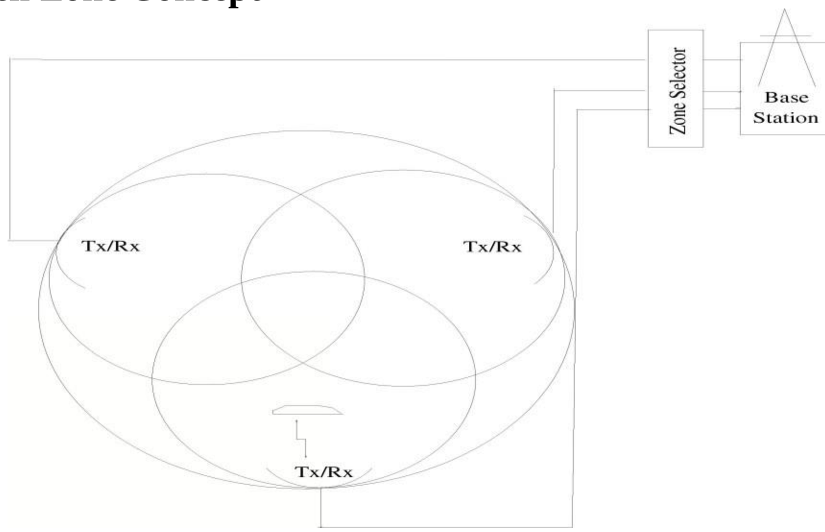

Figure 1.5.4.1: The micro-cell zone concept

The increased number of handoffs required when sectoring is employed results in an increased load on the switching and control link elements of the mobile system. To overcome this problem, a new microcell zone concept has been proposed. As shown in Figure 1.5.4.1, this scheme has a cell divided into three microcell zones, with each of the three zone sites connected to the base station and sharing the same radio equipment. It is necessary to note that all the microcell zones, within a cell, use the same frequency used by that cell; that is no handovers occur between microcells. Thus when a mobile user moves between two microcell zones of the cell, the BS simply switches the channel to a deferent zone site and no physical re-allotment of channel takes place. Locating the mobile unit within the cell: An active mobile unit sends a signal to all zone sites, which in turn send a signal to the BS. A zone selector at the BS uses that signal to select a suitable zone to serve the mobile unit - choosing the zone with the strongest signal. Base Station Signals: When a call is made to a cellular phone, the system already knows the cell location of that phone. The base station of that cell knows in which zone, within that cell, the cellular phone is located. Therefore when it receives the signal, the base station transmits it to the suitable zone site. The zone site receives the cellular signal from the base station and transmits that signal to the mobile phone after amplification. By confining the power transmitted to the mobile phone, co-channel interference is reduced between the zones and the capacity of system is increased.

Benefits of the micro-cell zone concept:

1) Interference is reduced in this case as compared to the scheme in which the cell size is reduced.

2) Handoffs are reduced (also compared to decreasing the cell size) since the microcells within the cell operate at the same frequency; no handover occurs when the mobile unit moves between the microcells.

3) Size of the zone apparatus is small. The zone site equipment being small can be mounted on the side of a building or on poles.

4) System capacity is increased. The new microcell knows where to locate the mobile unit in a particular zone of the cell and deliver the power to that zone. Since the signal power is reduced, the microcells can be closer and result in an increased system capacity.

However, in a microcellular system, the transmitted power to a mobile phone within a microcell has to be precise; too much power results in interference between microcells, while with too little power the signal might not reach the mobile phone. This is a drawback of microcellular systems, since a change in the surrounding (a new building, say, within a microcell) will require a change of the transmission power.

Advance Mobile Phone Service (AMPS)

In the late 1970's, AT & Bell Lab developed the first US cellular telephone system called AMPS. The Federal Communication Commission (FCC) was allocated a total of 40 MHz of in the 800 MHz band for AMPS.

The AMPS system Uses a Seven – Cell reuse Pattern with provisions for sectoring and cell splitting to increase capacity when needed, The AMPS is not very private. Voices are transmitted using ordinary FM and conversation can be picked up with any FM receiver that ill tine the correct frequency. For the satisfactory system performance, 30 KHz channel requires a signal to interference ratio of 18 dB.

In the United States, reverse link use of frequencies between 824 MHz-849 MHz while forward link use frequencies between 869 MHz -894 MHz. Every radio channel actually consist of a pair of simplex channels separated by 45 MHZ. For amps, the maximum deviation of the FM modulator is ± 12 KHz. The control channel transmissions and blank and burst data streams are transmitted at 10 kbps. The wide band data streams have a maximum frequency deviation of ± 8 KHz and 6.4 KHz.

The AMPS cellular system were launched by using base stations with tall towers which support several receiving antennas and have transmitting antennas which radiate a few hundred watts of effective radiated power. Each base station has one control channel transmitter, one control channel receiver and eight or more FM duplex voice channels.

The commercial base stations support as many as 57 voice channels. The Forward Voice Channels (FVCs) carry the portion of the telephone conversation originating from the landline telephone network caller and going to the cellular subscriber. The Reverse Voice Channels (RVCs) carry the portion of the telephone conversation originating from ye cellular subscriber and going to the landline telephone network caller.

Each base station continuously transmits digital FSK data on the FCC of all times so that idle cellular subscriber units can lock on to the strongest RCC wherever they are. All subscribers must be locked on to FCC in order to receive calls, the base station Reverse Control Channel (RCC) receiver constantly monitors transmission from cellular subscribers that are locked into the matching FCC.

AMPS Voice Modulation Process

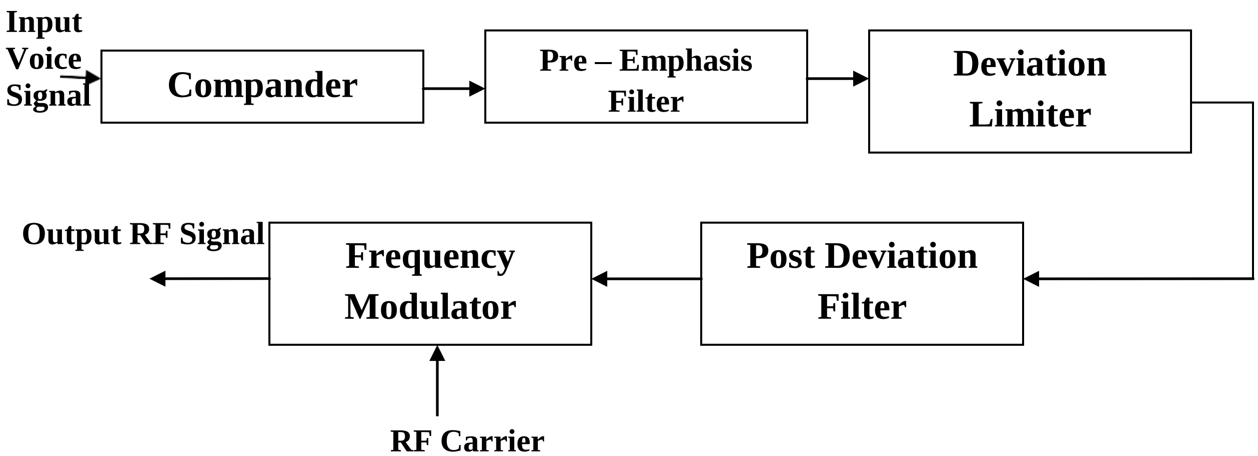

Figure 1.6.1.1: AMPS Voice modulation Process

Compander: In order to accommodate a large speech dynamic range, the input signals need to be compressed in amplitude range before Modulation. The companding is done by a 2:1 compander, which produces a 1 dB increase in output level for every 2 dB increase in input level. At the receiver, the inverse of compression is performed, thus assuming the restoral of the input voice level with a minimum of distortion.

Pre-emphasis: The output of the compressor is passed through a Pre-emphasis filter which has a nominal 6 dB/octave highpass response between 300Hz to 3 KHz.

Deviation Limiter: The deviation limiter ensures the maximum frequency deviation at the mobile station is limited to ± 12K Hz (± 10 KHz for ETACS). The supervisory signals and wide band data signals are excluded from this restriction.

Post deviation Limiter Filter: The output of deviation is filtered using a post deviation limiter filter. This is a LPF specified to have an attenuation which is greater than or equal to 40 $\log_{10}$ (f(Hz)/3000) dB in the frequemcy range between 3 KHz to 5.9 KHz and 6.1 KHz to 15 KHz. For 15 KHz and above the attenuation must be greater than 28 dB. It ensures that the 6 KHz SAT (Supervisory Audio Tone) tones, Which are always present during a call, do not interfere with the transmitted speech signal.

The AMPS use three SAT signals which are tones at frequencies of either 5970 Hz, 6000 Hz or 6030 Hz. A given BS will constantly transmit one or the three SAT tones one each voice channel while it is in use.

The SAT tone is automatically sent by the subscriber unit when a user terminates a call or turns the cellular phone off during a call. This allows the BS and the MSC to know that the call was terminated deliberately by the user, as opposed to being dropped by the system.

EIA/TIA IS – 136 DIGITAL CELLULAR SYSTEM

It is also referred to as digital AMPS (DAMPS), American Digital Cellular (ADC), or North American TDMA (NA-TDMA), IS-136, the succesor to IS-54, supports a TDMA air interface similar to that of GSM, and this considered as an evolutionary technology. It took four months to create the IS-54 specification, and no significant trial was conducted. IS-54 was renamed IS-136.

Using TDMA, every IS-136 frequency carrier supports three voice channels, where the speech coding rate is 7.95 kbps. IS-136 operate in the same spectrum with the same frequency spacing (30 KHz) used by the existing AMPS system. Thus, IS-136 capacity is around three time that of AMPS. An existing AMPS system can be easily upgraded with IS-136 on a circuit – by 0 circuit basis. In this way, the evolution from AMPS to DAMPS can be made gracefully.

IS-136 includes point to point short messaging, Broadcast messaging, group addressing, Private user Group, Hierarchical cell structures and slotted paging channels to support sleep mode in the hand set to conserve battery power.

EIA/TIA IS-95 DIGITAL CELLULAR SYSTEM

This Digital Cellular System was developed by Qualcomm, and has been operating in United States since 1996. IS-95 is based on Code Division Multiple Access (CDMA) technology. CDMA many user to share common frequency/Time channel for transmission; the user signals are distinguished by spreading them with different codes. In theory, this technology optimizes the utilization of the frequency, bandwidth by equalizing signal to signal ratio (SNR) among all the users, thereby more equitability sharing the system power resources among them. While AMPS uses that are near base station typically enjoy SNRs in excess of 80 dB, Users at the edge of cell coverage areas experience near the lower limit. With CDMA, users who are near base station transmit less power, maintaining the same SNR as users at the edge of a cell’s coverage. By utilizing the minimum necessary amount of power, system wide co- channel interference kept as minimum

IS-95 MSs may need to maintain links with two or more stations continuously during phone calls, So that, as multiple path varies, the base station with the best received signal on a burst – by – burst basis will be selected to communicate with the MS.

The channel Bandwidth used by IS-95 is 1.25 MHz This bandwidth is relatively narrow for a CDMA system, which makes a service migration from analog to digital within an existing network more difficult than at AMPS and DAMPS. In third Generation wideband CDMA proposal, the bandwidth has been extended to 5 MHz. The speech coding rate for IS-95 is 13 Kbps or 8 kbps. IS-95's capacity is estimated to be 10 times that of AMPS.

The IS-95 development has been similar to that of AMPS, but no large scale trial was conducted: it look two years to generate the specification. Prior to 1997, the most significant IS-95 development effort was taking place in Korea. In 1997, the Korean government decided to implement IS-95 technology. The Korean IS-95 system began commercial operation in April 1996.

CORDLESS TELEPHONYAND LOW TIER PCS

This section introduces cordless telephony technologies and low-tier PCS technologies.

Cordless Telephony

What is a Cordless Telephone?

Cordless telephones operate by the use of a low power radio link between handset and base station, which in turn is connected to the public telephone network.
Every effort is made to keep the regulation of cordless telephones as simple and un-bureaucratic as possible. Yet a degree of regulation is necessary in order to protect the public telephone system from being affected by incompatible apparatus and to prevent harmful radio interference.

Circumstances for License Exemption

The potential for cordless phones to cause interference to other radio users is small providing they operate under the correct technical conditions. In keeping with Ofcom's policy of light touch regulation and reduction of unnecessary burden on business, the need for licenses has been removed. Details of the current exemption requirements for cordless phones are contained in Schedule 4 to the Statutory Instrument (SI) entitled "The Wireless Telegraphy (Exemption) Regulations 2003 (SI 2003 No 074)" – as amended. Copies of the SIs are available from any Stationary Office Bookshop or from the **Office of Public Sector Information**.

CT 0

A first generation analogue cordless telephone which provides a maximum range of about 200 meters between handset and base station and is primarily designed for domestic use. This version operates in the 31 and 39 MHz frequency bands. Eight channels are available. Equipment operating on these frequencies must comply with the R&TTE Directive and the United Kingdom Interface Requirement **IR 2011**. These frequencies may be used to send and receive voice or data messages over a telecommunications system and the operation has to be on no more than one pair of frequencies during each connection.

Older CT0 cordless telephones use the frequency bands 1642 to 1782 kHz and 47 MHz or 47 MHz and 77 MHz and must conform to the EU's Radio Equipment and Telecommunications Terminal Equipment Directive 1999/5/EC (R&TTE Directive) and the

United Kingdom Interface Requirement **IR 2011**. Operation must be on not more than one of the pairs of frequencies set out below at any one time.
From 1 April 2005 it has not be permitted to bring new CT0 equipment using the frequency bands 1642 to 1782 kHz and 47 MHz or 47 MHz and 77 MHz into service. However transitional arrangements provide that equipment in use at that date may continue to be used.

Analogue Cordless Telephone Systems

Generic Standard	Current Standard	Frequencies (MHz)	Description	Status
CT0 (current)	MPT 1384	Base Tx: 31.0375 – 31.2125 MHz Mobile Tx: 39.9375 – 40.1125 MHz	Analogue FM. Frequency Division Multiple Access (FDMA). Voice only. Four two-frequency duplex channels	Retain status
CT0	MPT 1322	Base Tx: 1.642 – 1.782 kHz Mobile Tx: 47.45625 – 47.54375 MHz	Analogue FM. FDMA. Voice only. Eight two-frequency duplex channels	**Phased out from 1st April 2005**
CT0 (extended)	MPT 1371	Base Tx: 47.43125 / 47.41875 MHz Mobile Tx: 77.5125 / 77.5500 MHz	Analogue FM. Specialist product intended for agricultural use in rural areas	**Phased out from 1st April 2005**

Table 1.9.1.4 Summary of Analogue Cordless Telephony Standards & Frequencies

CT 2

These systems use digital speech and digital transmission technology thereby reducing the interference suffered by analogue CT0 equipment. The equipment must conform to the R&TTE Directive and the United Kingdom Interface Requirement **IR 2011** and operate in the frequency band 864.1 MHz to 868.1 MHz using frequency division multiple access digital technology.

Digital Cordless Telephones Systems

Generic Standard	Current Standard	Frequencies (MHz)	Description	Status
DECT	EN 300 175	Base & Mobile Tx: 1880 – 1900 MHz	Digital. 32 kB/s ADPCM voice coding. Time Division Multiple Access (TDMA) and FDMA. Supports voice and data up to 1.1 MB/s 10 RF channels; 12 voice circuits per 1728 kHz RF channel	Retain status
CT2	I-ETS 300 131 Or MPT 1334	Base & Mobile Tx: 864.1 – 868.1 MHz	Digital. 32 kB/s ADPCM voice coding. FDMA / Time Division Duplex (TDA). Supports voice and data on 40 FDM channels; 1 voice circuit per 100 kHz RF channel	**Phased out from 1st April 2005**

Table 9.1.6 Summary of Digital Cordless Telephony Standards & Frequencies

DECT (Digital Enhanced Cordless Telecommunications)

DECT is a digital cordless phone specification that was developed by ETSI (European Telecommunications Standards Institute) and operates throughout Europe in accordance with ETSI standard EN 300 175.

DECT systems may consist of one or more base stations, portable stations and repeater stations (for the purpose of this paragraph, “repeater stations” means a station which relays the voice or data message or visual image between the base station and one or more portable stations). The stations can be used to send and receive voice and data messages or visual images either directly between a base station and a portable station or between a base station and a portable station through a repeater station. The DECT system must operate within the frequency band 1880 – 1900 MHz.

DECT systems may be placed on the UK market if the equipment complies with the R&TTE Directive and the relevant United Kingdom Interface Requirement: **IR 2011**

1.10 Third Generation Wireless Networks

Third generation wireless systems will evolve from mature second generation systems. The aim of third generation wireless networks is to provide a single set of standards that can meet a wide range of wireless applications and provide universal access throughout the world.

In third generation wireless systems, the distinctions between cordless telephones and cellular telephones will disappear, and a universal personal communicator (a personal handset) will provide access to a variety of voice, data, and video communication services. Third generation systems will use the Broadband Integrated Services Digital Network (B-ISDN) to provide access to information networks, such as the Internet and other public and private databases. Third generation networks will carry many types of information (voice, data, and video), will operate in varied regions (dense or sparsely populated regions), and will serve both stationary users and vehicular users traveling at high speeds. Packet radio communications will likely be used to distribute network control while providing a reliable information transfer [Goo9O]. The terms Personal Communication System (PCS) and Personal Communication Network (PCN) are used to imply emerging third generation wireless systems for hand-held devices. Other names for PCS include Future Public Land Mobile Telecommunication Systems (FPLMTS) for worldwide use which has more recently been called International Mobile Telecommunication (IMT-2000), and Universal Mobile Telecommunication System (UMTS) for advanced mobile Personal services in Europe.

UNIT - 2

MOBILITY MANAGEMENT

Handoff

When a mobile user is engaged in conversation, the MS is connected to a BS via a radio link. If the mobile user moves coverage area of another BS, the radio link to the old BS is eventually disconnected, and a radio link to the new BS should be established to continue the conversation. This process is variously referred to as automatic link transfer, handover, or handoff.

Three strategies have been proposed to detect the need for handoff:

In mobile-controlled Handoff (MCHO), the MS continuously monitors the signals of the surrounding BSs and initiate the handoff process when some handoff criteria are met. MCHO is used in DECT and PACS.

In Network-controlled handoff (NCHO), the surrounding measure the signal from the MS, and the network initiate the handoff process when some handoff criteria are met. NCHO is used in CT-2 Plus and AMPS.

In mobile-assisted handoff (MAHO), the network asks the MS to measure the signal from surrounding BSs. The network makes the handoff decision based on reports from the MS. MAHO is used in GSM and IS-95 CDMA.

The BSs involved in handoff may be connected to the same MSC (inter cell Handoff or inter-BS handoff) or two different MSCs (inter system Handoff or inter MSC handoff)

Inter-BS Handoff

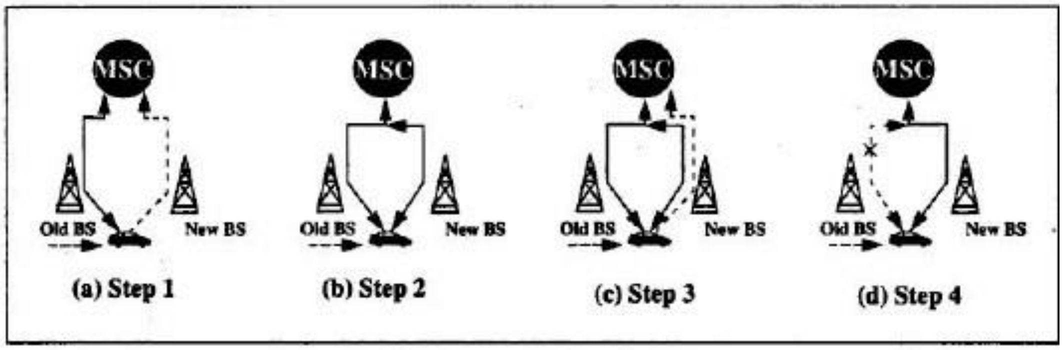

Figure 2.1.1.1 Inter-BS link Transfer

In inter-BS handoff, the new and the old BSs are connected to the same MSC. Assume that the need for handoff is detected by the MS; the following actions are taken:

1. The MS momentarily suspends conversation and initiates the handoff procedure by signaling on an idle (currently free) channel in the new BS. Then it resumes the conversation on the old BS
2. Upon receipt of the signal, the MSC transfers the encryption information to the selected idle channel of the new BS and set up the new conversation path to the MS through that channel. The switch bridges the new path with the old path and informs the MS transfer from the old channel to the new channel.
3. After the MS has been transferred to the mew BS, it signals the network, and resumes conversation using the new channel.
4. Upon receipt the handoff completion signal, the network removes the bridge from the path and releases resources associated with the old channel.

This Handoff Procedure is used with the mobile –controlled handoff strategy. For the network-controlled handoff strategy, all handoff signaling message is exchanged between the MS and the old BS through the failing link. The whole process must be completed as quickly as possible, to ensure that the new link is established before the old link fails.

If the new BS does have an idle channel, the handoff may be dropped (or force to terminate). The forced termination is probability is an important criterion in the performance evaluation of a PCS network. Forced termination of an ongoing call is considered less desirable than blocking a new call attempt.

Most PCS networks handle a handoff in the same manner as a new call attempt. That is, if no channel is available, the handoff is blocked and the call is held on the current channel in the old cell until the call is completed or the failing link is no longer available. This is referred as the non prioritized scheme. To reduce forced termination and to promote call completion, three channel assignment schemes have been proposed:

Reserved Channel Scheme. Similar to the non prioritized scheme, except that some channels in each BS are reserved for handoff calls.

Queuing priority scheme. Based on the fact that adjacent coverage areas of BSs overlap. Thus**,** there is a considerable area where a call can be handled by either BS. This area is called the handoff area. If no channel is available in the new BS during handoff, the new BS buffers the handoff request in a waiting queue. The MS continues to use the channel with the old BS until either a channel in the new BS becomes available (or handoff is connected) or the MS moves out the handoff area (and the call is forced to terminate).

Subrating Scheme. Creates a new channel for a handoff call by sharing resources with an existing call if no channel if no channel is available in the new Bs. Subtrating means an occupied full-rate channel is temporarily divided in to two channels at the half the original rate: one to serve the existing call and the other to serve the handoff request. When occupied channels are released, the subrated channels are immediately switched back to full-rate channels.

