DETERMINATION OF OPTIMAL CELL SIZE FOR MULTITIER WIRELESS CELLULAR SYSTEM

Dissertation Submitted to
JAWAHARLAL NEHRU UNIVERSITY
In partial fulfillment of requirements for the award of the degree of

Master of Technology
In
Computer Science & Technology

By
SANDEEP SINGH

GUIDED BY
PROF. C. P. KATTI

SCHOOL OF COMPUTER AND SYSTEMS SCIENCES
JAWAHARLAL NEHRU UNIVERSITY
NEW DELHI - 110067

DETERMINATION OF OPTIMAL CELL SIZE
FOR
MULTITIER WIRELESS CELLULAR SYSTEM

Dissertation Submitted to
JAWAHARLAL NEHRU UNIVERSITY
In partial fulfillment of requirements for the award of the degree of

Master of Technology
In
Computer Science & Technology

By
SANDEEP SINGH

GUIDED BY
PROF. C. P. KATTI

SCHOOL OF COMPUTER AND SYSTEMS SCIENCES
JAWAHARLAL NEHRU UNIVERSITY
NEW DELHI - 110067

CERTIFICATE

It is certified that the Dissertation entitled "Determination of Optimal Cell Size for Multitier Wireless Cellular System", being submitted by Sandeep Singh, for the award of degree of Master of Technology in Computer Science & Technology, School Of Computer & Systems Sciences, Jawaharlal Nehru University, New Delhi, is a record of his own work carried out by him under my supervision and guidance.

I recommend his dissertation for the above degree.

C P Katti

Prof. C. P. Katti

School of Computer & Systems Science,

Jawaharlal Nehru University,

New Delhi – 110067

P C Saxena

Prof. P. C. Saxena 5/1/99

Dean,

School of Computer & Systems Sciences,

Jawaharlal Nehru University,

New Delhi – 110067

DECLARATION

I hereby declare that the dissertation entitled "Determination of Optimal Cell Size for Multitier Wireless Cellular System", is my original work and has not been submitted elsewhere towards the award of any degree, diploma or certificate.

I take complete responsibility for the authenticity of the work.

Dated : New Delhi

Place : 05/01/99

Sandeep Singh

Dedicated to my

Parents

ACKNOWLEDGEMENT

It is my immense pleasure to express thanks and obligations to all those who have been sinequanon to this dissertation.

I wish to begin this note of thanks by expressing my heart-felt gratitude and acknowledge to Prof. C. P. Katti, School of Computer and Systems Sciences, J.N.U., for his valuable guidance and inspiration given to me, without which the completion of this dissertation would have been impossible.

I am also deeply indebted to Dr. P. C. Saxena, Dean, School of Computer and Systems Sciences, for permitting me to undertake this project and helped me with his numerous valuable suggestions with which I acquired a wider perspective. Moreover, he remains a constant source of encouragement and gives a professionally competent advice during the whole work.

My sincere thanks is also due to Mr. Jugal Kishore Sharma, Research Engineer, C-DOT, who helped me to get deeper and practical insight into the mode of functioning of Wireless Networks and mainly the CELLULAR Networks.

I am also extremely thankful to all the faculty members for their kind cooperation and needful help.

Last but not the least, I thank all my colleagues for their kind assistance. Their devotion and dedication is really fantastic and the credit goes to them for the successful completion of this dissertion.

Sandeep Singh

CONTENTS

ABSTRACT

The goal of Personal Communication Services (PCS) is to provide the integrated communication (e.g., voice, video and data) between nomadic subscribers independent of time, location and mobility patterns.

Multitier Architectures are economical in situations when there are mobiles characterized by different mobility patterns, running with a different quality of service(QoS) requirements and having substantially different call arrival density and average holding time.

The Cellular System for the next generation of Wireless Multimedia Network will rely on cell's size that is smaller than those used today.

The size of cell depends on

-Mobile's speed.

-System's load.

-Required Quality of Services(QoS).

When there are multiple Mobility classes it is useful to consider cell splitting which results in a Multitier System. Manufacturers always feel uncomfortable in deciding the cell size in Multitier Wireless Cellular System. Therefore there is necessity to give the solution for the determination of optimal cell size in a Multitier Wireless Cellular System.

Chapter - 1

Introduction

Communication has become a fundamental part of the society of late. The age has come where people want a fast and better way, to communicate with others. We are in the age where communication is more important than ever before. Basically a communication is a temporary relationship between telecommunication users, for the purpose of exchanging information. A communication makes use of the transmission chain established through networks between users. There is increasing competition from a system that uses radio waves instead of wires and fibers for communication. This system will play an increasingly important role in the networking of notebook computer, shirt-pocket telephones, and personal digital assistants in the coming years.

1.1 Mobile Communication

Mobile communication is nothing but a medium of communication between two mobile users. Mobile communication is one such issue, which is growing rapidly at present. The social mobility of previous years is changing into physical and transportational mobility. More people travel by car, by airplane, for business and pleasure. In this type of today's world, people tend to evolve new ways and methods in order to suit their needs. New technologies get evolved. Mobile communication has also been evolved by the people to fulfil their needs.

When Marconi turned theory into practical reality in 1894, he had already seen the commercial possibility for a system of telegraphy, free from the limitations of wires. A century later, the invention of the transistor has led to the ability for anyone to communicate while on the move.