Intersystem Handoff

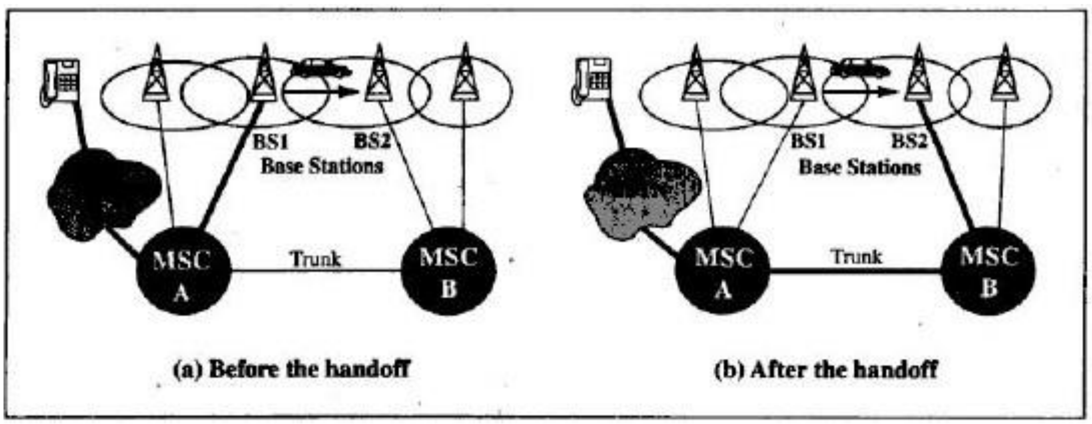

Figure 2.1.2.1 Intersystem handoff

In intersystem handoff, the new and old BSs are connected to two different MSCs. In the description that follows, we trace the intersystem handoff procedure of IS-41, where network-controlled handoff is assumed above figure illustrates the trunk connection before and after the intersystem handoff. In this figure, a communicating mobile user moves out of the BS served by MSC A and entered the area covered by MSC B. Intersystem handoff requires the following steps:

1. MSC A requests MSC B to perform handoff measurements on the call in progress. MSC B then selects a candidate BS, BS2 and interrogates it for signal quality parameters on the call in progress. MSC B returns the signal quality parameter values, along with other relevant information, to MSC A.

2. MSC A checks if the MS has made too many handoff recently (this to avoid, for example, numerous handoffs between BS1 and BS2 where the MS is moving within the overlapped area) or if intersystem trunks are not available. If so, MSC A exists the procedure. Otherwise, MSC A asks MSC B to set up a voice channel. Assuming that the voice channel is available in BS@, MSC B instructs MSC A to start the radio link transfer.
3. MSC A sends the MS a handoff order. The MS synchronous to BS2. After the MS is connected to BS2, MSC B informs MSC A that the handoff is successful. MSC A then connects the call path (trunk) to MSC B and completes the handoff procedure.

Roaming Management

Two basic operations in roaming management are

- **registration (or location update)**, the process whereby an MS informs the system of its current location, and
- **location tracking**, the process during which the system locates the MS. Location tracking is required when the network attempts to deliver a call to the mobile user.

The roaming management strategies proposed in the IS-41 and GSM MAP standards are two-level strategies in that they use a two-tier system of **home** and **visited databases**.

Home Location Register (HLR)

- When a user subscribes to the services of a PCS network, a record is created in the system's database, called the **home location register (HLR)**.
- This is referred to as the home system of the mobile user.
- The HLR is a network database that stores and manages all mobile subscriptions of a specific operator.
- Specifically, the HLR is the location register to which an MS identity is assigned for record purposes, such as directory number, profile information, current location, and validation period.

Visitor Location Register (VLR)

- When the mobile user visits a PCS network other than the home system, a temporary record for the mobile user is created in the visitor location register (VLR) of the visited system.
- The VLR temporarily stores subscription information for the visiting subscribers so that the corresponding MSC can provide service.
- In other words, the VLR is the "other" location register used to retrieve information for handling calls to or from a visiting mobile user.

Registration Procedure

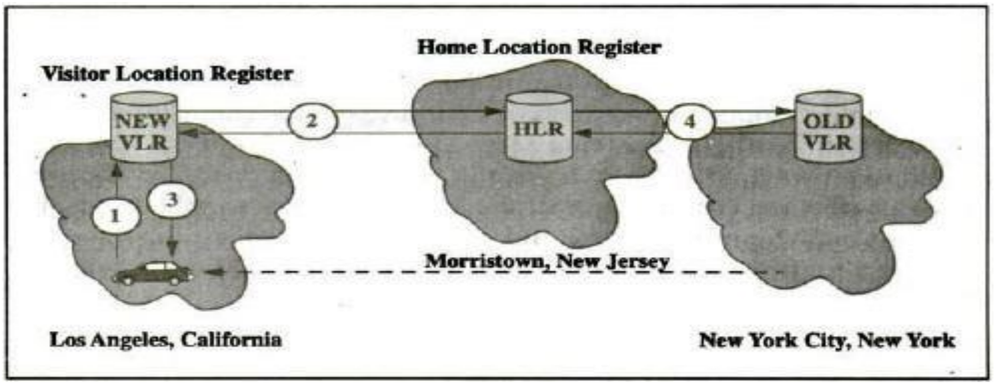

Figure 2.2.1 Registration Procedure

- Step 1. Suppose that the home system of a mobile user is in Morristown. When the mobile user moves from one visited system (e.g., New York City) to another (e.g., Los Angeles), it must register in the VLR of the new visited system.
- Step 2. The new VLR informs the mobile user's HLR of the person's current location-the address of the new VLR. The HLR sends an acknowledgment, which includes the MS's profile, to the new VLR.
- Step 3. The new VLR informs the MS of the successful registration.
- Step 4. After step 2, the HLR also sends a **deregistration message** to cancel the obsolete location record of the MS in the old VLR. The old VLR acknowledges the deregistration.

Call delivery procedure

- To originate a call, the MS first contacts the MSC in the visited PCS network.
- The call request is forwarded to the VLR for approval.
- If the call is accepted, the MSC sets up the call to the called party following the standard PSTN call setup procedure.
- **Step 1**. If a wireline phone attempts to call a mobile subscriber, the call is forwarded to a switch, called the **originating switch** in the PSTN, which queries the HLR to find the current VLR of the MS. (1) The HLR queries the VLR in which the MS resides to get a routable address. (2) If the originating switch is not capable of querying the HLR (i.e., it is not equipped to support mobility), the call is routed through the PSTN to the subscriber's gateway MSC, which queries the HLR to determine the current VLR serving the MS.

- **Step 2.** The VLR returns the routable address to the originating switch through the HLR.
- **Step 3**. Based on the routable address, a trunk (voice circuit) is set up from the originating switch to the MS through the visited MSC.

Roaming Management under SS7

- The missing parts in the picture are the interactions between the PCS network and the PSTN.
- This section briefly describes how mobile roaming is managed by the PSTN signaling.

Common channel signaling (CCS)

- Common channel signaling (CCS) is a signaling method that provides control and management functions in the telephone network.
- CCS consists of
  - supervisory functions,
  - addressing, and
  - Call information provisioning.
- A CCS channel conveys messages to
  - initiate and terminate calls;
  - determines the status of some part of the network; and
  - Controls the amount of traffic allowed.
- CCS uses a separate **out-of-band signaling** network to carry signaling messages.
- Signaling System No. 7 (SS7) is a CCS system developed to satisfy the telephone operating companies' requirements for an improvement to the earlier signaling systems, which lacked the sophistication required to deliver much more than plain old telephone service (POTS).
- Signaling between a PCS network and the PSTN are typically achieved by the SS7 network.

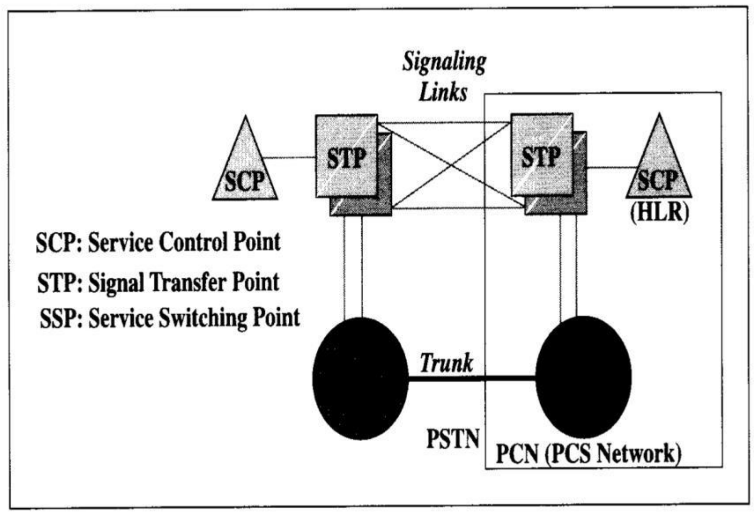

Figure 2.2.1.1 Interconnection between PCS network and PSTN

- Figure 2.2.1.1 shows the network elements that are involved in the interconnection between a PCS network and the PSTN. In the figure, the dashed lines represent the signaling links; the solid line represents a trunk.
- The SS7 network consists of three distinct components:
  - **Service Switching Point (SSP).**
  - **Signal Transfer Point (STP).**
  - **Service Control Point (SCP).**

Service Switching Point (SSP)

- A telephone switch interconnected by SS7 links. The SSPs perform call processing on calls that originate, tandem, or terminate at that node.
- A local SSP in the PSTN can be a central office (CO) or end office (EO).
- An SSP in a PCS network is called a mobile switching center (**MSC**).

Signal Transfer Point (STP)

- A switch that relays SS7 messages between network switches and databases. Based on the address fields of the SS7 messages, the STPs route the messages to the correct out-going signaling links. To meet the stringent reliability requirements, STPs are provisioned in mated pairs, as shown in Figure 2.7.

Service Control Point (SCP).

- Contains databases for providing enhanced services. An SCP accepts queries from an SSP and returns the requested information to the SSP .
- In mobile applications, an SCP may contain an HLR or a VLR.

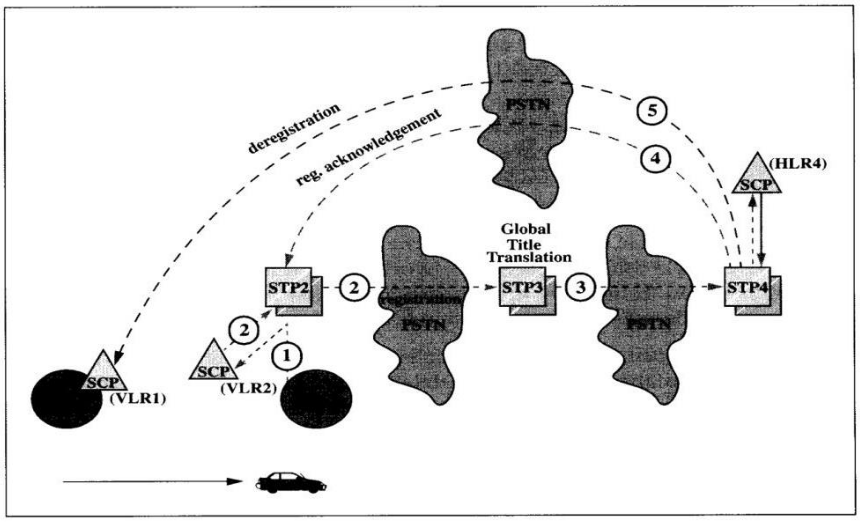

Figure 2.2.1.2

Registration

- In this example, the MS moves from VLR1 to VLR2.
- Step 1.
    - The MS enters the area controlled by MSC2.
    - MSC2 launches a registration query to its VLR through STP2, assuming that VLR2 and MSC2 are not co-located.
- Step 2.
    - VLR2 sends a registration message to the MS's HLR (HLR4 in Figure 2.8).
    - VLR2 may not know the actual address of HLR. Instead, VLR2 sends the message containing the MS identity, called the **Mobile Identification Number (MIN)**, to an **STP (STP3** in our example) that can translate the MIN into the HLR address.

- Step 3.
    - The MIN-to-HLR address translation is performed at STP3 by a table-lookup technique called **global title translation (GTT)**. STP3 then forwards the registration message to HLR.
- Step 4.
    - After the registration, HLR sends an acknowledgment back to VLR2.
    - Since the address of VLR2 is known, the acknowledgment may be sent to VLR2 using a shortcut, without passing through STP3.
- Step 5.
    - After step 3, HLR sends a deregistration message to VLR1 to cancel the obsolete record.
    - VLR1 then acknowledges the cancellation (not shown in Figure 2.8).

Implicit deregistration

- Obsolete VLR records are not deleted until the database is full.
- If the database is full when an MS arrives, a record is deleted, freeing storage space to accommodate the newly arrived MS.
- A replacement policy is required to select a record for replacement (it is possible that a valid record is replaced, and the information is lost).
- Advantage: no deregistration messages are sent among the SS7 network elements.

Periodic re-registration

- The MS periodically reregisters to the VLR.
- If the VLR does not receive the re-registration message within a timeout period, the record is deleted.
- This approach only creates local message traffic between the MSC and the VLR. Furthermore, no SS7 signaling messages are generated if the VLR is co-located with the MSC.

Pointer Forwarding Scheme

- To reduce the registration traffic at steps 2 and 3 in Figure 2.1.3, a **pointer forwarding scheme** was proposed, which consists of two operations:
- Move operation (registration).
- Find operation (call delivery).

Move operation (registration)

- When an MS moves from one VLR to another, **a pointer** is created from the old VLR to the new VLR. No registration to the HLR is required (see Figure 2.1.3(a)).

Find operation (call delivery)

- When the HLR attempts to locate the MS for call delivery, the pointer chain is traced. After the find operation, the HLR points directly to the destination VLR (see Figure 2.1.3 (b)).

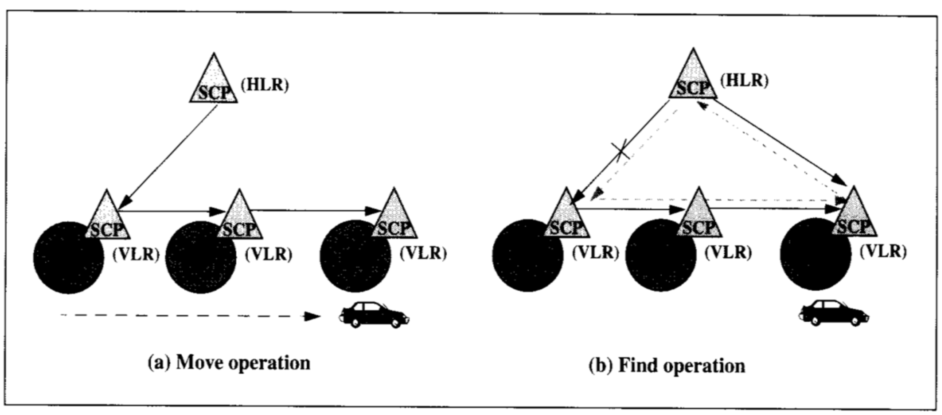

Figure 2.2.1.3 Pointer forwarding Scheme

- Depending on the memory capacities of the VLRs, the pointers in the obsolete chain may or may not be deleted.
- To limit the pointer traversal time in the find operation, the registration procedure in Figure 2.2.1.2 may be performed for every k move operations.
- In other words, the number of pointers visited in the find operation will be limited by k. The pointer forwarding scheme should not be considered when the net cost of pointer creation and pointer traversal is higher than the cost of accessing the HLR.
- As performance studies indicate, the pointer forwarding scheme significantly reduces the network traffic in many cases.

Call Delivery

- Similar to the registration process, visits to several STPs and a GTT may be required to access the HLR in call delivery.
- Several STPs may be visited to obtain the routable address from the VLR.
- To reduce the call delivery traffic, a cache scheme was proposed to maintain a cache in the originating SSPs.
- Another possibility is to maintain the cache in the STP that performs GTTs, that is, STP3 in Figure 2.2.1.5.
- A cache entry consists of two fields: the **MIN of an MS** and **the address of the current visited VLR of the MS**. The cache contains entries for MSs recently accessed from the SSP

Cache Scheme

- When the calling party originates a call to an MS, the SSP first checks if the cache entry for the MS exists. There are three possibilities:
- Case 1: The cache entry does not exist. The call delivery procedure illustrated in Figure 2.2.1.4 is performed.
- Case 2: The cache entry exists and is current. The VLR is directly accessed as shown in Figure 2.2.1.5.
- Case 3: The cache entry exists but is obsolete. The procedure detects that the cache entry is obsolete if the queried VLR's response is negative. The call deliiverv procedure illustrated in Figure 2.2.1.5 is performed.

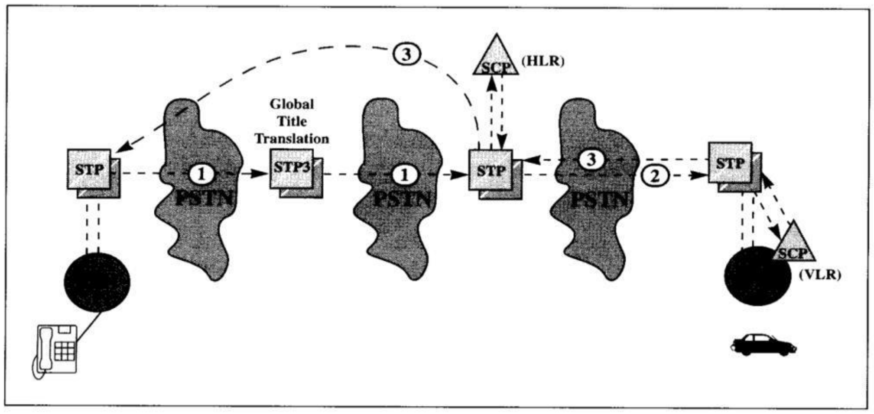

Figure 2.2.1.4 Call delivery through SS7

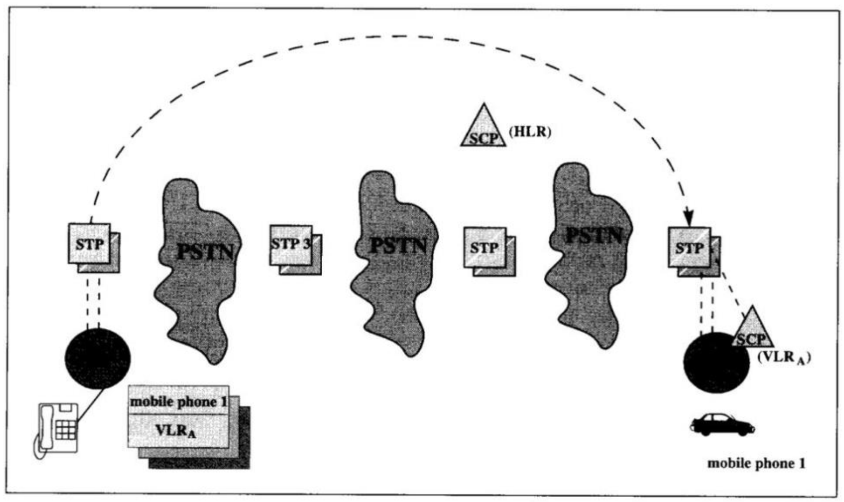

Figure 2.2.1.5 cache Scheme

- Note that implicit deregistration and periodic re-registration can be used with the cache scheme, but the obsolete cache information may not be detected until the MS is paged.
- Since the cache information may be obsolete, some heuristics are required to determine whether the cached information will be used to locate the MS.
- One technique is to have the SSP estimate the cache hit ratio, or the probability that case 2 is true.
- If the probability is high, the entry is considered "current" and is enabled; otherwise, the entry is disabled.
- Another heuristic determines the obsoleteness of an entry based on the period that an MS resides in a VLR as indicated in the cache entry.

- If the cache entry indicates that the MS has stayed in a VLR for a period longer than a specified threshold, the entry is assumed to be obsolete.
- The threshold can be adjusted in real time based on cache hit statistics. If case 3 is more likely to occur than case 2, then the cache scheme should not be considered.
- Performance studies indicate that the cache scheme significantly reduces the call delivery cost in many cases.

Roaming Management for CT2

- In a public environment, CT2 is a one-way calling PCS system; that is, a CT2 handset can originate outgoing calls, but cannot receive incoming calls.
- We describe how to construct two-way calling mechanism into CT2. As we will demonstrate later, introducing roaming management for CT2 is expensive.
- Nevertheless, this introduction provides a model so that the reader can understand the design complexity required to implement a total mobility solution for an one-way PCS system.

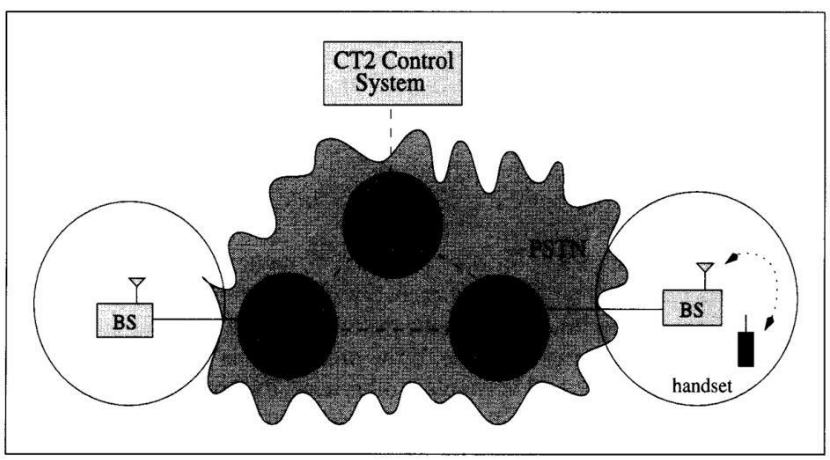

Figure 2.2.1 CT2 system

Basic Public CT2 System (One-Way Calling)

- The original public CT2 system was designed as a tele-point service, and did not support call delivery.
- CT2 BS is connected directly to a switch in the PSTN.
- The **CT2 control system** is responsible for monitoring and billing, which may be connected indirectly to the BSs through the PSTN.

- The messages between the CT2 control system and the BSs are delivered through the PSTN.
- CT2 system can provide only the **call origination service**. It is impossible to provide call delivery service as in cellular systems such as DAMPS and GSM.
- Some CT2 systems (e.g., the systems in Hong Kong) utilized the paging system to provide call delivery; thus, when a wireline user A wanted to call a CT2 user B, A would first page B through the paging system.
- From the paging message, B identified B the telephone number of A, then dialed back to A through the CT2 system.
- Advantage: no modifications are made to the CT2 architecture.
- Disadvantage:
    - the inconvenience caused by the involvement of the paging system, and thus for the reverse charging.
    - Also, if both A and B use CT2 handsets in different CT2 systems, it is impossible to connect the call.

Meet-at-a-Junction CT2 System (Two-Way Calling)

- An advanced CT2 system may follow the "**meet-at-a-junction**" approach to provide the call delivery capability.
    - The CT2 architecture for this approach is illustrated in Figure 2.2.2.
    - In this approach, the CT2 service area is partitioned into several location areas.
    - All BSs in the same location area are connected to an area controller.
    - Through the Public Switched Data Network (PSDN) all area controllers are connected to the database, called the **location register**.

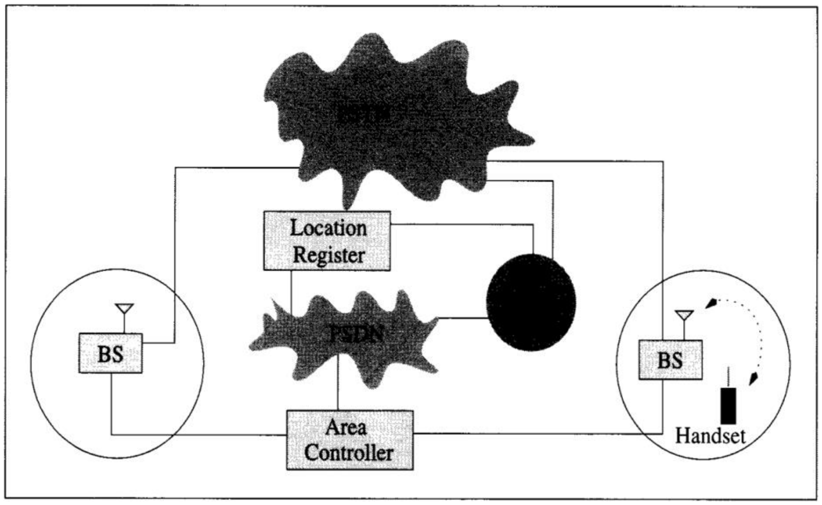

Figure 2.2.2 Meet at a junction Procedure

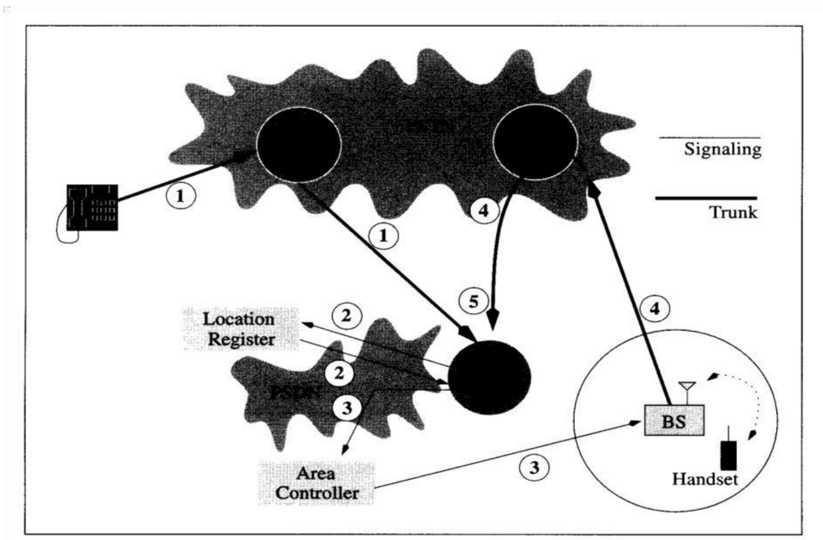

Figure 2.2.3 Call Delivery Procedure

Call Delivery Procedure

- A handset will **register** at the location register after it enters a location area.
- A location record for the handset is created in the location register, which indicates the location area-the address of the corresponding area controller, where the handset resides.
- From the registration list of the location register, the BSs poll the handsets periodically. If the polled handset does not reply, the CT2 system assumes that the handset has left the location area and the handset's location record is deleted.

- If a handset does not receive the polling message for a long time, for example, when the handset moves to a new location area and the movement is not known by the location register, the handset reregisters to reclaim its existence.
- **Two dials** are required in the call delivery procedure,
  - one from the originating switch to S1 and
  - the other from the BS to S1.
- The CT2 modifications for two-way calling services have been considered expensive.
  - In Taiwan, for example, a CT2 call delivery was considered as two phone calls.
  - The CT2 services in Hong Kong were terminated in 1996. In the same year, many European countries replaced CT2 by DECT as the standard cordless technology.
  - In Taiwan, the bandwidth for CT2 was reclaimed for PACS and PHS in 2000.

HANDOFF DETECTION

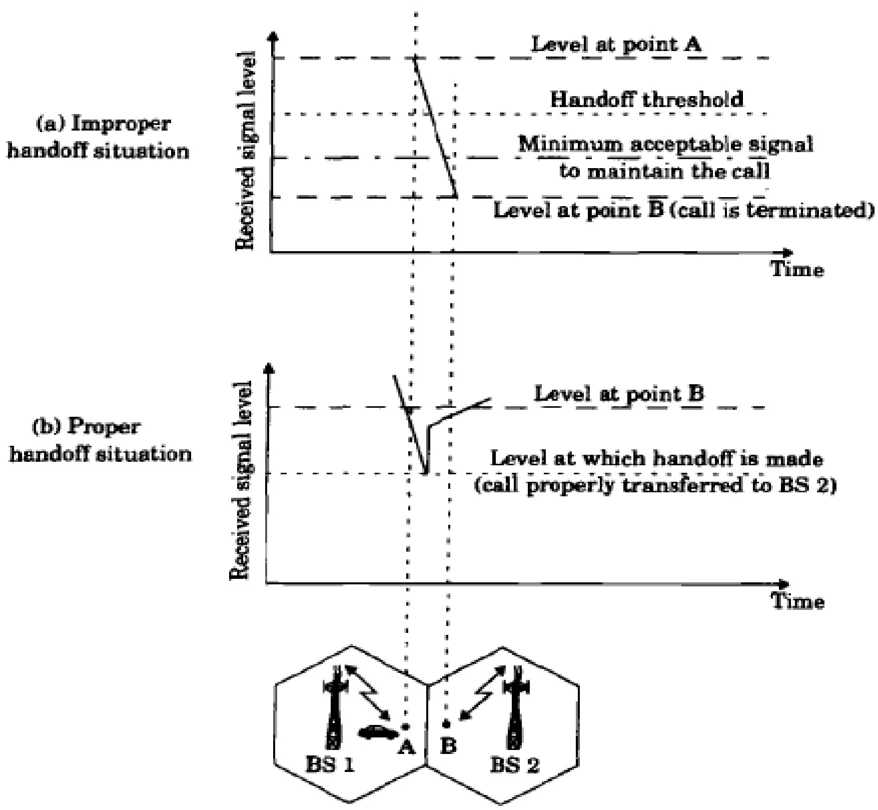

Figure 2.3.1 Handoff strategies

When a mobile moves into a different cell while a conversation is in progress, the MSC automatically transfers the call to a new channel belonging to the new base station. This handoff operation not only involves identifying a new base station, but also requires that the voice and control signals be allocated to channels associated with the new base station. Processing handoffs is an important task in any cellular radio system. Many handoff strategies prioritize handoff requests over call initiation requests when allocating unused channels in a cell site. Handoffs must be performed successfully and as infrequently as possible, and be imperceptible to the users. In order to meet these requirements, system designers must specify an optimum signal level at which to initiate a handoff. Once a particular signal level is specified as the minimum usable signal for acceptable voice quality at the base station receiver (normally taken as between —90 dBm and —100 dBm), a slightly stronger signal level is used as a threshold at which a handoff is made. This margin, given by $\Delta = P_{Handoff} - P_{minimum\ usable}$' cannot be too large or too small. If A is too large, unnecessary handoffs which burden the MSC may occur, and if Δ is too small, there may be insufficient time to complete a handoff before a call is lost due to weak signal conditions. Therefore, Δ is chosen carefully to meet these conflicting requirements. Figure 3.1 illustrates a handoff situation. Figure 3.1 (a) demonstrates the case where a handoff is not made and the signal drops below the minimum acceptable level to keep the channel active. This dropped call event can happen when there is an excessive delay by the MSC in assigning a handoff, or when the threshold Δ is set too small for the handoff time in the system. Excessive delays may occur during high traffic conditions due to computational loading at the MSC or due to the fact that no channels are available on any of the nearby base stations (thus forcing the MSC to wait until a channel in a nearby cell becomes free). In deciding when to handoff, it is important to ensure that the drop in the measured signal level is not due to momentary fading and that the mobile is actually moving away from the serving base station. In order to ensure this, the base station monitors the signal level for a certain period of time before a handoff is initiated. This running average measurement of signal strength should be optimized so that unnecessary handoffs are avoided, while ensuring' that necessary handoffs are completed before a call is terminated due to poor signal level. The length of time needed to decide if a handoff is necessary depends on the speed at which the vehicle is moving. If the slope of the short-term average received signal level in a given time interval is steep, the handoff should be made quickly. Information about the vehicle speed, which can be useful in handoff decisions, can also be computed from the statistics of the received short-term fading signal at the base station. The time over which a call may be maintained within a cell, without handoff, is called the dwell time The dwell time of a particular user is governed by a number of factors, which include propagation, interference, distance between the subscriber and the base station, and other time varying effects.

In first generation analog cellular systems, signal strength measurements are made by the base stations and supervised by the MSC. Each base station constantly monitors the signal strengths of all of its reverse voice channels to determine the relative location of each mobile user with respect to the base station tower. In addition to measuring the RSSI of calls in progress within the cell, a spare receiver in each base station, called the locator receiver, is used to determine signal strengths of mobile users which are in neighboring cells. The locator receiver is controlled by the MSC and is used to monitor the signal strength of users in neighboring cells which appear to be in need of handoff and reports all RSSI values to the MSC. Based on the locator receiver signal strength information from each base station, the MSC decides if a handoff is necessary or not.

In second generation systems that use digital TDMA technology, handoff decisions are mobile assisted. In mobile assisted handoff (MAHO), every mobile station measures the received power from surrounding base stations and continually reports the results of these measurements to the serving base station. A handoff is initiated when the power received from the base station of a neighboring cell begins to exceed the power received from the current base station by a certain level or for a certain period of time. The MAHO method enables the call to be handed over between base stations at a much faster rate than in first generation analog systems since the handoff measurements are made by each mobile, and the MSC no longer constantly monitors signal strengths. MAHO is particularly suited for microcellular environment its where handoffs are more frequent. During the course of a call, if a mobile moves from one cellular system to a different cellular system controlled by a different MSC, an intersystem handoff becomes necessary An MSC engages in an intersystem handoff when a mobile signal becomes weak in a given cell and the MSC cannot find another cell within its system to which it can transfer the call in progress. There are many issues that must be addressed when implementing an intersystem handoff. For instance, a local call may become a long-distance call as the mobile moves out of its home system and becomes a roamer in a neighboring system. Also, compatibility between the two MSCs must be determined before implementing an intersystem handoff. Chapter 9 demonstrates how intersystem handoffs are implemented in practice. Different systems have different policies and methods for managing handoff requests. Some systems handle handoff requests in the same way they handle originating calls. In such systems, the probability that a handoff request will not be served by a new base station is equal to the blocking probability of incoming calls. However, from the user's point of view, having a call abruptly terminated while in the middle of a conversation is more annoying than being blocked occasionally on a new call attempt. To improve the quality of service as perceived by the users, various methods have been devised to prioritize handoff requests over call initiation requests when allocating voice channels.

Prioritizing Handoffs

One method for giving priority to handoffs is called the guard channel concept, whereby a fraction of the total available channels in a cell is reserved exclusively for handoff requests from ongoing calls which may be handed off into the cell. This method has the disadvantage of reducing the total carried traffic, as fewer channels are allocated to originating calls. Guard channels, however, offer efficient spectrum utilization when dynamic channel assignment strategies, which minimize the number of required guard channels by efficient demand based allocation, are used. Queuing of handoff requests is another method to decrease the probability of forced termination of a call due to lack of available channels. There is a tradeoff between the decrease in probability of forced termination and total carried traffic. Queuing of handoffs is possible due to the fact that there is a finite time interval between the time the received signal level drops below the handoff threshold and the time the call is terminated due to insufficient signal level. The delay time and size of the queue is determined from the traffic pattern of the particular service area. It should be noted that queuing does not guarantee a zero probability of forced termination, since large delays will cause the received signal level to drop below the minimum required level to maintain communication and hence lead to forced termination.

Practical Handoff Considerations

In practical cellular systems, several problems arise when attempting to design for a wide range of mobile velocities. High speed vehicles pass through the coverage region of a cell within a matter of seconds, whereas pedestrian users may never need a handoff during a call. Particularly with the addition of microcells to provide capacity, the MSC can quickly become burdened if high speed users are constantly being passed between very small cells. Several schemes have been devised to handle the simultaneous traffic of high speed and low speed users while minimizing the handoff intervention from the MSC. Another practical limitation is the ability to obtain new cell sites. Although the cellular concept clearly provides additional capacity through the addition of cell sites, in practice it is difficult for cellular service providers to obtain new physical cell site locations in urban areas. Zoning laws, ordinances, and other nontechnical bathers often make it more attractive for a cellular provider to install additional channels and base stations at the same physical location of an existing cell, rather than find new site locations. By using different antenna heights (often on the same building or tower) and different power levels, it is possible to provide "large" and "small" cells which are co-located at a single location. This technique is called the umbrella cell approach and is used to provide large area coverage to high speed users while providing small area coverage to users traveling at low speeds. Figure 3.2 illustrates an umbrella cell which is co-located with some smaller microcells. The umbrella cell approach ensures that the number of handoffs is minimized for high speed users and provides additional microcell channels for pedestrian users. The speed of each user may be estimated by the base station or MSC by evaluating how rapidly the short term average signal strength on the RVC changes over time, or more sophisticated algorithms may be used to evaluate and partition users. If a high speed user in the large umbrella cell is approaching the base station, and its velocity is rapidly decreasing, the base station may decide to hand the user into the co-located microcell, without MSC intervention.

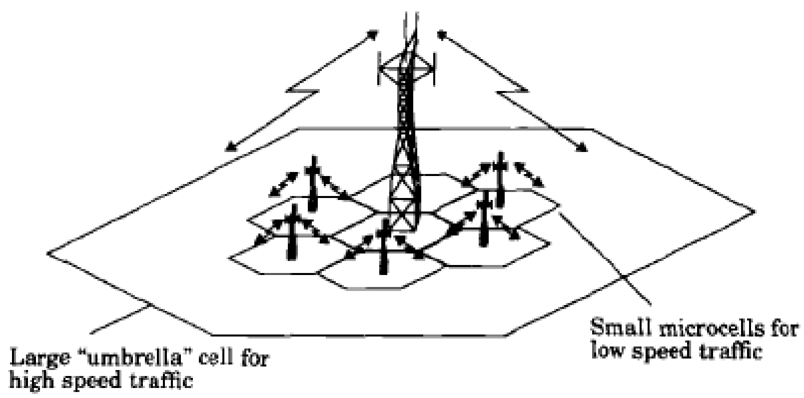

Figure 2.3.2 Umbrella approach

Another practical handoff problem in microcell systems is known as cell dragging. Cell dragging results from pedestrian users that provide a very strong signal to the base station. Such a situation occurs in an urban environment when there is a line-of-sight (LOS) radio path between the subscriber and the base station. As the user travels away from the base station at a very slow speed, the average signal strength does not decay rapidly. Even when the user has traveled well beyond the designed range of the cell, the received signal at the base station may be above the handoff threshold, thus a handoff may not be made.

This creates a potential interference and traffic management problem, since the user has meanwhile traveled deep within a neighboring cell. Thus solve the cell dragging problem, handoff thresholds and radio coverage parameters must be adjusted carefully.

In first generation analog cellular systems, the typical time to make a handoff, once the signal level is deemed to be below the handoff threshold, is about 10 seconds. This requires that the value for Δ to be on the order of 6 dB to 12 dB. In new digital cellular systems such as GSM, the mobile assists with the handoff procedure by determining the best handoff candidates, and the handoff, once the decision is made, typically requires only 1 or 2 seconds. Consequently, Δ is usually between 0 dB and 6 dB in modem cellular systems. The faster handoff process supports a much greater range of options for handling high speed and low speed users and provides the MSC with substantial time to "rescue" a call that is in need of handoff. Another feature of newer cellular systems is the ability to make handoff decisions based on a wide range of metrics other than signal strength. The co channel and adjacent channel interference levels may be measured at the base station or the mobile, and this information may be used with conventional signal strength data to provide a multi-dimensional algorithm for determining when a handoff is needed.

The IS-95 code division multiple access (CDMA) spread spectrum cellular system, provides a unique handoff capability that cannot be provided with other wireless systems. Unlike channelized wireless systems that assign different radio channels during a handoff (called a hard handoff), spread spectrum mobiles share the same channel in every cell. Thus, the term handoff does not mean a physical change in the assigned channel, but rather that a different base station handles the radio communication task. By simultaneously evaluating the received signals from a single subscriber at several neighboring base stations, the MSC may actually decide which version of the user's signal is best at any moment in time. This technique exploits macroscopic space diversity provided by the different physical locations of the base stations and allows the MSC to make a "soft" decision as to which version of the user's signal to pass along to the PSTN at any instance. The ability to select between the instantaneous received signals from a variety of base stations is called soft Handoff.

Channel Assignment techniques

For efficient utilization of the radio spectrum, a frequency reuse scheme that is consistent with the objectives of increasing capacity and minimizing interference is required. A variety of channel assignment strategies have been developed to achieve these objectives. Channel assignment strategies can be classified as either fixed or dynamic. The choice of channel assignment strategy impacts the performance of the system, particularly as to how calls are managed when a mobile user is handed off from one cell to another.

In a fixed channel assignment strategy; each cell is allocated a predetermined set of voice channels. Any call attempt within the cell can only be served by the unused channels in that particular cell. If all the channels in that cell are occupied, the call is blocked and the subscriber does not receive service. Several variations of the fixed assignment strategy exist. In one approach, called the borrowing strategy, a cell is allowed to borrow channels from a neighboring cell if all of its own channels are already occupied. The mobile switching center (MSC) supervises such borrowing procedures and ensures that the borrowing of a channel does not disrupt or interfere with any of the calls in progress in the donor cell.

In a dynamic channel assignment strategy, voice channels are not allocated to different cells permanently. Instead, each time a call request is made, the serving base station requests a channel from the MSC. The switch then allocates a channel to the requested cell following an algorithm that takes into account the likelihood of fixture blocking within the cell, the frequency of use of the candidate channel, the reuse distance of the channel, and other cost functions. Accordingly, the MSC only allocates a given frequency if that frequency is not presently in use in the cell or any other cell which falls within the minimum restricted distance of frequency reuse to avoid co-channel interference. Dynamic channel assignment reduces the likelihood of blocking, which increases the trunking capacity of the system, since all the available channels in a market are accessible to all of the cells. Dynamic channel assignment strategies require the MSC to collect real-time data on channel occupancy, traffic distribution, arid radio signal strength indications (RSSI) of all channels on a continuous basis. This increases the storage and computational load on the system but provides the advantage of increased channel utilization and decreased probability of a blocked call.

Radio link transfer IS-41 Network signaling

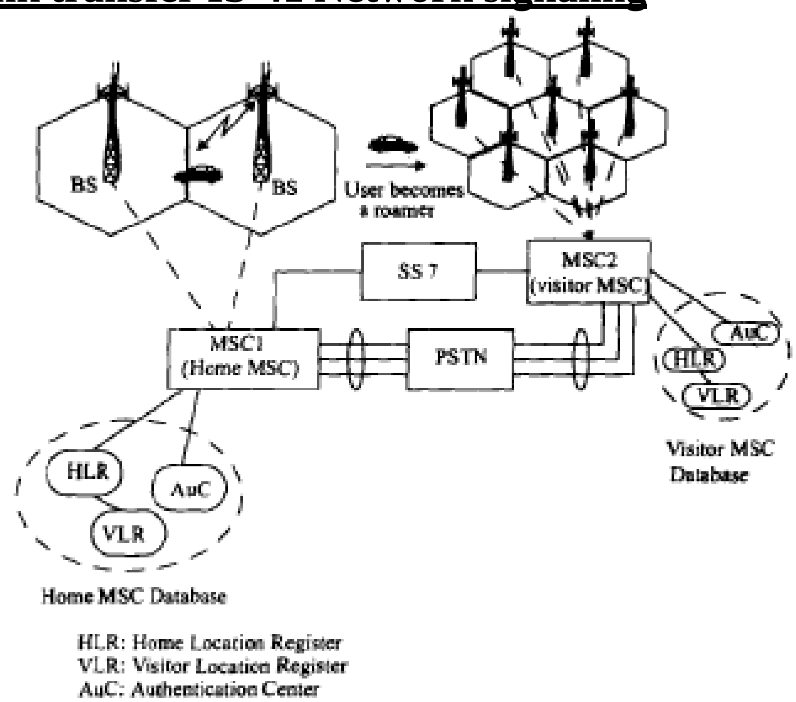

Figure 2.5.1 Block diagram of Cellular network

Until the early 1990s, U.S. cellular customers that roamed between different cellular systems had to register manually each time they entered a new market during long distance travel. This required the user to call an operator to request registration. In the early 1990s, U.S. cellular carriers implemented the network protocol standard 15-41 to allow different cellular systems to automatically accommodate subscribers who roam into their coverage region. This is called inter operator roaming. IS-41 allows MSCs of different service providers to pass information about their subscribers to, other MSCs on demand. IS-41 relies on a feature of AMPS called autonomous registration. Autonomous registration is a process by which a mobile notifies a serving MSC of its presence and location.

The mobile accomplishes this by periodically keying up and transmitting its identity information, which allows the MSC to constantly update its customer list. The registration command is sent in the aver head message of each control channel at five or ten minute intervals, and includes a timer value which each mobile uses to determine the precise time at which it should respond to the serving base station with a registration transmission. Each mobile reports its MIN and ESN during the brief registration transmission so that the MSC can validate and update the customer list within the market. The MSC is able to distinguish home users from roaming users based on the MIN of each active user, and maintains a real-time user list in the home location. Register (HLE) and visitor location register (VLR) as shown in Figure 2.5.1. 15-41allows the MSCs of neighboring systems to automatically handle the registration and location validation of roamers so that users no longer need to manually register as they travel. The visited system creates a VLR record for each new roamer and notifies the home system via IS-41 so it can update its own HLR.

Intersystem handoff and Authentication

Intersystem Handoff

– Handoff between two radio channels that are controlled by two different MSCs

Issues Associated with Intersystem Handoff

– Coordinating cell identification between neighboring MSCs
– Coordinating inter-MSC facility identification between neighboring MSCs
– Supporting MS characteristics after handoff
– Limiting the length of "handoff chain"

Intersystem Handoff Functions

– Handoff measurement
– Handoff forward
– Handoff back
– Path minimization
– Path minimization

Handoff Management

Handoff Measurement Functions

– Identify the need
– Identify the candidates
– Evaluate the candidates
– Select a target

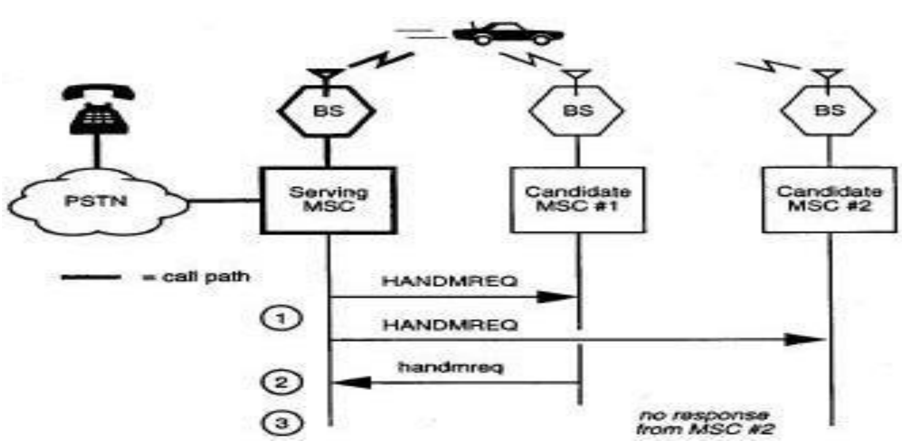

Figure 2.6.1 Example of Handoff Measurement Processes

1. The serving MSC requests handoff measurements from both candidate MSC1 and candidate MSC2.
2. Candidate MSC1 returns measurement information.
   Candidate MSC2 measures an unacceptable signal quality level, so does not respond.

Handoff Forward

Handoff Forward Functions

– Move the MS from the serving MSC to the target MSC

– Maintain a call path by establishing a circuit between serving MSC and target MSC

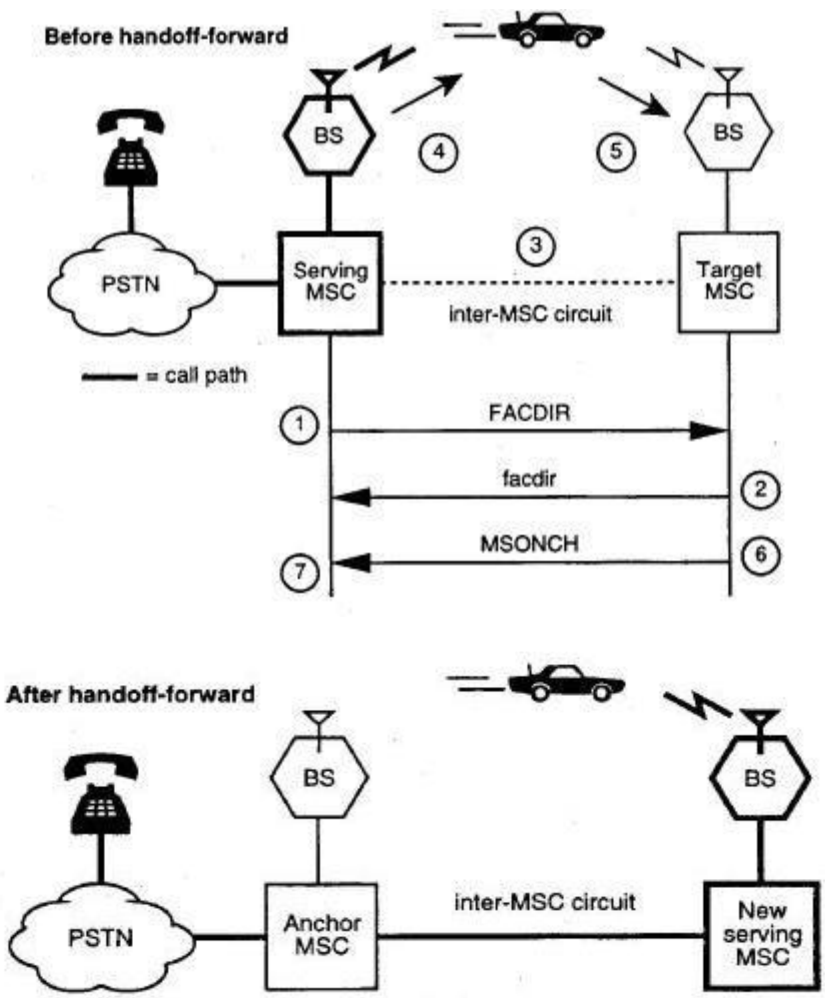

Figure 2.6.2 Example of Handoff Forward Processes

1. The serving MSC requests a handoff forward.
2. The target MSC accepts the handoff request.
3. The selected inter-MSC circuit is now ready for the handoff.
4. The serving MSC issues a handoff order to the MS.
5. The MS tunes to the new channel and is detected by the target MSC.
6. The target MSC notifies the serving MSC that the MS has been detected.
7. The serving MSC connects the call path to the inter-MSC circuit computing the handoff

Handoff Back

Handoff Back Functions

– Target MSC is already connected to serving MSC

– Once MS is moved to new channel, unused inter-MSC circuit is removed

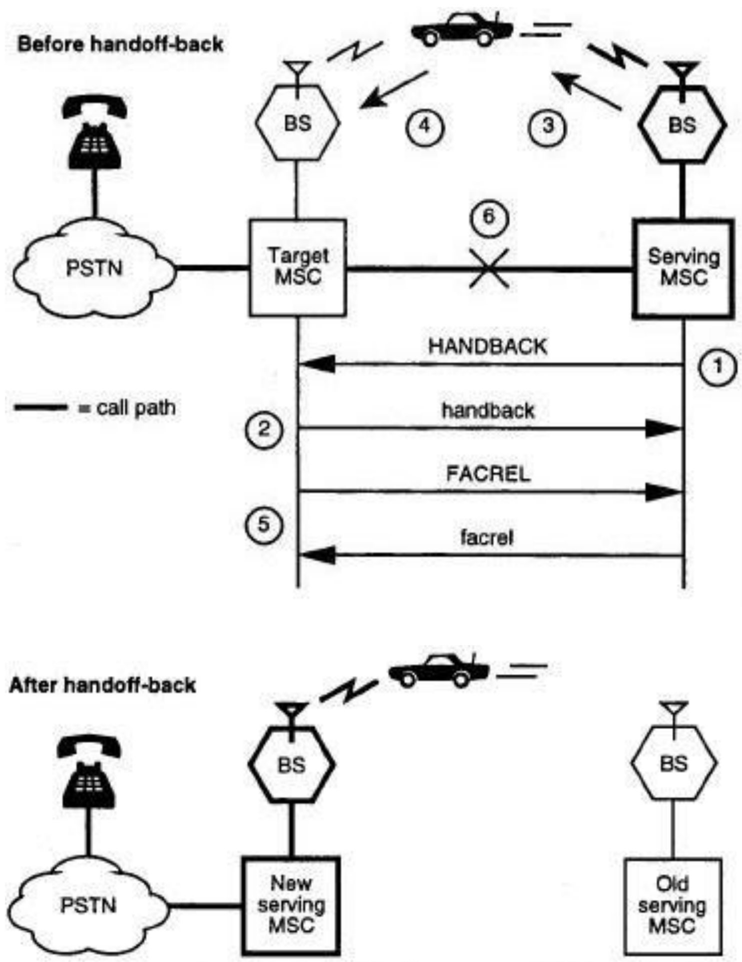

Figure 2.6 3Example of Handoff Back Processes

1. The serving MSC requests a handoff back.
2. The target accepts the handoff request.
3. The serving MSC issues a handoff order to the MS.
4. The MS tunes to the new channel and is detected by the target MSC.
5. The target MSC requests the release of the necessary inter-MSC circuit and the serving MSC accepts the request.
6. The inter-MSC circuit is released and is now ready for other handoff.

Path Minimization
Path Minimization Functions
– Eliminate unnecessary inter-MSC circuits between anchor MSC and target MSC

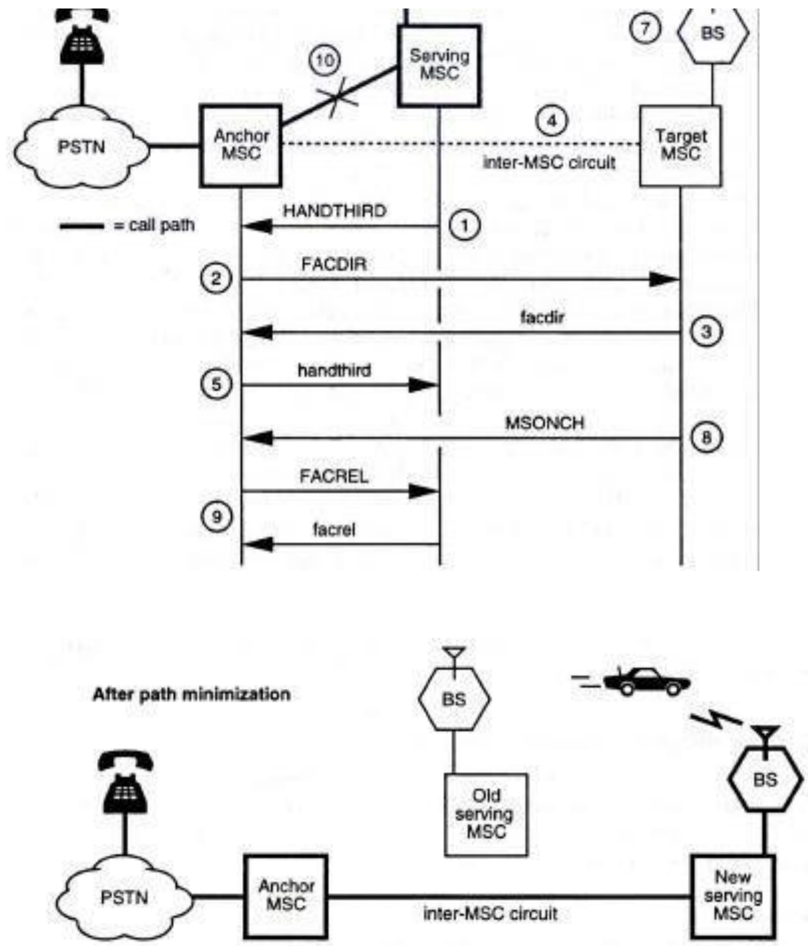

Figure 2.6.4 Example of Path Minimization Processes

1. The serving MSC sends a path minimization request to the anchor MSC.
2. The anchor MSC attempts to determine if path minimization is possible; it sends a handoff request to the target MSC.
3. The target MSC accepts the handoff request.
4. The selected inter-MSC circuit between the anchor MSC and the target MSC is now ready for the handoff.
5. The anchor MSC accepts the path minimization request.
6. The serving MSC issues a handoff order to the MS.
7. The MS tunes to the new channel and is detected by the target MSC.
8. The target MSC notifies the anchor MSC that the MS has been detected.
9. The anchor MSC connects the call path to the inter-MSC circuit, completing the handoff. It then releases the unnecessary inter-MSC circuit to the serving MSC.
10. The inter-MSC circuit is released and is now ready for handoff process.

Call Release

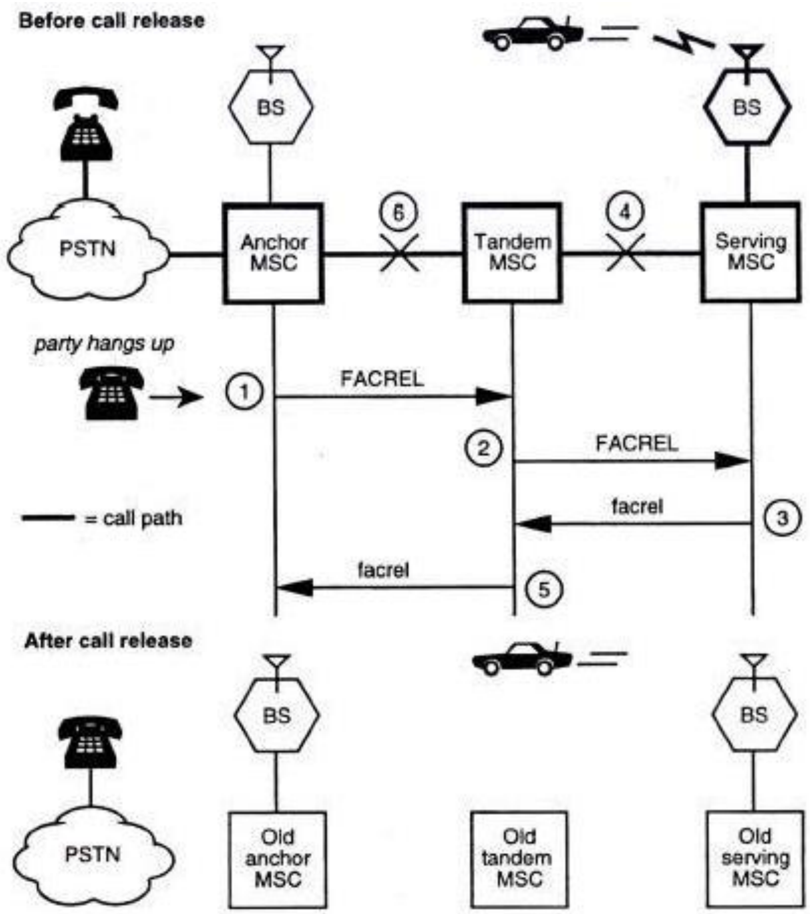

Figure 2.6.5 Example for Call Release

1. One of the parties to the call hangs up. The anchor MSC releases the unnecessary inter-MSC circuit toward the serving MSC.
2. The tandem MSC requests release of the unnecessary inter-MSC circuit to the serving MSC.
3. The serving MSC accepts the release request .The facrel message may contain billing information for use by the anchor MSC.
4. The inter-MSC circuit between the tandem MSC and the serving MSC is released and is now ready for other handoff process.
5. The tandem MSC accepts the release request. It forwards any billing information in step 3.
6. The inter-MSC circuit between the tandem MSC and the anchor MSC is released and it is now ready for other handoff process.

PACS Network Signaling

PACS is a third generation Personal Communications System originally developed and proposed by Bellcore in. PACS is able to support voice, data, and video images for indoor and microcell use. PACS is designed to provide coverage within a 500 meter range. The main objective of PACS is to integrate all forms of wireless local loop communications into one system with full telephone features, in order to provide wireless connectivity for local exchange carriers (LECs). Bell core developed PACS concept with LECs in mind and named it Wireless Access Communication System (WACS), but when the Federal Communications Commission introduced an unlicensed PCS band, the WACS standard was modified to produce PACS. In the original WACS proposal, ten TDMA/FDM time slots were specified in a 2 ms frame, and a 500 kbps channel data rate was proposed for a channel bandwidth of 350 kHz using QPSK modulation. In PACS, the channel bandwidth, the data rate, the number of slots per frame, and the frame duration were altered slightly, and $\pi/4$ QPSK was chosen over QPSK.

PACS System Architecture

PACS was developed as a universal wireless access system for wide spread applications in private and public telephone systems which operate in either licensed or unlicensed PCS bands. PACS may be connected to a PBX or Centrex, and may be served by a Central Office in residential applications. The PACS architecture consists of four main components: the subscriber unit (SU) which may be fixed or portable, the radio ports (RP) which are connected to the radio port control unit (RPCU), and the access manager (AM), as shown in Figure 2.7.1.1. Interface A, the air interface, provides a connection between the SU and RP. Interface P provides the protocols required to connect the SUs through the RPs to the RPCU, and also connects the RPCU with its RPs by using an Embedded Operations Channel (EOC) provided within the interface.

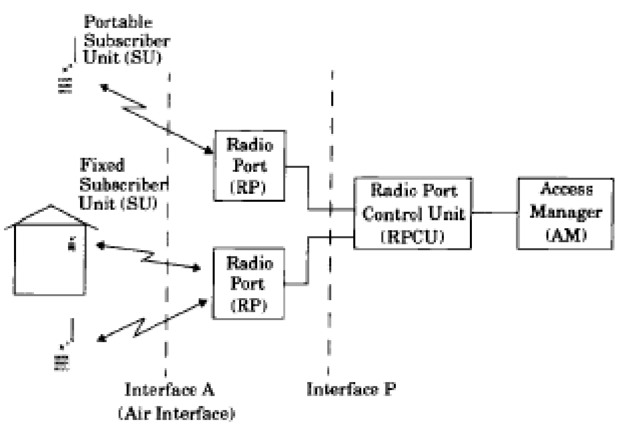

Figure 2.7.1.1 PACS system architecture.

The PACS PCS standard contains a fixed distribution network and network intelligence. Only the last 500 m of the distribution network is designed to be wireless.

PACS Radio Interface

The PACS system is designed for operation in the U.S. PCS band. A large number of RF channels may be frequency division multiplexed with 80 MHz separation, or time division multiplexed. PACS and WACS channel bandwidth is 300 kHz. WACS originally used TDMA with frequency division duplexing (FDD), with eight time slots provided in a 2.0 ms frame on each radio channel. When used with FDD, the reverse link time slot is offset from its paired forward link time slot by exactly one time slot plus 62.5 gs. The forward link covers 1850 MHz to 1910 MHz and the reverse covers 1930 MHz to 1990 MHz. The version of PACS developed for the unlicensed U.S. PCS band (PACSUB) between 1920 and 1930 MHz uses TDD instead of FDD [JTC95J. The PACS time slot and frame structure are shown in Figure 7.2. Modulation — PACS uses itI4-DQPSK modulation. The RF signal is shaped using a raised cosine rolloff shaping filter (rolloff factor of 0.5) such that 99% of the transmitted signal power is contained within a channel bandwidth of 288 kHz. Eight time slots, each containing 120 bits, are sent in a 2.5 ms frame.

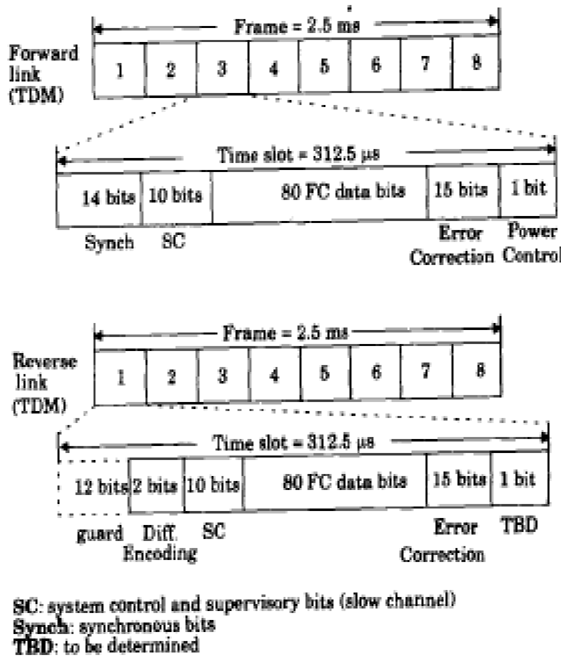

Figure 2.7.2PACS Frame Structure

When used with TDD, the time offset between the forward and reverse time slot for each user is exactly two time slots (625 ps) apart. Speech Coding — WACS uses 32 kbps A1)PCM for digital speech encoding. ADPCM provides low complexity, minimum cost, and radio link PACS Channels — PACS provides system broadcasting channels (SBC) which are used primarily on the forward link to broadcast paging messages. A 32 kbps SBC provides alerting and system information for up to 80,000 users. A synchronization channel (SYC) and the slow channel (SC) are used on the forward link to synchronize each subscriber unit. User information is transmitted only in the fast channel (FC) on both the forward and reverse links. As shown in Figure 10.21, each PACS time slot contains eighty fast channel bits and ten slow bits. There are several other special purpose logical channels defined in PACS.

Multiple Access — PACS is a TDMA based technology that supports either FDD or TDD. Many portable handsets and data terminals may be served from one installation of fixed radio equipment at the end of a feederline from a central office. The radio links may be shared among customers on the basis of individual user activity, and are designed to provide a wide range of user transmission rates within a common architecture.

Power Control — The PACS subscriber unit uses adaptive power control to minimize battery drain during transmissions and to reduce the co-channel interference on the reverse path.

Table 2.7.2.2 FAGS Radio Specifications (FOD or TDD implementation)

Parameter	Specification
Multiple Access	TDMA
Duplexing	FDD or TDD
Frequency Band	1 — 3 GHz
Modulation	$\pi/4$ DQPSK
Channel Spacing	300 kHz
Portable Transmitter Average Power	200 mW
Base Station Average Power	800 mW
Probability of Coverage Within Service Area	greater than 90%
Channel coding	CRC
Speech coding	16 bit ADPCM
Time Slots per Frame	8
Frame Duration	2.5 ms
Users per Frame	8 (FDD) or 4 (TDD)
Channel Bit Rate	384 kbps
Speech Rate	32 kbps
Bit Error	Less than 10^{-2}
Voice Delay	less than 50 ms

2.8 Cellular Digital Packet Data

CDPD is a data service for first and second generation U.S. cellular systems and uses a full 30 kHz AMPS channel on a shared basis provides mobile packet data connectivity to existing data networks and other cellular systems without any additional bandwidth requirements. It also capitalizes on the unused air time which occurs between successive radio channel assignments by the MSC (it is estimated that for 30% of the time, a particular cellular radio channel is unused, so packet data may be transmitted until that channel is selected by the MSC to provide a voice circuit). CDPD directly overlays with existing cellular infrastructure and uses existing base station equipment, making it simple and inexpensive to install. Furthermore CDPD does not use the MSC, but rather has its own traffic routing capabilities. CDPD occupies voice channels purely on a secondary; non interfering basis, and packet channels are dynamically assigned (hopped) to different cellular voice channels as they become vacant, so the CDPD radio channel varies with time. As with conventional, first generation AMPS, each CDPD channel is duplex in nature. The forward channel serves as a beacon and transmits data from the PSTN side of the network, while the reverse channel links all mobile users to the CDPD network and serves as the access channel for each subscriber. Collisions may result when many mobile users attempt to access the network simultaneously. Each CDPD simplex link occupies a 30 kHz RF channel, and data is sent at 19,200 bps. Since CDPD is packet-switched, a large number of modems are able to access the same channel on an as needed, packet-by-packet basis. CDPD supports broadcast, dispatch, electronic mail, and field monitoring applications. GMSK BT=O.5 modulation is used so that existing analog FM cellular receivers can easily detect the CDPD format without redesign. CDPD transmissions are carried out using fixed-length blocks. User data is protected using a Reed Solomon (63,47) block code with 6-bit symbols. For each packet, 282 user bits are coded into 378 bit blocks, which provide correction for up to eight symbols. Two lower layer protocols are used in CDPD. The mobile data link protocol (MDLP) is used to convey information between data link layer entities (layer 2 devices) across the CDPD air interface. The MDLP provides logical data link connections on a radio channel by using an address contained in each packet frame. The MDLP also provides sequence control to maintain the sequential order of frames across a data link connection, as well as error detection and flow control. The radio resource management protocol (RRMP) is a higher, layer 3 protocol used to manage the radio channel resources of the CIJPD system and enables an M-ES to find and utilize a duplex radio channel without interfering with standard voice services, The RRMP handles base-station identification and configuration messages for all M-ES stations, and provides information that the M-ES can use to determine usable CDPD channels without knowledge of the history of channel usage. The RRMP also handles channel hopping commands, cell handoffs, and M-ES change of power commands. CDPD version 1.0 uses the X.25 wide area network (WAN) sub profile and frame relay capabilities for internal sub networks. Table 2.8.1 lists the link layer characteristics for CDPD. Figure 2.8.2 illustrates a typical CDPD network. Note that the subscribers (the mobile end system, or M-ES) are able to connect through the mobile data base stations (MDBS) to the Internet via intermediate systems (MD-IS), which act as servers and routers for the subscribers. In this way, mobile users are able to connect to the Internet or the PSTN. Through the I-interface, CDPD can carry either Internet protocol (IP) or 0S1 connectionless protocol (CLNP) traffic.

Table 2.8.1 Link Layer Characteristics for CDPD

Protocols	MDLP, RRMP, X.25
Channel Data Rate (bps)	19,200
Channel Bandwidth (kHz)	30
Spectrum Efficiency (b/Hz)	0.64
Random Error Strategy	cover with burst protect
Burst Error Strategy	RS 63,47 (6 bits per symbol)
Fading Performance	withstands 2.2 ms fade
Channel Access	slotted DSMA/CD

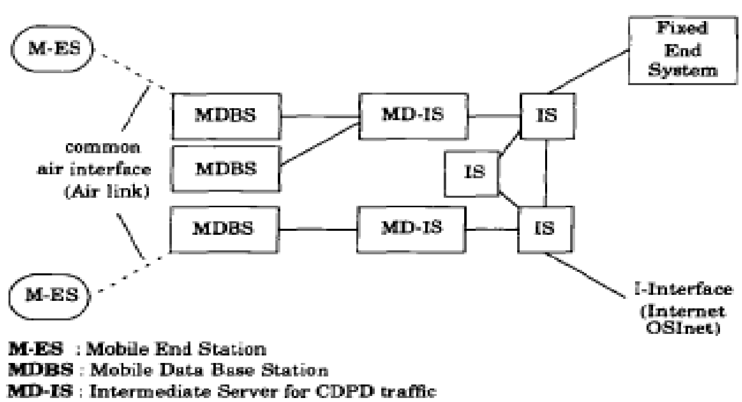

Figure 2.8.2 The CDPD network.

UNIT 3

GSM

GSM Network Signaling

The GSM technical specifications define the different entities that form the GSM network by defining their functions and interface requirements.

The GSM network can be divided into four main parts:

- The Mobile Station (MS).
- The Base Station Subsystem (BSS).
- The Network and Switching Subsystem (NSS).
- The Operation and Support Subsystem (OSS).

The architecture of the GSM network is presented in figure 3.1.1.

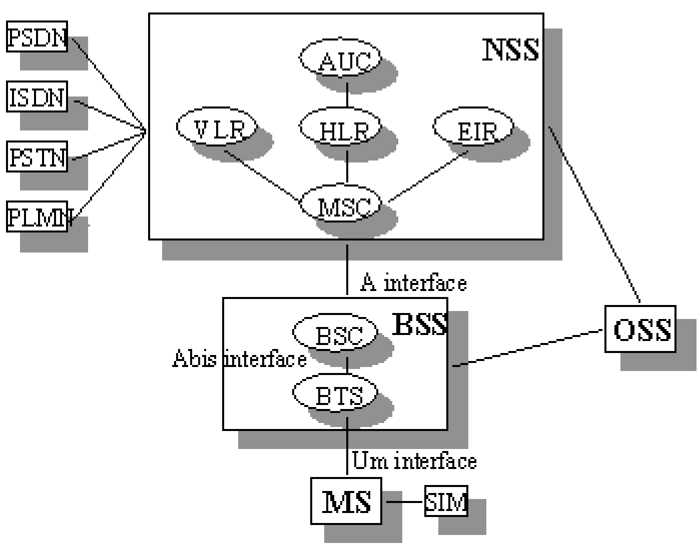

Figure 3.1.1 Architecture of the GSM network

Mobile Station

A Mobile Station consists of two main elements:

- **The Subscriber Identity Module (SIM)**: It is protected by a four-digit Personal Identification Number (PIN). In order to identify the subscriber to the system, the SIM card contains amongst others a unique International Mobile Subscriber Identity (IMSI). User mobility is provided through maping the subscriber to the SIM card rather than the terminal as we done in past cellular systems.

- **Mobile equipment/terminal (ME):** There are different types of terminals (MN) distinguished principally by their power and application:

  - `Fixed' terminals mainly installed in cars. Their maximum allowed output power is **20W**
  - Portable terminals can also be installed in vehicles. Their maximum allowed output power is **8W**.
  - Handheld terminals; their popularity is owed to their weight and volume, which is continuously decreasing. According to some specification these terminals may emit up to **0.8W**. However, as technology has evolved their maximum allowed power output is limited to **0.1W**.

Base Station Subsystem

The BSS provides the interface between the ME and the NSS. It is in charge of the transmission and reception. It may be divided into two parts:

- **Base Station Controller (BSC):** It controls a group of BTSs and manages their radio resources. A BSC is principally **in charge of handoffs**, frequency hopping, *exchange* functions and ***power control*** over each managed BTSs.
- **Base Transceiver Station (BTS) or Base Station:** it maps to transceivers and antennas used in **each cell** of the network. It is usually placed in the center of a cell. **Its transmitting power defines the size of a cell**. Each BTS has between 1-16 transceivers depending on the density of users in the cell.

NSS

Its main role is to manage the communications between the mobile users and other users, such as mobile users, ISDN users, fixed telephony users, etc. It also includes data bases needed in order to store information about the subscribers and to manage their mobility. The different components of the NSS are described below.

- **MSC:** the central component of the NSS. The MSC performs the switching functions of the network. It also provides connection to other networks.
- **GMSC:** A gateway that interconnects two networks: the **cellular network** and the **PSTN**. It is in charge of routing calls from the fixed network towards a GSM user. The GMSC is often implemented in the same machines as the MSC.
- **HLR:** The HLR stores information of the suscribers belonging to the coverage area of a MSC; it also stores the current location of these subscribers and the services to which they have access. The location of the subscriber maps to the **SS7** address of the Visitor Location Register (VLR) associated to the MN.
- **VLR:** contains information from a subscriber's HLR necessary to provide the subscribed services to visiting users. When a subscriber enters the covering area of a new MSC, the VLR associated to this MSC will request information about the new subscriber to its corresponding HLR. The VLR will then have enough data to assure the subscribed services without needing to ask the HLR each time a communication is established. The VLR is always implemented together with a MSC; thus, the area under control of the MSC is also the area under control of the VLR.
- **Authentication Center (AuC):** It serves security purposes; it provides the parameters needed for authentication and encryption functions. These parameters allow verification of the subscriber's identity.
- **Equipment Identity Register (EIR):** EIR stores security-sensitive information about the mobile equipments. It maintains a list of all valid terminals as identified by their International Mobile Equipment Identity (IMEI). The EIR allows then to forbid calls from stolen or unauthorized terminals (e.g., a terminal which does not respect the specifications concerning the output RF power).
- **GSM Interworking Unit (GIWU):** The GIWU provides an interface to various networks for data communications. During these communications, the transmission of speech and data can be alternated.

Operation and Support Subsystem (OSS)

It is connected to components of the NSS and the BSC, in order to **control and monitor** the GSM system. It is also in charge of controlling the **traffic load** of the BSS. It must be noted that as the number of BS *increases* with the scaling of the subscriber population some of the maintenance tasks are transferred to the BTS, allowing *savings* in the cost of ownership of the system.

Geographical areas

A cell, as identified by its Cell Global Identity (CGI) number, maps to the radio coverage of a BTS. Similarly an LA as identified by its **Location Area Identity** (LAI) number, is a cluster of cells served by a **single** MSC/VLR. A *group of LA* under the control of the same MSC/VLR defines the ***MSC/VLR area***. A Public Land Mobile Network (PLMN) is the area served by **one** network operator.

Network operations

In this paragraph, the description of the GSM network is focused on the different functions to fulfill by the network and not on its physical components. In GSM, five main functions can be defined:

Transmission: of *data* and *signaling*. Not all the components of the GSM network are strongly related with both types of types of Tx. While the MSC, BTS and BSC, among others, are involved with data and signaling, components such as HLR, VLR or EIR registers, are only concerned with signaling.

- **Radio Resources Management (RRM).**
- **Mobility Management (MM).**
- **Communication Management (CM).**
- **Operation, Administration and Maintenance (OAM).**

Radio Resources Management (RRM)

The role of the RR function is to establish, maintain and release communication links between mobile stations and the MSC. The elements that are mainly concerned with the RR function are the MN and the BTS. However, since the RR component performs connection management also **during** cell handoffs, it also affects the MSC which is the handoff management component.

The RR is also responsible for the management of *frequency resources* as well as *varying* radio interface conditions. Main component operations are:

- Channel assignment, change and release.
- Handoff
- Frequency hopping.
- Power-level control.
- Discontinuous transmission and reception.
- Timing advance.

Mobility Management (MM)

The MM component handles:

- **Location Management:** Location is managed through periodically or on-demand. At power-on time, the MH signals an **IMSI attach. On-demand** location updates are signaled when the MN moves to a different PLMN or new location area (LA). The signal is sent to the new MSC/VLR, which forwards it to the *subscriber's* HLR. Upon authorization in the ***new*** MSC/VLR, the subscriber's HLR **removes** the registration entry of the MN at the **old** MSC/VLR. If after the update time interval, the MN has not registered, it is then deregistered. On power-off, the MN performs an **IMSI detach**.

- **Security and authentication:** Authentication involves the SIM card and the Authentication Center. A secret key, stored in the SIM card and the AuC together with a ciphering algorithm called A3, are used to authenticate the user. The **MN** and the **AuC** *compute a SRES through A3* using the *secret key* and a ***nonce*** generated by the AuC. If the two computed SRES are the same, the subscriber is authenticated. The different services to which the subscriber has access are also checked. Next the security check is performed in the equipment identity (IMEI). If the IMEI number of the mobile is authorized in the EIR, the mobile station is allowed to connect the network. To assure ***user confidentiality***, the user is registered with a Temporary Mobile Subscriber Identity (TMSI) after its **first** location update procedure. Enciphering is another option to guarantee a very strong security.

Communication Management (CM)

The CM component manages:

Call control (CC): it controls call setup, management and tear-down in relation to management of type of service. Call routing is the primary task for this component. To reach a mobile subscriber, a user dials the Mobile Subscriber ISDN (MSISDN) number which includes:

- a *country* code
- a national destination code; this identifies the *subscriber's* ***operator***
- a code mapping to the **subscriber's HLR.**
- The call is then ***passsed*** to the GMSC (if the call is originated from a fixed network) that 'knows' the HLR corresponding to the particular MSISDN number. The GMSC **signals** the HLR for call routing information. The HLR requests this information from the subscriber's **current** VLR. This VLR **allocates** ***temporarily*** a Mobile Station Roaming Number (MSRN) for the call. The MSRN number is the information *returned* by the HLR to the ***GMSC***. It is later that routes the call through the MSRN number, to the subscriber's **current** MSC/VLR. In the subscriber's current LA, the mobile is paged.

Operation, Administration and Maintenance (OAM)

The OAM component allows the operator to monitor and control the system as well as **modify** the **configuration** of the elements of the system. Not only the OSS is part of the OAM, but also the BSS and NSS participate in functions such as:

- Provide the operator with all the information it needs. This information is forwarded to the OSS to control the network.
- Perform self-test tasks in addition to the OAM functions.
- Control of multiple BTSs by the BSS.

GSM MOBILITY MANAGEMENT

To exercise location tracking, a mobile service area is partitioned into several Location Areas (LA) or registration areas. **Every LA consists of a group of BTSs.** The major task of mobility management is to update the location of an MS when it moves from one LA to another.

Location Update Concept (Registration)

The location update (registration) procedure is initiated by the MS.

□ **Step 1.** The BTs periodically broadcast the corresponding LA addresses to the MSs.

□ **Step 2.** When an MS receives an LA address different from the one stored in it memory, it sends a registration message to the network.

Note that

Every VLR maintains the information of a group of LAs. When an MS visits an LA, a temporary record of the MS is created in the VLR to indicate its location (i.e. LA address).

For every MS, a permanent record is maintained in HLR. The record stores the address of VLR visited by the MS .MS

Two Issues of GSM Mobility Databases

Fault Tolerance: If the location database fails, the loss or corruption of location information will seriously degrade the service offered to the subscribers.

Database Overflow: The VLR may overflow if too many users move into the VLR-controlled area in a short period. If the VLR is full when a mobile user arrives, the user fails to register in the database, and thus cannot receive cellular service. This phenomenon is called VLR overflow.

Basic Location Update Procedure

Case 1. Inter-LA Movement

Case 2. Inter-MSC Movement

Case 3. Inter-VLR Movement

Inter-LA Movement

The MS moves from LA1 to LA2, where both LAs are connected to the same MSC. In GSM 04.08, nine messages are exchanged between the MS and the MSC, and ten messages are exchanged between the MSC and the VLR. Four major steps are discussed here.

Step 1.

A location update request message is sent (MS->BTS->MSC). The MS identifies itself by the Temporary Mobile Subscriber Identity (TMSI), which is an alias for IMSI. IMSI (International Mobile Subscriber Identity) is used to identify the called. IMSI is not known to the User but GSM network. TMSI is used to avoid sending the IMSI on the radio path, which is temporary identity, is allocated to an MS by the VLR at inter-VLR registration, and can be changed by the VLR.

Step 2.

The MSC forwards the location update request to the VLR by a TCAP message, this message includes (Address of the MSC, TMSI of MS, Prev. Location Area Identification (LAI), Target LAI, Other Related Information).

Steps 3 and 4.

The VLR notices that both LA1 and LA2 belong to the same MSC. The VLR updates the LAI field of the VLR record. The VLR replies an ACK to the MS through the MSC.

Inter-MSC Movement

The two LAs belong to different MSCs of the same VLR.

Steps 1 and 2. The location update request is sent from the MS to the VLR.

Step 3.

The VLR notices that the Prev. LA and the Target LA belong to MSC1 and MSC2, which are connected to the same VLR, respectively. The VLR updates the LAI and the MSC fields of the VLR record. The VLR derives the HLR address of the MS from the MS's IMSI stored in the VLR record. The VLR sends the MAP_UPDATE_LOCATION to the HLR.

(IMSI of MS, Target MSC Address, Target VLR Address, other related information)

Step 4.

By using the received IMSI, the HLR identifies the MS's record. The MSC number field of the record is updated. An acknowledgement is sent VLR.

Steps 5 and 6.

Similar to steps 3 and 4 in Inter-BTS movement, the acknowledgement is forwarded to the MS.

Inter-VLR Movement

Step 1. The location update request is sent from MS to the VLR.

Steps 2 and 3.

Since the MS moves from VLR1 to VLR2, VLR2 does not have a VLR record of the MS, and the IMSI of the MS is not known. From the MAP_UPDATE_LOCATION_AREA message, VLR2 identifies the address the VLR1. VLR2 sends MAP_SEND_IDENTIFICATION to VLR1. Note that to enhance security, confidential data (IMSI) typically is not sent over the air.

Steps 4 and 5.

VLR2 creates a VLR record for the MS, and sends a registration message to update the HLR. The HLR updates the record of the MS. An acknowledge is sent back to VLR2.

Step 6.

VLR2 generates a new TMSI and sends it to the MS. In GSM, the TMSI is changed from time to time to avoid fraudulent usage.

Steps 7 and 8. The obsolete record of the MS in VLR1 is deleted.

3.2.3 GSM Basic Call Origination

Step 1.

The MS u1 sends the call origination request to the MSC.

Step 2.

The MSC forwards the request to the VLR by sending MAP SEND INFO FOR OUTGOING CALL.

Step 3.

The VLR checks the u1's profile and sends MAP SEND INFO FOR OUTGOING CALL ack to the MSC to grant the call request.

Step 4.

The MSC sets up the trunk according to the standard PSTN call setup procedure.

GSM Basic Call Termination

Step 1.

When the MSISDN number is dialed by a PSTN user, the call is routed to a gateway MSC by an SS7 ISUP IAM message.

Step 2.

To obtain the routing information, the GMSC or ISDN exchange interrogates the HLR by sending MAP_SEND_ROUTING_INFORMATION to the HLR. The message contains the MSISDN of the MS and other related info.

Step 3.

The HLR sends a MAP_PROVIDE_ROAMING_NUMBER message to the VLR to obtain the Mobile Subscriber Roaming Number (MSRN). The message consists of IMSI of the MS, the MSC number.

Steps 4 and 5.

The VLR creates the MSRN by using the MSC number stored in the VLR record of the MS. This roaming number is sent back to the gateway MSC through the HLR.

Step 6.

The MSRN provides the address of the target MSC where the MS resides. An SS7 ISUP IAM message is directed from the gateway MSC to the target MSC to setup the voice trunk.

Mobility Databases: Home Location Register (HLR)

Mobile Station Information. For example,

the IMSI (used by the MS to access the network), and IMSI

MSISDN (which is the ISDN number—"Phone Number "of the MS)

Location Information. For example,

the ISDN number (address) of the VLR (where the MS resides), and

the ISDN number of the MSC (where the MS resides)

Service Information. For example,

□ service subscription ,

□ service restrictions ,

supplementary services

Mobility Databases: Visitor Location Register

Mobile Station Information. For example,

□ IMSI

□ MSISDN

□ TMSI

Location Information. For example,

□ MSC Number

□ Location Area ID (LAI)

Service Information.

A subset of the service Information stored in HLR

Note that in the MS-related fields

Length TMSI <= 8 digits (TMSI structure defined by the operator)

□ LAI = XXX + XX + XXXXXXXXXXXXXXXX

GSM SHORT MESSAGE SERVICE

Short message service is a mechanism of delivery of short messages over the mobile networks. It is a store and forward way of transmitting messages to and from mobiles. The message (text only) from the sending mobile is stored in a central short message center (SMS) which then forwards it to the destination mobile. This means that in the case that the recipient is not available, the short message is stored and can be sent later. Each short message can be no longer than 160 characters. These characters can be text (alphanumeric) or binary Non-Text Short messages. An interesting feature of SMS is return receipts. This means that the sender, if wishes, can get a small message notifying if the short message was delivered to the intended recipient. Since SMS used signaling channel as opposed to dedicated channels, these messages can be sent/received simultaneously with the voice/data/fax service over a GSM network. SMS supports national and international roaming. This means that you can send short messages to any other GSM mobile user around the world. With the PCS networks based on all the three technologies, GSM, CDMA and TDMA supporting SMS, SMS is more or less a universal mobile data service.

Note: *The actual limit of size of SMS is 160 characters if Latin alphabets are used. If non-Latin alphabets like Chinese or Arabic are used, the limit is 70 characters.*

How does SMS work

The figure below shows a typical organization of network elements in a GSM network supporting SMS.

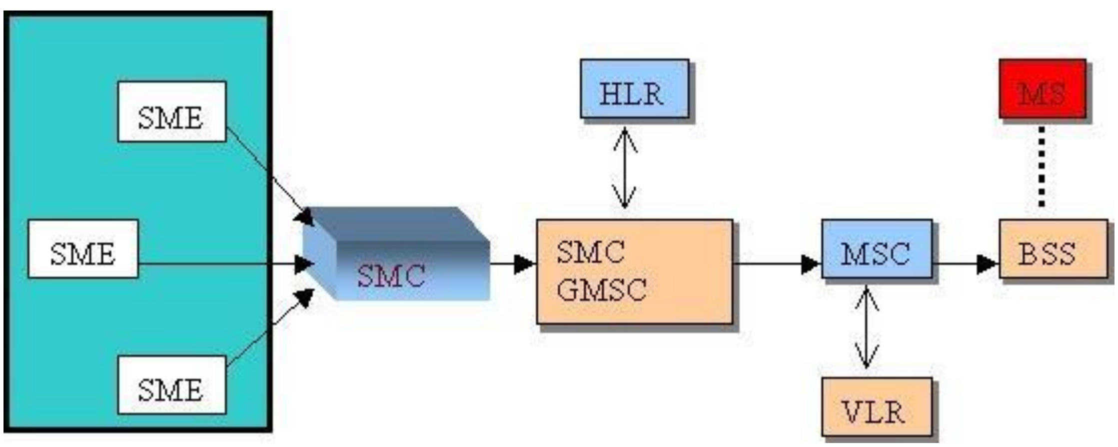

Figure 3.3.1

The SMC (Short Message Center) is the entity which does the job of store and forward of messages to and from the mobile station. The SME (Short Message Entity) which can be located in the fixed network or a mobile station, receives and sends short messages.

The SMS GWMS (SMS gateway MSC) is a gateway MSC that can also receive short messages. The gateway MSC is a mobile network’s point of contact with other networks. On receiving the short message from the short message center, GMSC uses the SS7 network to interrogate the current position of the mobile station form the HLR, the home location register.

HLR is the main database in a mobile network. It holds information of the subscription profile of the mobile and also about the routing information for the subscriber, i.e. the area (covered by a MSC) where the mobile is currently situated. The GMSC is thus able to pass on the message to the correct MSC.

MSC (Mobile Switching Center) is the entity in a GSM network which does the job of switching connections between mobile stations or between mobile stations and the fixed network.

A VLR (Visitor Location Register) corresponds to each MSC and contains temporary information about the mobile, information like mobile identification and the cell (or a group of cells) where the mobile is currently situated. Using information form the VLR the MSC is able to switch the information (short message) to the corresponding BSS (Base Station System, BSC + BTSs), which transmits the short message to the mobile. The BSS consists of transceivers, which send and receive information over the air interface, to and from the mobile station. This information is passed over the signaling channels so the mobile can receive messages even if a voice or data call is going on.

Applications

Some of the common applications of SMS are:

- Exchanging small messages like "See you at 8.30 tonight at xyz". SMS is particularly suited for these kinds of short messages because SMS is much cheaper than calling some one and giving the same message. Calling some one to give the same message would invariably take more time and hence more cost.
- Many operators offer e-mail service over SMS. Every user is assigned an e-mail address at signup and any message delivered to that email is converted to short messages and delivered to the mobile.
- It is possible to send e-mail messages (less than 160 characters) from a mobile phone to any e-mail address via SMS.
- Information services like news, weather, entertainment and stock prices etc. can be availed just by sending a keyword like NEWS, WEATH etc to the short message center number.
- SMS can be used by the network operators to provide services like balance enquiry in case of prepaid cards using SMS.
- Mobile chatting is one more hot application of SMS
- SMS can be used to notify users that they have received new voice-mail or fax messages.
- It provides an alternative to alphanumeric paging services
- Using SIM-Toolkit, now a part of GSM specifications, SMS can be used to have on the air activation of features. By sending codes embedded in short messages from the server network operators can remotely provision the user's wireless terminal
- Internet e-mail alerts.
- Downloading new ring tones.

INTERNATIONAL ROAMING FOR GSM

GSM supports roaming services that allow a subscriber in a GSM network to receive service when the user visits a different GSM network.
If the networks are located in different countries, the current GSM implementation for call delivery to the roamer can be very expensive.
In current GSM international roaming implementations, call delivery to a GSM roamer resultsin one or two international calls.

Three Scenarios for GSM
Suppose that a GSM user from Taiwan (namedJohn) roams to Singapore.

Scenario 1:
- if a person in Taiwan calls John, the result is a local call + an international call.
- the caller is charged for a local GSM call.
- John is charged for an international call from Taiwan toSingapore.

Scenario 2:
- If the caller is from a third country (e.g., Hong Kong), the call delivery to John results in two international calls.
- The caller is charged for an international call from Hong Kong to Taiwan.
- John is charged for an international call from Taiwan to Singapore.

Scenario 3:
- If the caller is in Singapore, the call delivery results in two international calls, even though both caller and callee are in Singapore.
- This scenario is in fact a special case of Scenario 2, and is referred to as Tromboning.

3.4.1 International GSM Call Setup

The call delivery procedure to a GSM roamer is basically the similar to the GSM basic callsetup
Procedure:
Two International Switch Centers (ISCs) are involved in the voice path.
- All countries have a national network, which is connected to an international network.

ISCs offer inter-working functions between the national networks and the internationalnetwork.
The call path of every international call is composed of three segments:
- One in the origination country,
- Another in the international network, and
- The third in the destination country.

These circuit segments are interconnected by two ISCs.
- One ISC in the origination country and
- The other ISC in the destination country.

Consider the previous example where Jenny (in Singapore) places a call to John (who has roamed from Taiwan to Singapore).

Step 1:

John's GSM home system is in Taiwan, so Jenny first dials the International Switch Center Access Code (ISCA) + the Country Code (CC) + John's MSISDN.

 MSISDN = National Destination Code (NDC) + 6-digit Subscriber Number (SN)

Step 1.1:

When Switch A interprets the MSCA, it identifies the call as an international call, and then sets up the call to Singapore's ISC B.

Step 1.2:

Based on the CC, ISC B routes the call to Taiwan ISC C.

Step 1.3:

ISC C interprets the prefix of the remaining digits, and sets up the voice trunk to GMSC D.

Step 2:

GMSC D queries HLR E to obtain the MSRN.

Steps 3 and 4:

HLR E queries VLR F.

Note that these message travel between Taiwan and Singapore

Step 5:

The MSRN is returned to GMSC D.

Step 6:

Based on the MSRN, GMSC D sets up the trunk to MSC G.

GSM operation, Administration and maintenance

To manage the network GSM requires OA&M functions follow the standard Telecommunication Management Network (TMN) concept

The TMN Component

Operations System (OS)

With the operations system function (OSF), the OS is responsible for the overall TMN management billing, accounting, management of mobile equipment, HLR measurement Reside in an operation and maintenance center (OMC)

Network Element (NE)

NEs in GSM are HLR, VLR, MSC, AuC, BSC, BTS, EIR monitored or controlled by the OS Network Element Functions (NEFs) represent the telecommunications and support functions to be managed by the OS

Data Communication Network (DCN)

The OSs, NEs, and other TMN elements communicate through DCN by using data communication function (DCF) The DCN technology can be WAN, LAN, or others The GSM OMC typically connects to MSCs and BSCs by X.25

Mediation Device (MD)

The MD adapts the OS to the specific NEs Uses the mediation function (MF) to route or pass information between standardized interface

Q-Adapter (QA)
Use the Q-adaptor function (QAF) to connect the non-TMN entities
Workstation (WS)
Interacts the operation/maintenance personnel with the OS through the workstation functions (WSFs) With WSFs, staff access the status of the network and monitor the system parameters

TMN architecture

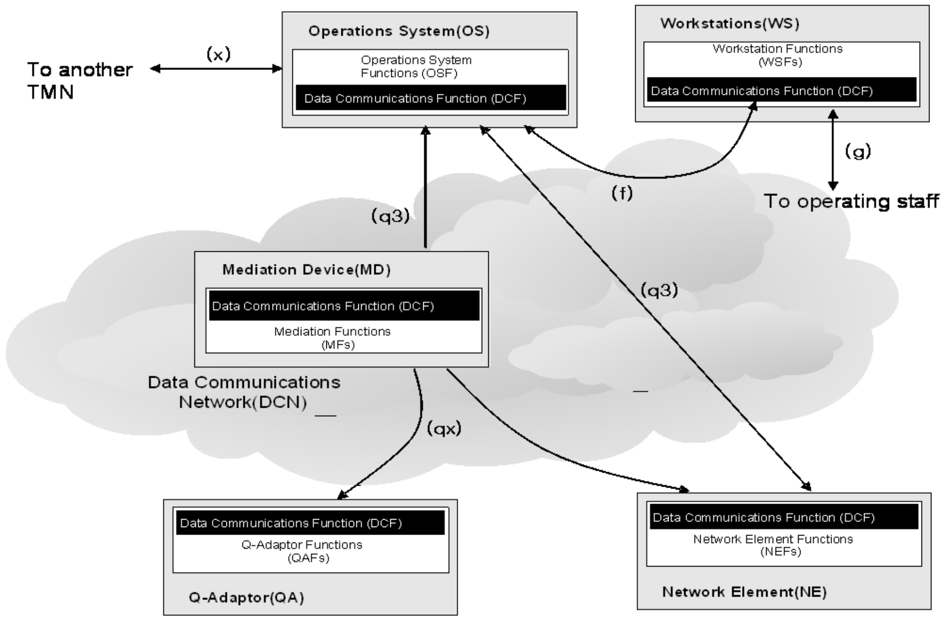

Figure 3.5.1.1

TMN connection for the base station system

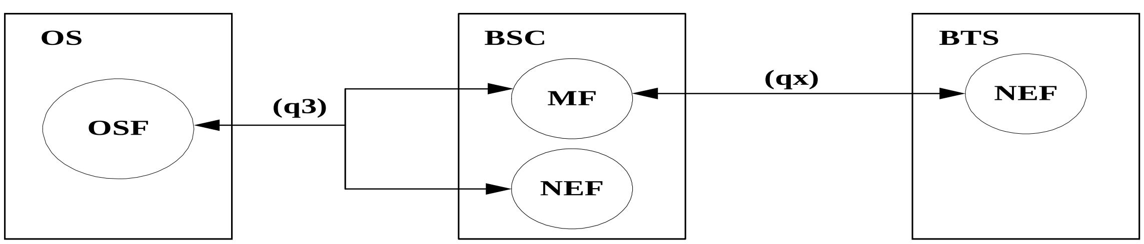

Figure 3.5.1.2

The relationship between components of TMN functions are defined by using the reference points
q3 : connects an OSF to an MF or an NEF
qx : connects an MF to an NEF or a QAF
x : connects an OSF to another OSF , OSF-like functionality in a different TMN
f : connects an OSF to a WSF
g : connects an WSF to the operating staff

Call-Recording Functions

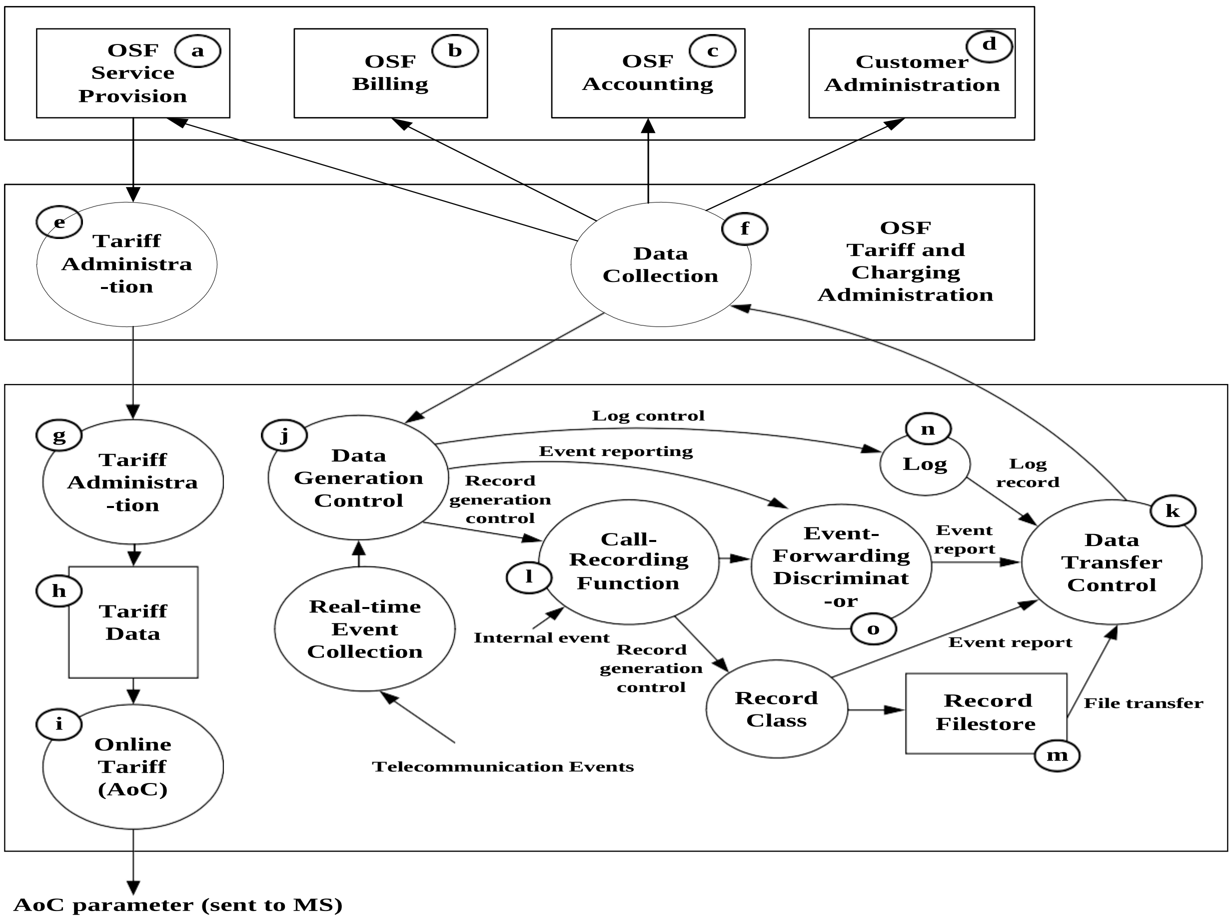

Figure 3.5.2.1 Tariff and charging administration

The billing of the mobile subscribers, statistics of service usage, and roaming traffic must be monitored by the OS. This information is provided by the NEs. Managed by the tariff and charging administration

Administration includes the following services

- ❑ Service Provision : introduce new or modified services to the GSM
- ❑ Billing : determines the charge for the services
- ❑ Accounting

Inter-PLMN:

- Required for roaming traffic management, which is settled by means of the transfer account procedure (TAP)
- TAP records are regularly exchanged between GSM network
- For visitor from another GSM network

The mobile-originated call charges are calculated and converted to an agreed accounting currency

Fixed-network: manage call traffic between MS and the fixed network signaling traffic for functions such as location updates

Customer Administration: handles customer queries such as billing complaints

Tariff Administration

Tariff administration function provides the tariff administration information to the NEs. The OSF uses the tariff class management functions to assign a tariff class with service, distance, and time-based tariff-dependent charging parameters. These dependencies are elaborated next:

- The service charging dependencies are defined based on the customized AoC
- The AoC (advice of charge) service definition may consist of one or more
  - Service types
  - Radio channel types
  - Connection type
- The distance dependencies are defined based on the origins, destinations, and charging zone

Data Collection

Data collection functions provide the specifications of the collected data to the NEs through the data generation control in the NEF (record generation, event reporting, and log control). The OSF data collection functions collect the data from these NEs through the data transfer control Call-recording function generates potential call and event records based on the internal telecommunication events in the NE. The record generation control determines where the records are sent:

- The records may be forwarded to the record file store
- The records may be saved in a log file
- The records may also be passed to the EFDs controlled by the event-reporting function

Performance Measurement and Management

Performance of GSM network, Evaluate based on the data provided by NEs

data: user/signaling traffic levels, quality of service network configuration verification, resource access measurements

Measurement job

- is created, modified, displayed, suspended, resumed, deleted in the OS
  - is implemented as a simple Scanner object
- is scheduled in a period to accumulate measurement data for inspection
- instruct measurement function objects in the NEs to collect the data

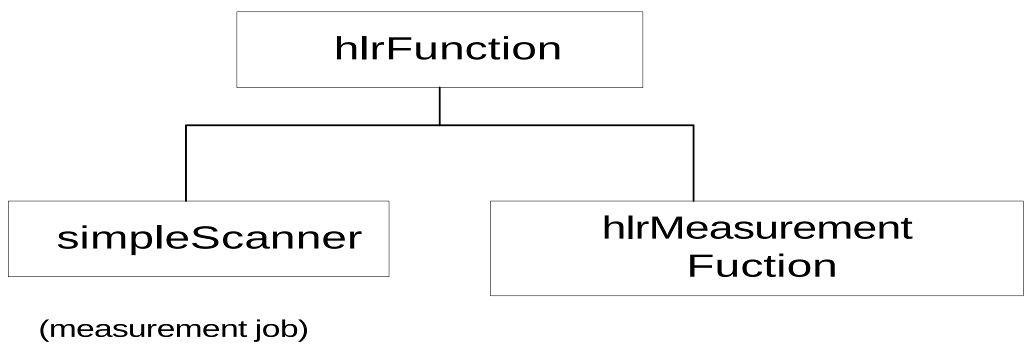

Figure 3.5.3.1

Simple Scanner Object

- Measurement types
  - attLocationUpdate : number of the attempted location updates
  - succlocationUpdate : number of the successful location updates
- Measured network resources : The network resource is HLR
- Measurement function : The simple Scanner specifies one or more measurement functions in the NEs to collect the desired data

- Measurement schedule :
    - specify start time & stop time of the active measurement period
    - should be started within 90 days after measurement job is created
- Granularity period :
    - specify periodic interval of sending measured data from HLR to OS
- Scan report
    - is sent from NE to OS at the end of every granularity period
    - include timestamp to indicate when it is sent to OS

Subscriber and Service Data Management

- Subscriber and Service Data Management
    - Define management for NEs … AuC, HLR, VLR, and EIR
    - Managed data in different NEFs may depend on each other
    - example :
        - To create a subscriber profile in the HLR, subscriber data should already exist in the AuC
        - If it does not, creation in the HLR fails
    - MSISDNs and IMSIs are managed in HLR
    - An MSISDN can associate with several basic service
        - Established between the msisdnHlr object and the basic ServiceInHlr objects
    - Some supplementary services are specified with parameters
    - When a subscriber is deleted from the HLR, the corresponding subscriberInHlr object and all its contained objects are removed

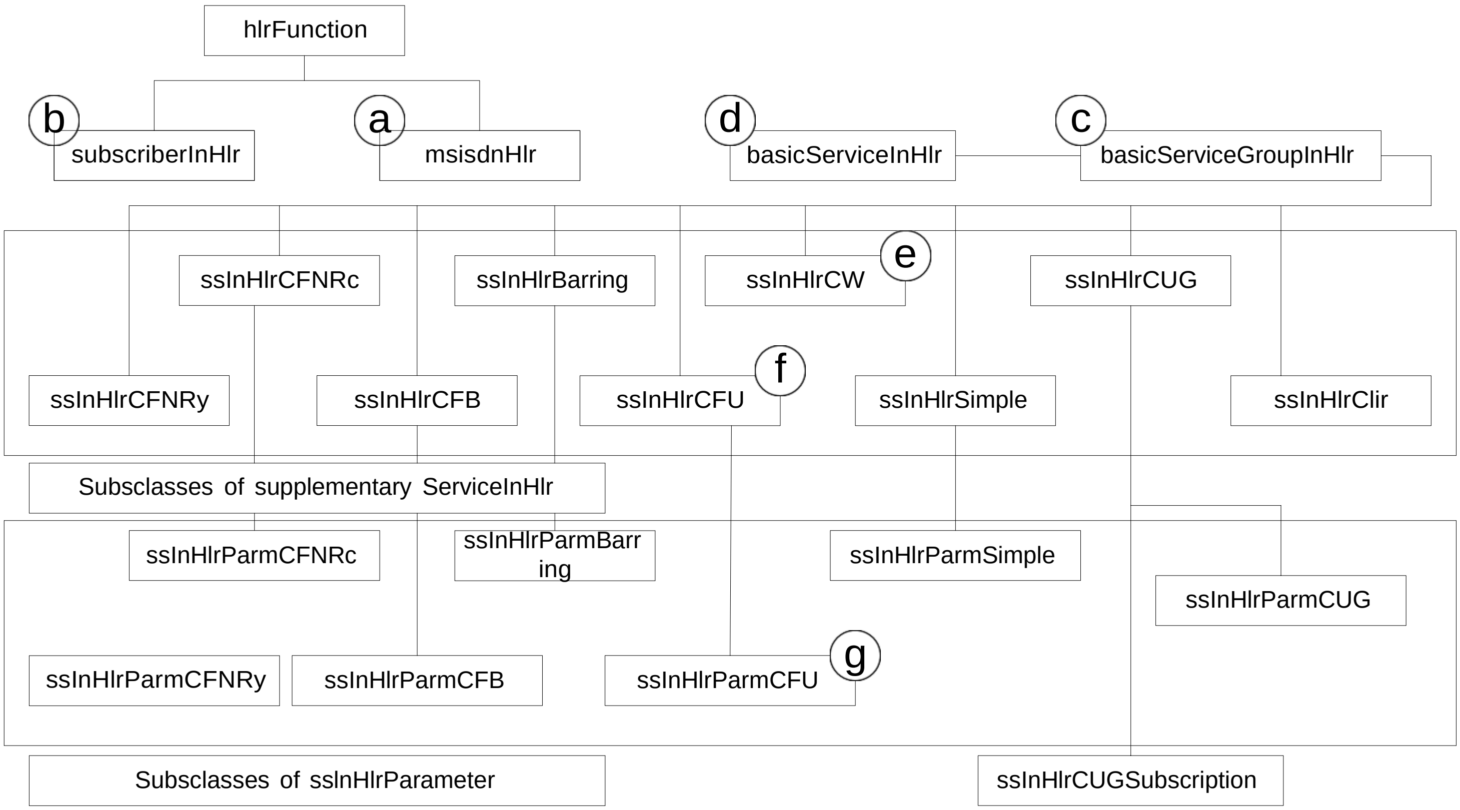

Figure 3.5.4.1 HLR subscriber administration object class containment

UNIT 4

WIRELESS APPLICATION PROTOCOL

WAP model

Before we describe WAP model, first we would like you to understand how Standard Internet works.

The Internet Model:

The Internet model makes it possible for a client to reach services on a large number of origin servers; each addressed by a unique Uniform Resource Locator (URL).

The content stored on the servers is of various formats, but HTML is the predominant. HTML provides the content developer with a means to describe the appearance of a service in a flat document structure. If more advanced features like procedural logic are needed, then scripting languages such as JavaScript or VB Script may be utilised.

The figure below shows how a WWW client request a resource stored on a web server. On the Internet, standard communication protocols, like HTTP and Transmission Control Protocol/Internet Protocol (TCP/IP) are used.

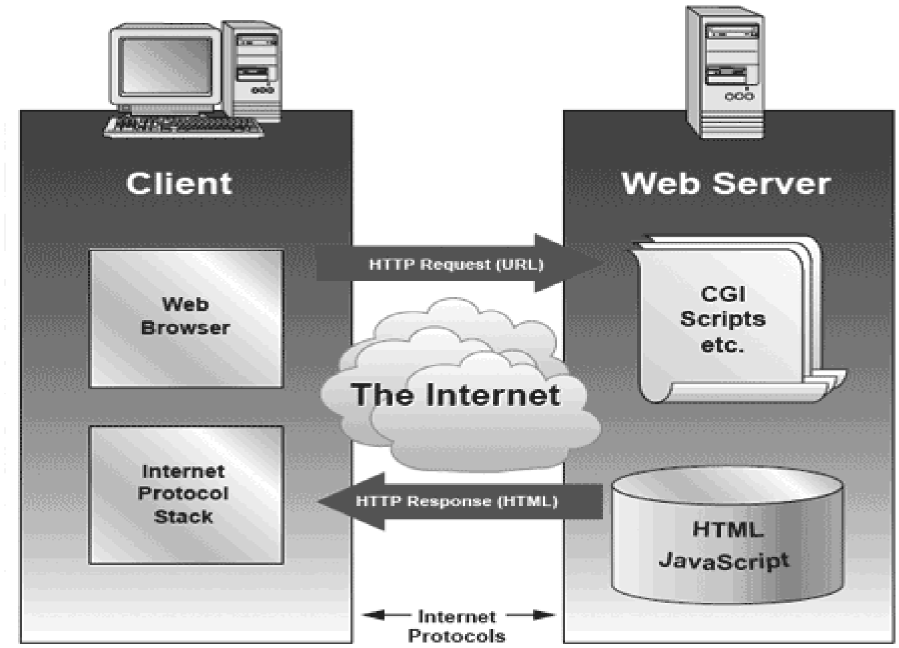

Figure 4.1.1

The content available at the web server may be static or dynamic. Static content is produced once and not changed or updated very often, for example a company presentation. Dynamic content is needed when the information provided by the service changes more often, for example timetables, news, stock quotes and account information. Technologies such as Active Server Pages (ASP), Common Gateway Interface (CGI), and Servlets allow content to be generated dynamically.

The WAP Model:

The figure below shows the WAP programming model. Note the similarities with the Internet model. Without the WAP Gateway/Proxy the two models would have been practically identical.

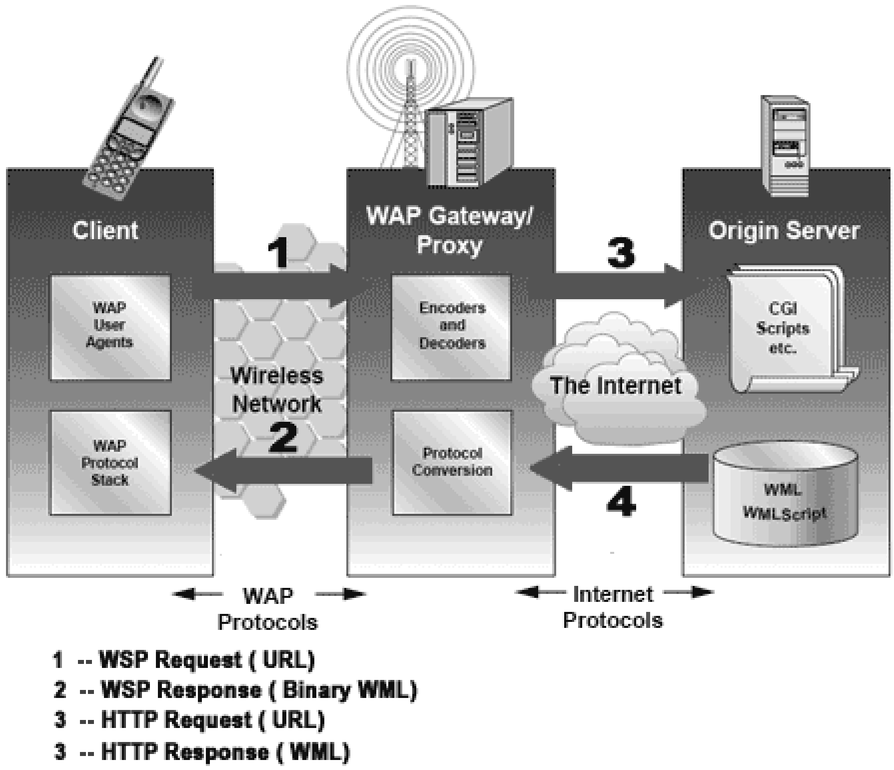

Figure 4.1.2

WAP Gateway/Proxy is the entity that connects the wireless domain with the Internet. You should make a note that the request that is sent from the wireless client to the WAP Gateway/Proxy uses the Wireless Session Protocol (WSP). In its essence, WSP is a binary version of HTTP.

A markup language - the Wireless Markup Language (WML) has been adapted to develop optimized WAP applications. In order to save valuable bandwidth in the wireless network, WML can be encoded into a compact binary format. Encoding WML is one of the tasks performed by the WAP Gateway/Proxy.

How WAP Model Works?

When it comes to actual use, WAP works like this:

1. The user selects an option on their mobile device that has a URL with Wireless Markup language (WML) content assigned to it.
2. The phone sends the URL request via the phone network to a WAP gateway, using the binary encoded WAP protocol.
3. The gateway translates this WAP request into a conventional HTTP request for the specified URL, and sends it on to the Internet.
4. The appropriate Web server picks up the HTTP request.

5. The server processes the request, just as it would 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.
6. The Web server adds the HTTP header to the WML content and returns it to the gateway.
7. The WAP gateway compiles the WML into binary form.
8. The gateway then sends the WML response back to the phone.
9. The phone receives the WML via the WAP protocol.
10. The micro-browser processes the WML and displays the content on the screen.

WAP Gateway

A **WAP gateway** sits between mobile devices using the WAP protocol and the World Wide Web, passing pages from one to the other much like a proxy. This translates pages into a form suitable for the mobiles, for instance using the Wireless Markup Language (WML). This process is hidden from the phone, so it may access the page in the same way as a browser accesses HTML, using a URL (for example, http://example.com/foo.wml), provided the mobile phone operator has not specifically prevented this.

As shown in the following figure, the WAP gateway acts as the bridge between the wireless network containing wireless clients and the computer network containing application servers.

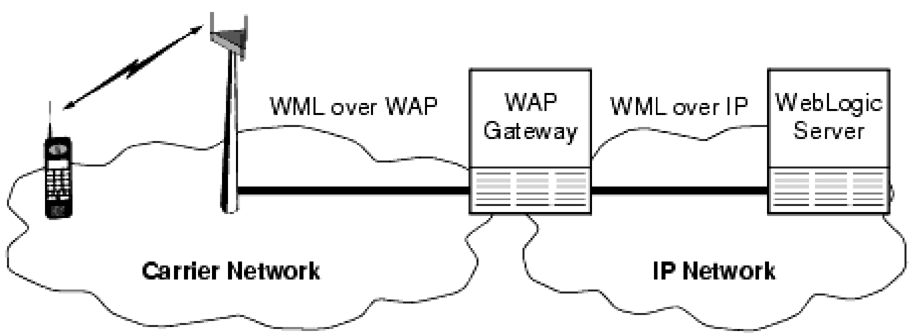

Figure 4.2.1 WAP Application Architecture

WAP Gateway Functionality

A WAP gateway typically includes the following functionality:

- Protocol gateway—the protocol gateway translates requests from the WAP protocol stack to the WWW protocol stack (HTTP and TCP/IP).
- Content encoders and decoders—the content encoders translate Web content into compact encoded formats to reduce the number and size of packets traveling over the wireless data network.

When a wireless client sends a request to a WAP application running on Web Logic Server, the request is first routed through the WAP gateway where it is decoded, translated to HTTP, then forwarded to the appropriate URL. The response is then re-routed back through the gateway, translated to WAP, encoded, and forward to the wireless client. This proxy architecture allows application developers to build services that are network and terminal independent.

WAP Gateway Security and Security Concerns

The security layer of the WAP protocol stack is called Wireless Transport Layer Security (WTLS). WTLS is based upon the established Transport-Layer Security (TLS) protocol standard.

For a secure connection employing the WAP protocol, a very small security risk exists at the WAP gateway during the switching of WTLS (WAP side) to SSL (IP side) and SSL to WTLS. Since the WAP protocol allows a session to be redirected from the carrier's gateway to the enterprise's gateway, an enterprise may want to control this minimal risk by including a WAP gateway behind its firewall. As shown in the following figure, the enterprise secures the server running the WAP gateway in a controlled environment to eliminate any exposure to the security risk.

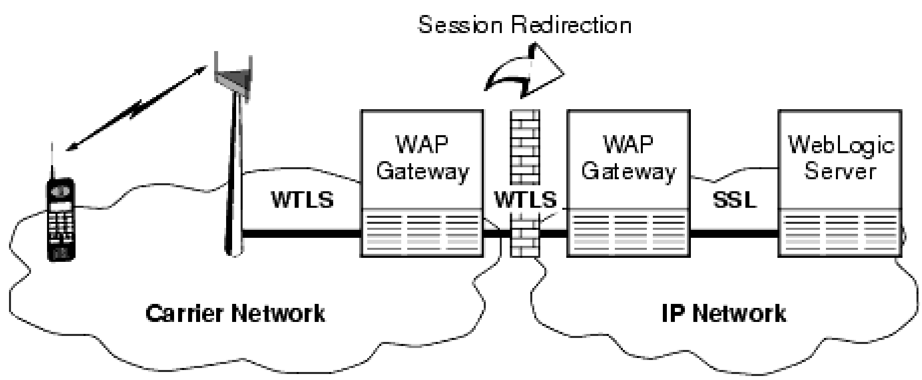

Figure 4.2.2 WAP Session Redirection

Since the carrier is a trusted entity and is continuously responsible for protecting voice, fax, computer and other types of data, enterprises probably do not need to host their own WAP gateway.

WAP Protocol

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

Application Layer

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

Session Layer

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

Transaction Layer

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

Security Layer

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

Transport Layer

Wireless Datagram Protocol (WDP). The WDP allows WAP to be bearer-independent by adapting the transport layer of the underlying bearer. The WDP presents a consistent data format to the higher layers of the WAP protocol stack, thereby offering the advantage of bearer independence to application developers.

Each of these layers provides a well-defined interface to the layer above it. This means that the internal workings of any layer are transparent or invisible to the layers above it. The layered architecture allows other applications and services to utilise the features provided by the WAP-stack as well. This makes it possible to use the WAP-stack for services and applications that currently are not specified by WAP.

The WAP protocol architecture is shown below alongside a typical Internet Protocol stack.

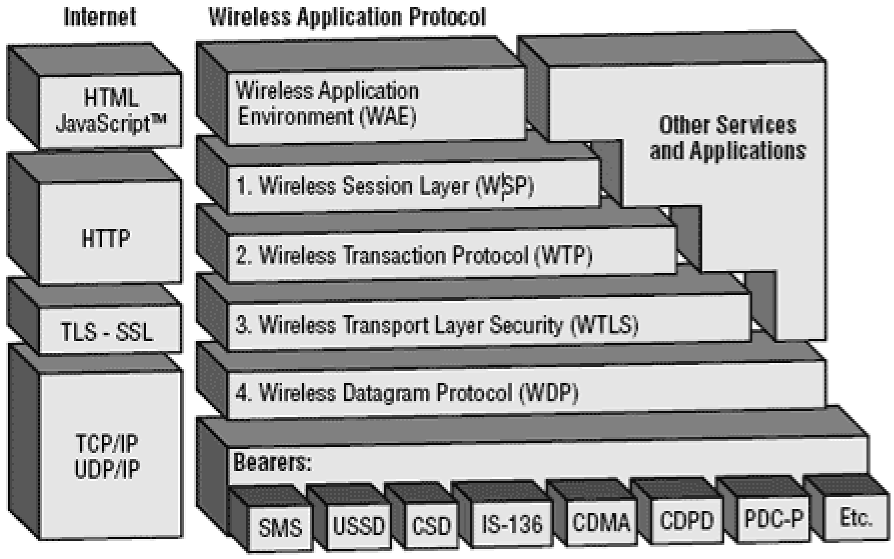

Figure 4.3.1

UAProf and Catching

The UAProf (User Agent Profile) specification is concerned with capturing capability and preference information for wireless devices. This information can be used by content providers to produce content in an appropriate format for the specific device. It is an XML document that contains information about the user agent type and device capabilities. It is a standard defined and maintained by the Open Mobile Alliance.

UAProf is related to the Composite Capability/Preference Profiles Specification created by the World Wide Web Consortium.

UAProf files typically have the file extensions rdf or xml, and are usually served with mimetype application/xml. They are an XML-based file format. The RDF format means that the document schema is extensible. User agent profiles are stored in a server called the profile repository. Very often a profile repository is maintained by a mobile device manufacturer. For example, the user agent profiles describing the capabilities of Nokia cell phones are stored in a profile repository maintained by Nokia.

A UAProf file describes the capabilities of a mobile handset, including Vendor, Model, Screensize, Multimedia Capabilities, Character Set support, and more. Recent UAProfiles have also begun to include data conforming to MMS, PSS5 and PSS6 schemas, which includes much more detailed data about video, multimedia, streaming and MMS capabilities.

A mobile handset sends a header within an http request, containing the URL to its UAProf. The http header is usually X-WAP-Profile:, but sometimes may look more like 19-Profile:, WAP-Profile: or a number of other similar headers.

UAProf production for a device is voluntary: for GSM devices, the UAProf is normally produced by the vendor of the device (e.g. Nokia, Samsung, LG) whereas for CDMA / BREW devices it's more common for the UAProf to be produced by the telecommunications company.

Wireless Bearer for Wap

WAP is in the air, both literally and figuratively. A mobile phone consortium called UnwiredPlanet has been working on WAP (Wireless Access Protocol) since May of 1995 in aneffort to establish the foundation for the mobile phone's version of the Web. After several false starts, that work seems to be bearing fruit this year: Nokia was caught by surprise at the demand for its first WAP-enabled phone, Ericsson is right behind with its model, and analysts are predicting that by 2002, more people will access the internet through mobile phones than through PCs. However, we've got to be careful when we tout WAP as the next major networking development after the Web itself, because it differs in two crucial ways: the Web grew organically (and non-commercially) in its first few years, and anyone could create or view Web content without a license. WAP, by contrast, is being pushed commercially from the jump, and it is fenced in by a remarkable array of patents which will affect both producers and consumers of WAP content. These differences put WAP's development on a collision course with the Web as it exists today.

Even after years of commercial development, the Web we have is still remarkably cross-platform, open to amateur content, unmanaged, and unmanageable, and it's tempting to think that that's just what global networks look like in the age of the internet. However, the Web is not just the story of the internet, it's also a story of the computing ecology of the 1990's. The Web has grown up in an environment where hardware is radically divorced from software: Anyone can install anything on their own PC with no interference (or even knowledge) from the manufacturer. The ISP business operates with a total separation of content and delivery: Internet access is charged by the month, not by the download. And most important of all, the critical pair of protocols -- http and HTML -- were allowed to spread unhampered by intellectual property laws. The separation of these layers meant that ISPs didn't have to co-ordinate with browser engineers, who didn't have to co-ordinate with site designers, who didn't have to co-ordinate with hardware manufacturers, and this freedom to innovate one layer at a time has been part and parcel of the Web's remarkable growth.

None of those things are true with WAP. The integration of WAP software with the telephone hardware is far tighter than it was on the PC. The mobile phone business is predicated on charging either per minute or per byte, making it much easier to charge directly for content. Most importantly, WAP's patents have been designed from the beginning to prevent anyone from creating a way to get content onto mobile phones without cutting the phone companies themselves in on the action, as evidenced by Unwired Planets first patent in 1995, the astonishingly broad "Method and architecture for an interactive two-way data communication network." WAP, in other words, offers a chance to rebuild the Web, without all that annoying freedom, and without all that annoying competition.

Many industries have looked at the Web and thought that it was almost perfect, with two exceptions -- they didn't own it, and it was too difficult to stifle competition. Microsoft's first versions of MSN, Apple's e-world, the pre-dot-com AOL, were all attempts to build a service which that grow like the Web but let them charge consumers like pay-per-view TV. All such attempts have failed so far, because wherever restrictions of either content creators or users were put in place, growth faltered in favor of the freer medium. With WAP, however, we are seeing our first attempt at a walled garden where there is no competition within a "freer" medium -- the Unwired Planet patents cover every mobile device ever made, which may give them the leverage to enforce its ideal of total commercial control of mobile internet access. If predictions of the protocol's growth, ubiquity, and hegemony are correct, then WAP may pose the first real threat to the freewheeling internet.

WAP Developer Kit

While still in its infancy, the Wireless Application Protocol has certainly generated a tremendous amount of interest. As WAP services are already beginning to appear in Europe and many more are on their way in North America and Asia, a variety of WAP vendors have also made available development tools that enable WAP application development and deployment. Please note that this is not a complete WAP tutorial. You can visit our WAP Training section for that information. In this review, we will examine three leading WAP development toolkits:

- Ericsson WapIDE 2.0
- Nokia WAP Toolkit 1.2
- Phone.com UP.SDK 4.0

While all three companies were instrumental in the formation of the WAP Forum, it is interesting to note that their development tools differ in many ways. It is also important to note that each of these companies sells commercial WAP servers which would probably be used in conjunction with their respective toolkit. We will delay a review of commercial WAP servers for a later issue.

Ericsson WapIDE 4.0

The Ericsson WapIDE product consists of a suite of tools that support the design and testing of WAP applications as well as the ability to design a new WAP device in order to test the device for look-and-feel issues. The WapIDE Software Development Kit is currently only available for Windows NT 4.0 and Windows 95/98. Included with the IDE are products for testing server applications. These products include Perl 5.0, Tcl/Tk, and the Xitami Web Server. Installing the WapIDE first requires the installation of the IDE followed by the installation of the SDK. I attempted to opt out of the Xitami Web Server installation (since I'm already running Microsoft IIS and Apache on my machine!) but the installation apparently failed at that point. I suppose one never knows when they might need three HTTP servers on one laptop! Figure 1 shows the WapIDE interface to the tools including the Browser (used to test applications), the App Designer (used to construct applications), and the Server Toolset (a set of tools including a WML/WMLScript compiler and a Syntax Analyzer).

It's not clear to me why the Server tools weren't simply included in the App Designer. It seems a bit disjointed to jump back and forth between applications in order to build code and then compile the code. The Browser (see Figure 4.6.2) supports the use of different devices (the R320s is the default) and allows the user to test the sample WAP URLs included with the toolkit or to test their own creations. A variety of sample WAP applications are included with the IDE for banking, stock quotes, and schedules.

Figure 4.6.2

The bulk of your time will be spent in the AppDesigner application. This tool integrates a WML editor with the WapIDE browser that coding and testing can be done within one application. It's a bare-bones development environment with no frills. The documentation is also a bit sparse although quite a few Adobe Acrobat documents are available for download from the Ericsson

WAP Developer site.

Other WAP products from Ericsson include the WAP Application Server (a Solaris-based Java application server designed to scale to 50,000 users that allows developers to build device-independent applications) and the WAP Gateway (an Intel platform-based product that acts as a server to a GSM network and bearers such as SMS and USSD).

Nokia WAP Toolkit 1.2

The WAP Toolkit 1.2 product from Nokia is similar in some respects to Ericsson's WapIDE. Both products contain graphical development environments (though neither one supports any type of of drag-and-drop UI creation), browsers, and WML/WMLScript compilers. The Nokia toolkit currently runs only on Windows NT 4.0 but note that the Nokia WAP Toolkit also requires a Java 2 runtime. You will want to make a visit to Sun's Java Web site to download either the Java 2 SDK or the Java 2 Runtime Environment (JRE) before evaluating the WAP Toolkit product.

After installation, the WAP Toolkit Program Group (under Windows) will contain shortcuts to the toolkit Integrated Development Environment (IDE) as well as excellent documentation on WAP, WML, WMLScript, and the toolkit itself. The toolkit application itself (see Figure 4) supports the creation, modification, and testing of WML/WMLScript code within one application.

Figure 4.6.3

The user can toggle between loading the WAP applications through HTTP or via a WAP gateway. Nokia also sells a separate Java Servlet-based WAP Server product. This Server incorporates the application server and WAP gateway functionality into one product. In all, the Nokia WAP products appear to be well-thought out and functional and is superior, from a user interface standpoint, to the Ericsson WapIDE product.

Phone.com UP.SDK 4.0

The Phone.com UP.SDK product (available for Windows 95/98/NT and Solaris) differs a bit from the Nokia and Ericsson product in that no graphical IDE is provided with the product. Instead of focusing on providing an integrated environment for editing and testing WML/WMLScript code, UP.SDK focuses much more heavily on providing a set of reusable code libraries for use with languages such as WML, Perl, C, C++, and Visual Basic. As Phone.com is the manufacturer of the leading WAP microbrowser, naturally the UP.SDK comes with a WAP browser known as the UP.Simulator (see Figure 4.6.4). Note that the Simulator is currently only available for the Windows platform.

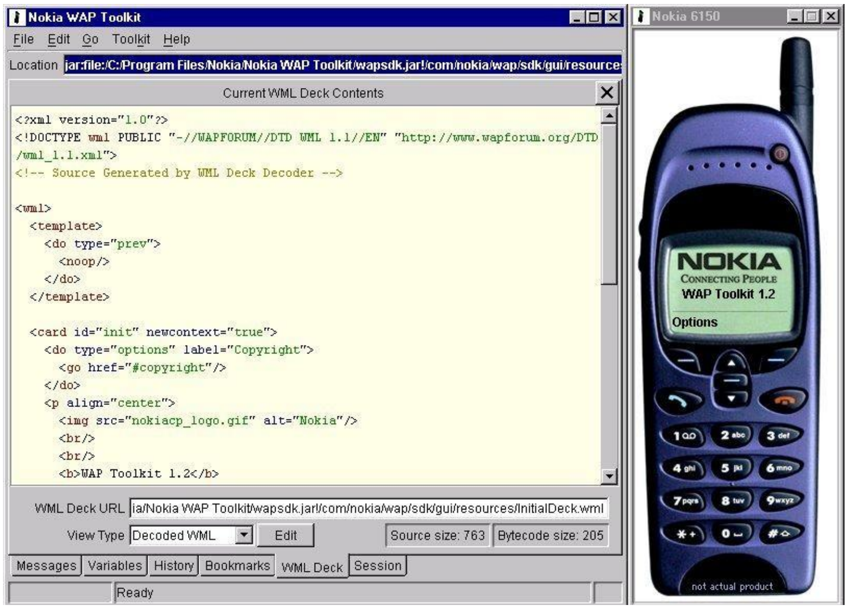

Figure 4.6.4

You will need a live Internet connection because the simulator actually dynamically connects to the Phone.com developer Web site. It does this in order to download samples and access live WAP applications on the Web. I definitely recommend checking this product out because it will give you a good feel for how WAP can be used (I was able to check my local weather and favorite stock quotes in a manner of seconds using the Up.Simulator). The UP.SDK also includes Perl and C library functions for generating WML and handling HTTP requests as well as C++ (Solaris) and COM (Windows) objects for notification, digest, and fax handling. The UP.SDK also includes tools for requesting and installing SSL certificates for security purposes. Besides providing the standard WAP functionality, Phone.com extends WAP's capabilities through fax and notification support. The UP.LINK server includes a Fax Manager product which allows handheld users to fax information directly from their WAP browser! Postscript, ASCII text, Microsoft Word, RTF, and Adobe Acrobat document types are accepted as fax or fax response formats. Asynchronous notifications can also be pushed to handheld clients via the Phone.com Notification API. This API allows the control of alerts, document cache, and decks on the client.

Mobile station application execution environment

In addition to the use of standardised network services (e.g. call forwarding, call barring, CCBS, call diversion etc.), MExE provides additional capabilities to control telephony events and manipulate standardised network services in a user-friendly manner.

A MExE handset provides the generic capability to negotiate and interact with services (in the form of applications and content) in servers, other handsets and internet/intranet WebPages etc. Further, MExE provides standardised execution environments to which 3rd party software developers may write services to execute directly in the MExE handsets.

MExE provides the user with a more sophisticated user interfaces (e.g. browsers) with a rich variety of MMI concepts to personalise,

Control and invoke services (e.g.. softkeys, icons, voice recognition etc.). Additionally downloaded services provide users with the capability to control the look and feel of services.

MExE also brings security to the support of 3rd party services in the wireless handset. With security domains reserved for network operators, handset manufacturers, and third parties , the source and content of downloaded services may be authenticated by the MExE client. The provision of such a security model enables the user to control whether services are installed, configure which functions may be performed by services, and to identify the extent of permissions granted to services. The protection of user data and resources help prevent attacks from potentially fraudulent services.

This annex gives an overview of how new 3rd generation services may be supported by MExE handsets, and gives some examples of possible services that may be supported on them. The ability to support some services may depend on the physical handset resources available to the MExE services, the classmark of the MExE client, and handset manufacturers may provide a range of handsets aimed at supporting different types of services.

Access to MExE services

There are several ways in which these new 3rd generation MExE services may be supported, and the following scenarios give an overview of the possible scenarios.

Services execute on remote servers

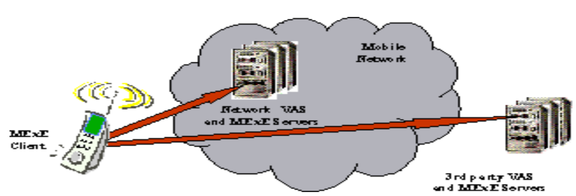

Figure 4.7.1

The services are provisioned and execute on remote servers, WebPages etc., to which the MExE client establishes a connection. The MExE client uses the services as provided by those remote servers. The MExE client effectively receives content (i.e. secured personal financial information) from the remote application which is presented to the user in the MExE client.

Application downloaded into the MExE client

The services are provisioned and execute on remote servers, to which the MExE client establishes a connection. The MExE client downloads an application which acts as a local browser to interact with the remotely provided service. The user interacts with and uses the remote servers via the downloaded application. An example of such a service would be access to an internet/intranet page.

Service downloaded into the MExE handset

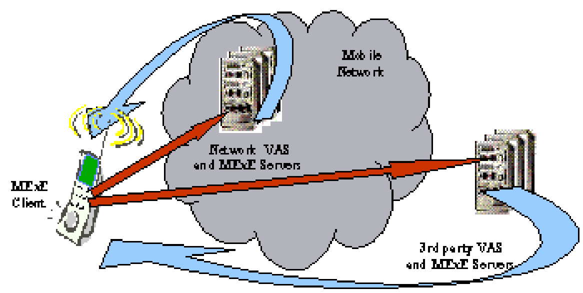

Figure 4.7.2

The services are available from remote servers, to which the MExE client establishes a connection. The MExE user downloads whichever services he desires from the remote servers, and installs, provisions and configures them on the MExE client. These services execute directly on the handset, without necessarily relying on servers to support the service. An example of such a service would be a game.

MExE handset to MExE handset services

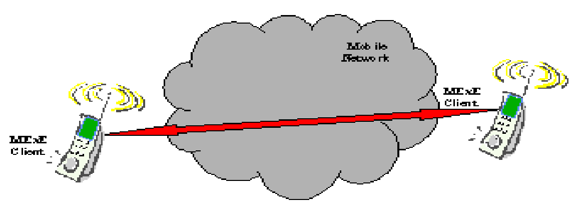

Figure 4.7.3

MExE handsets may wish to establish connections with each other to provide, receive and use interactive services. This direct MExE client to MExE client interaction of MExE services and any combination of the preceding scenarios may have been used to download services to the MExE client. These services may execute directly on the handset, without necessarily relying on servers to support the service. An example of such a service would be interactive games, sharing of calendar information, etc

UNIT 5

SPECIAL TOPICS

Third Generation Mobile Service

3G refers to the third generation of mobile telephony (that is, cellular) technology. The third generation, as the name suggests, follows two earlier generations.

The first generation (1G) began in the early 80's with commercial deployment of Advanced Mobile Phone Service (AMPS) cellular networks. Early AMPS networks used Frequency Division Multiplexing Access (FDMA) to carry analog voice over channels in the 800 MHzfrequency band.

The second generation (2G) emerged in the 90's when mobile operators deployed two competing digital voice standards. In North America, some operators adopted IS-95, which used Code Division Multiple Access (CDMA) to multiplex up to 64 calls per channel in the 800 MHz band. Across the world, many operators adopted the Global System for Mobile communication (GSM) standard, which used Time Division Multiple Access (TDMA) to multiplex up to 8 calls per channel in the 900 and 1800 MHz bands.

The International Telecommunications Union (ITU) defined the third generation (3G) of mobile telephony standards IMT-2000 to facilitate growth, increase bandwidth, and support more diverse applications. For example, GSM could deliver not only voice, but also circuit-switched data at speeds up to 14.4 Kbps. But to support mobile multimedia applications, 3G had to deliver packet-switched data with better spectral efficiency, at far greater speeds.

However, to get from 2G to 3G, mobile operators had make "evolutionary" upgrades to existing networks while simultaneously planning their "revolutionary" new mobile broadband networks. This lead to the establishment of two distinct 3G families: 3GPP and 3GPP2.

The 3rd Generation Partnership Project (3GPP) was formed in 1998 to foster deployment of 3G networks that descended from GSM. 3GPP technologies evolved as follows.

• General Packet Radio Service (GPRS) offered speeds up to 114 Kbps.

• Enhanced Data Rates for Global Evolution (EDGE) reached up to 384 Kbps.

• UMTS Wideband CDMA (WCDMA) offered downlink speeds up to 1.92 Mbps.

• High Speed Downlink Packet Access (HSDPA) boosted the downlink to 14Mbps.

• LTE Evolved UMTS Terrestrial Radio Access (E-UTRA) is aiming for 100 Mbps.

GPRS deployments began in 2000, followed by EDGE in 2003. While these technologies are defined by IMT-2000, they are sometimes called "2.5G" because they did not offer multi-megabit data rates. EDGE has now been superceded by HSDPA (and its uplink partner HSUPA). According to the 3GPP, there were 166 HSDPA networks in 75 countries at the end of 2007. The next step for GSM operators: LTE E-UTRA, based on specifications completed in late 2008.

A second organization, the 3rd Generation Partnership Project 2 (3GPP2) -- was formed to help North American and Asian operators using CDMA2000 transition to 3G. 3GPP2 technologies evolved as follows.

• One Times Radio Transmission Technology (1xRTT) offered speeds up to 144 Kbps.

• Evolution Data Optimized (EV-DO) increased downlink speeds up to 2.4 Mbps.

• EV-DO Rev. A boosted downlink peak speed to 3.1 Mbps and reduced latency.

• EV-DO Rev. B can use 2 to 15 channels, with each downlink peaking at 4.9 Mbps.

• Ultra Mobile Broadband (UMB) was slated to reach 288 Mbps on the downlink.

1xRTT became available in 2002, followed by commercial EV-DO Rev. 0 in 2004. Here again, 1xRTT is referred to as "2.5G" because it served as a transitional step to EV-DO. EV-DO standards were extended twice – Revision A services emerged in 2006 and are now being succeeded by products that use Revision B to increase data rates by transmitting over multiple channels. The 3GPP2's next-generation technology, UMB, may not catch on, as many CDMA operators are now planning to evolve to LTE instead.

In fact, LTE and UMB are often called 4G (fourth generation) technologies because they increase downlink speeds an order of magnitude. This label is a bit premature because what constitutes "4G" has not yet been standardized. The ITU is currently considering candidate technologies for inclusion in the 4G IMT-Advanced standard, including LTE, UMB, andWiMAX II. Goals for 4G include data rates of least 100 Mbps, use of OFDMA transmission, and packet-switched delivery of IP-based voice, data, and streaming multimedia.

Wireless Local Loop

In traditional telephone networks, your phone would be connected to the nearest exchange through a pair of copper wires.

Wireless local loop (WLL) technology simply means that the subscriber is connected to the nearest exchange through a radio link instead of through these copper wires.

What are the advantages of WLL over traditional wire-line connectivity?
In general, WLL is cheaper and quicker than copper wire connectivity. As the cost of copper rises over time and so does the cost of digging, this is likely to become an ever more significant advantage.

In a traditional wire-line network, the cost of the 'last mile' would amount to a substantial portion of the total cost of putting up the network.

This would be particularly true in remote locations with few subscribers or in difficult terrain. It is this part of the cost that WLL significantly reduces.

The economics of WLL thus works in its favour. WLL is also a more suitable technology for a quick rollout of a network as it bypasses digging ditches to lay copper wires.

This is a significant factor in crowded urban localities, where permission to dig may be almost impossible to get. Another major advantage of using a radio link for the last mile is that it considerably reduces the number of faults.

Close to 90% of all basic telephone faults occur in the last mile part of the network. With a radio link replacing the wires, these faults become almost negligible.

What are the major wireless access technologies?
There are various technologies like frequency division multiple access (FDMA), time division multiple access (TDMA) and code division multiple access (CDMA) used for WLL.

The one that is being used in India is CDMA. This is a full-fledged cellular mobile technology. In fact, it is the most dominant technology for mobile phone services in countries like the US and Korea.

If WLL is based on cellular technology, why are we talking of limited mobility?
This is a case of a regulatory restriction getting confused with a technology limitation. Government policy in India has laid down that fixed line operators will also be allowed to use WLL technology to offer mobility within a single billing area, or what is technically called a short distance calling area (SDCA), broadly equivalent to a single town or city.

However, they will not be allowed to offer mobile services with roaming facilities. This is a stipulation of the government, not a limitation of CDMA.

What is the reason for opposition to the introduction of WLL by cellular operators?

Again, it is not to the introduction of WLL per se, but to the concept of limited mobility that the cellular operators — who are based on the GSM technology, which is the dominant cellular mobile technology worldwide — are objecting.

Cellular operators say that the notion of limited mobility is farcical, firstly because it would be difficult to ensure that the mobility being offered remains 'limited'. More importantly, they point out, about 90% of all existing cellular subscribers in India do not use roaming facilities or move outside their SDCAs.

Thus, the mobility being offered by WLL operators is hardly limited for most customers and allowing limited mobility amounts to giving entry to another mobile operator in the circle.

But, you may ask, why is that objectionable. The cellular operators say it would not be if WLL operators — who are basic fixed line service providers — and cellular operators were given a level playing field in terms of licence fees, access charges and so on. They have gone to court challenging limited mobility.

Why are WLL tariffs so much lower than cellular tariffs if both are essentially mobile telephony?
Here again, there is a dispute. Cellular operators initially argued that WLL tariffs were set so low because basic service providers could cross-subsidise these from higher revenue shares from long distance calls.

Subsequently, the revenue shares from long distance calls were made the same for basic and cellular operators. Cellular operators now allege that the WLL tariffs (which are the same as fixed-line tariffs) are being maintained low as a "predatory pricing" tactic.

Basic service providers, on the other hand, insist that the tariffs involve no subsidy and that they have established this with the telecom regulator.

Bluetooth

During the past two decades, the advancement in microelectronics and VLSI technology dipped down the cost of many consumer electronic products to a level which was affordable for the common man. The first quarter of 2001, saw the vending of about 32.5 million PCs. The sale of cellular phones is predicted to reach 1 billion in 2005. With increase in the number of electronic devices, comes in the need of connecting them together for maximum interoperability and utilization. These devices connect with each other using a variety of wires, cables, radio signals and infrared light beams, and an even greater variety of connectors, plugs and protocols. Bluetooth is devised to replace these cables.

Bluetooth is a global standard for wireless connectivity. Bluetooth technology facilitates the replacement of the cables used to connect one device to another, with one universal short-range radio link operating in the unlicensed 2.45 GHz ISM band. The main objectives of Bluetooth technology can be described as follows,

- *Cable replacement*: Getting rid of the various types of cables and wires required for interconnectivity between various devices would enable the lay man to use all electronic devices without wasting time and money.
- *Small size*: the Bluetooth device is very small so that it can be attached to any device required like the cell phones without adding much to the weight of the system.
- *Low cost*: Bluetooth is aimed to be a low cost device approximately $5 in the near future.
- *Low power*: The utilization of power is very less (within 100 mW) as it is short range equipment and so it facilitates the use of small batteries for its usage.

Besides the characteristics mentioned above, Bluetooth can imitate a universal bridge to attach the existing data networks, and also as a mechanism for forming ad-hoc networks. Designed to operate in noisy frequency environments, the Bluetooth radio uses a fast acknowledgement and frequency hopping scheme to make the link robust.

HISTORY:

In 1994, Ericsson in Sweden launched an initiative to study a low-power, low-cost radio interface between mobile phones and their accessories. After three years, In 1997, Ericsson approached various manufacturers of mobile electronic devices to discuss the development and promotion of this short range wireless radio link as alone this phenomenon could not be implemented.

Thus in 1998, Ericsson, IBM, Intel, Toshiba and NOKIA formed the Special Interest Group (SIG) for the promotion and development of BLUETOOTH technology. The first Bluetooth silicon was also ready in 1998. As we can see that the SIG included two market leaders in mobile telephony, two in laptop computing and one in digital signal processing technology. The biggies being in the game gave an impetus to thousands of companies to join hands with the SIG for the endorsement and expansion of this technology.

One would wonder how Bluetooth got its name. It has an interesting heritage. Bluetooth is named after the 10^{th} century Viking King Harald Blatand (Blatand meaning Bluetooth). He was instrumental in uniting the countries in the Baltic region like Sweden, Denmark, Norway and thus emerging as a powerful force. Bluetooth aims at uniting the computing and telecommunication world and so achieving the same greatness.

WORKING OF BLUETOOTH:

Basically, Bluetooth is the term used to describe the protocol of a short range (10 meter) frequency-hopping radio link between devices. These devices implementing the Bluetooth technology are termed Bluetooth - enabled. Documentation on Bluetooth is divided into two sections, the Bluetooth Specification and Bluetooth Profiles.

- The **Specification** describes **how the technology works** (i.e. the Bluetooth protocol architecture),
- The **Profiles** describe **how the technology is used** (i.e. how different parts of the specification can be used to fulfill a desired function for a Bluetooth device).

BLUETOOTH PROTOCOL ARCHITECTURE:

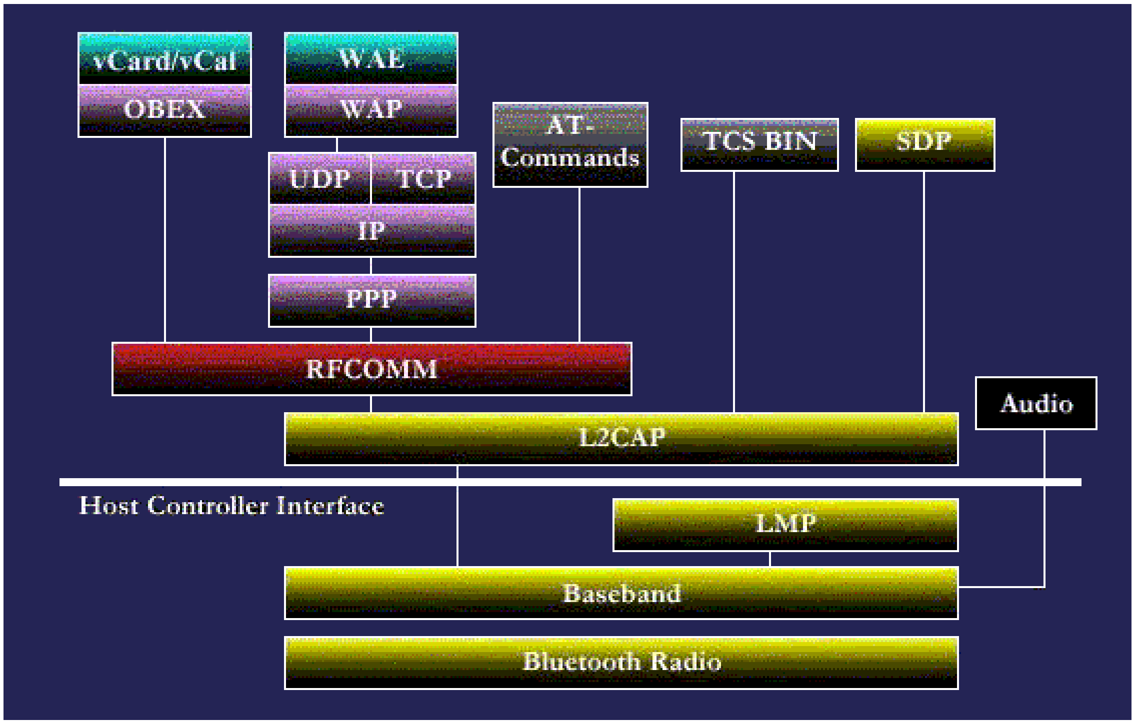

Figure 4.3.1

As the report is designed mainly for the spread spectrum techniques course, the protocols in the lower level are described more extensively and the upper layer protocols are just mentioned with a very brief description.

Moreover, one should note that the upper layer protocols are totally dependent on the lower level protocols whereas the lower level protocols can function independently even with a totally different set of upper protocols.

Bluetooth Radio: The Bluetooth Radio (layer) is the lowest defined layer of the Bluetooth specification. It defines the requirements of the Bluetooth transceiver device operating in the 2.4GHz ISM band. The Bluetooth air interface is based on three power classes,

- Power Class 1: designed for long range (~100m), max output power of 20 dBm,
- Power Class 2: ordinary range devices (~10m), max output power of 4 dBm,
- Power Class 3 short range devices (~10cm), with a max output power of 0 dBm.

The radio uses Frequency Hopping to spread the energy across the ISM spectrum in 79 hops displaced by 1MHz, starting at 2.402GHz and stopping at 2.480GHz.Some countries use the 79 RF channels whereas countries like Japan use 23 channels. Currently, the SIG is working to harmonize this 79-channel radio to work globally and has instigated changes within Japan, Spain, and other countries. Also, the Bluetooth radio module uses GFSK (Gaussian Frequency Shift Keying) where a binary one is represented by a positive frequency deviation and a binary zero by a negative frequency deviation. BT is set to 0.5 and the modulation index must be between 0.28 and 0.35. The receiver must have a sensitivity level for which the bit error rate (BER) 0.1% is met. For Bluetooth this means an actual sensitivity level of -70dBm or better.

Baseband: The Baseband is the physical layer of the Bluetooth. It manages physical channels and links apart from other services like error correction, data whitening, hop selection and Bluetooth security. As mentioned previously, the basic radio is a hybrid spread spectrum radio. Typically, the radio operates in a frequency-hopping manner in which the 2.4GHz ISM band is broken into 79 1MHz channels that the radio randomly hops through while transmitting and receiving data. A piconet is formed when one Bluetooth radio connects to another Bluetooth radio.

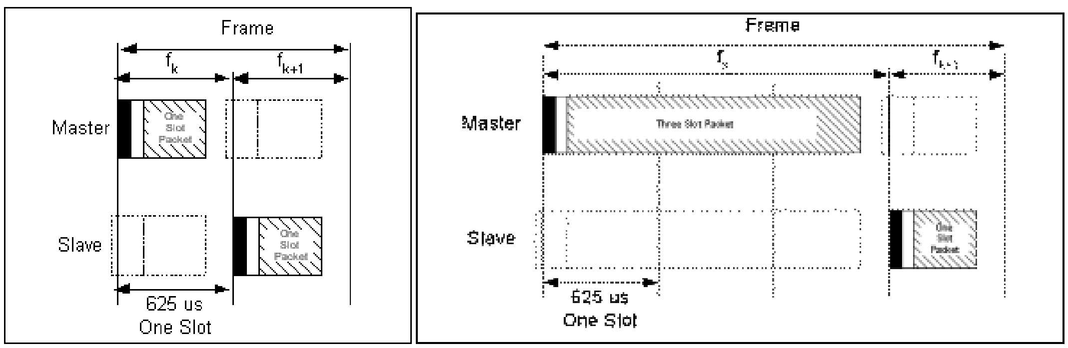

Figure 4.3.2

Both radios then hop together through the 79 channels. The Bluetooth radio system supports a large number of piconets by providing each piconet with its own set of random hopping patterns. Occasionally, piconets will end up on the same channel. When this occurs, the radios will hop to a free channel and the data are retransmitted (if lost). The Bluetooth frame consists of a transmit packet followed by a receive packet. Each packet can be composed of multiple slots (1, 3, or 5) of 625us. A typical single slot frame typically hops at 1,600 hops/second. Multi-slot frames allow higher data rates because of the elimination of the turn-around time between packets and the reduction in header overhead.

LMP: The Link Manager Protocol is used by the Link Managers (on either side) for link set-up and control.

HCI: The Host Controller Interface provides a command interface to the Baseband Link Controller and Link Manager, and access to hardware status and control registers.

L2CAP: Logical Link Control And Adaptation Protocol supports higher level protocol multiplexing, packet segmentation and reassembly, and the conveying of quality of service information.

RFCOMM: The RFCOMM protocol provides emulation of serial ports over the L2CAPprotocol. The protocol is based on the ETSI standard TS 07.10.

SDP: The Service Discovery Protocol provides a means for applications to discover which services are provided by or available through a Bluetooth device. It also allows applications to determine the characteristics of those available services.

PROFILES:

The profiles have been developed in order to portray how implementations of user models are to be accomplished. The user models describe a number of user scenarios where Bluetooth performs the radio transmission. A profile can be described as a vertical slice through the protocol stack. It defines options in each protocol that are compulsory for the profile. It also defines parameter ranges for each protocol. The profile concept is used to decrease the risk of interoperability problems between different manufacturers' products. For example: The Headset profile defines the requirements for Bluetooth devices necessary to support the Headset use case. The Fax profile defines to support the Fax use case. There are as many profiles as applications which are growing everyday.

TECHNICAL SPECIFICATIONS

SPECIFICATIONS	
Frequency band	2.4 GHz ISM band
Modulation	Gaussian shaped BFSK
Range	10 -100 m
Physical layer	FHSS
Coverage	Omni-directional. Non line of sight transmission
Data rate	1 Mbps/723 Kbps
Hopping rate	1600 hops/sec at 1 hop/packet
Channels	79/23 channels
Channel length	625 microseconds long
Data packet	Up to 2,745 bits in length
Reliable and secure	Good. Link layer authentication and encryption
Cost	$ 20 aims at $5 endpoint

Power	0.1 W (Active)
Acceptance	SIG have about 2500 member companies
Data / Voice support	One asynchronous data channel (732.2 kbps and reverse 57.6 kbps) OR Three simultaneous synchronous voice channels (64 kbps) OR Simultaneous asynchronous and synchronous channels.
Piconet	1 master and 7 slaves
Scatternet	Up to 10 piconets in a scatternet
Links	SCO and ACL links

ADVANTAGES

- Low Power Consumption
- Works in noisy environments
- No line of sight restriction
- Reliable and secure
- The 2.45 GHz ensures universal compatibility. Also complies with airline regulations
- The qualification and logo program ensure higher quality
- Very Robust as the radio hops faster and uses shorter packets

DISADVANTAGES

- Too many unfeasible applications so do we really need it ?
- No handoff / handover capability
- Initial stages so it needs to prove its worth
- Few analog or FH cordless phones have designed to operate at the 2.4GHz band. Certainly interference exists in between, but more serious effects would be exerted on analog 2.4GHz cordless phone
-

802.11	***Bluetooth***
Represents Internet	Represents faux internet
Already proved itself	Still to prove
Widespread connectivity	Connect at close proximity

APPLICATIONS

Bluetooth has a varied number of applications. Each application has a corresponding profile. Some of them are named as follows

- Mobile phones
- Laptops, desktops, pda's
- Digital cameras
- Printers
- Home networking
- Data access points
- Music
- Office equipment
- Medical
- Senior assisted living
- Child monitoring
- Wireless headsets
- Three-in-one phone, etc