Nowadays, It is a purely matter of convenience to receive and make calls at your leisure, at any time and any place. The mobile phone has become a fashionable and everyday object.

In this "information age", most businessmen find it necessary to access data (such as files) while on the move. Rather than using a fixed terminal, which might not be available at the time, portable computers, directly connected to a cellular network, are more convenient especially for those who do a lot of travelling. These portable computers could be used to send and receive faxes, e-mails and other forms of data.

1.2 Problem Definition

The main aim of my project is to Determine the Optimal Cell Size for a Multitier Wireless Cellular System. Since cell size play a major role for the selection of Cellular System according to cost point of view. When there are different types of mobility patterns, Cell splitting becomes necessary for fast and reliable communication. The cell splitting is the main cause for the generation of tier concept in Cellular System. Tier is nothing but a large geographical area covered by equally sized cell. Multitier Cellular System is a system in which we combine different cells in separate groups according to their size.

1.3 Organisation of Dissertation

The entire dissertation is divided in to seven chapters. The first chapter describes the introduction about Mobile Communication and overview of my project topic. Second chapter describes about cellular system. In this chapter, I have given the historical background, basic concept, and the equipment necessary to make the proper functioning of cellular system. Finally, in this chapter I tried to emphasis more on the heart of Cellular System that is, cell.

The third chapter discusses about the operation of cellular system (more specifically, the Global System for Mobile Communication). Here I have presented an overview of the GSM including the architecture, channel, and frame structure, speech processing, and typical call flow scenarios.

Fourth chapter discusses about the different types of Cellular System according to trunking concept.

According to trunking radio system, cellular system can be categorised while keeping following points in mind:

- Frequency
- Time
- Space
- Code

Fifth chapter discusses about the security features of GSM, that is to say the protective measures against fraud or eavesdropping on the radio interface.

Sixth chapter discusses about my proposed approach of this project. It discusses the Multitier Wireless Cellular System. In this chapter, I have given the algorithm for optimal system design with optimal cell size. Here, I have also given a network model, which provide the solution of this project problem.

The last chapter concludes the dissertation. Further it gives a brief scope and extenuation to the proposed solution.

Chapter - 2

Cellular System

2.1 *Historical Background*

The mobile communications industry started in 1921 when two-way radios were installed in the cars of the Detroit Police Department. This equipment was bulky and awkward to use, but it allowed the departments scout cars to keep in touch with headquarters.

Soon private individuals realized that they could benefit from mobile communications. The first commercial radio telephone service was introduced to the general public in St. Louis in 1964. No direct dialing capabilities were available. Therefore calls to and from mobile subscribers were routed through special operators.

There were long waiting periods to become a subscriber and once service was obtained, users often experienced long delays because only a small number of channels (radio frequencies) were available. Mobile units used a single channel, push-to-talk system that allowed only one person to speak at a time.

Although the creative thinkers at Bell Laboratories proposed the advanced computer technology necessary to make cellular communications a reality in 1946, AT&T did not introduce Improved Mobile Telephone Service (IMTS) until 1964. This service enabled subscribers to dial their calls without first reaching an operator. Channel selection was automatic and wait time was considerably reduced. Although an improvement, IMTS was still limited to 44 radio frequencies and only a few people could use the system at any one time.

Lack of system capacity remained a problem, and in 1971, AT&T fielded a proposal for the development of commercial radio telephone utilizing the 800 MHz frequency band, later to be named the cellular system. Chicago was chosen as the first city to test the cellular system. The first cellular radio system was named AMPS, Advanced Mobile Phone Service, began operations in 1978 and worked perfectly, as did another system built in Washington, DC/Baltimore area in 1981. When the Federal Communications Commission (FCC) authorized cellular service in 1982, a new wireless industry was born.

2.2 *Basic concept*

A cellular mobile telephone system is in reality a highly sophisticated two-way radio system. It is called "cellular" because the system is made up of much low-power wireless or radio transmitters, each of which is at the heart of a small geographic coverage area called a "cell". Each of these "cells" combines to create the larger "cellular system" that provides coverage for a city or metropolitan area. It takes its name from the fact that conceptually, the system is like a honeycomb made up of many hexagonal cells. The system is often graphically depicted that way. In reality the actual shape and size of individual cells may vary depending on terrain and location. Additionally, variable power levels allow cells to be sized according to the subscriber density and demand within a particular region.

Prior to the concept of the cellular system, two-way radio or mobile telephone communications operated much as television or radio broadcasting does today. One very powerful transmitter or transceiver, located at the highest spot in an area would broadcast in a radius of up to fifty kilometers. This severely limited the amount of two-way radio or mobile telephone traffic that could occur in that area on any channel or system of radio frequencies. If one person was using a particular channel, no one else in that fifty-kilometer radius could use it.

The "cellular concept" structured the mobile telephone network in a different way and allowed for greater volume on and the more efficient use of a frequency spectrum. Instead of using one powerful transmitter, many low-power transmitters were placed throughout a coverage area. For example, by dividing a metropolitan region into one hundred different areas (cells) with low-power transmitters using twelve conversations (channels) each, the system capacity theoretically could be increased from twelve conversations -- or voice channels using one powerful transmitter -- to twelve hundred conversations (channels) using one hundred low-power transmitters.

This concept only became viable, however, when technology was developed that allowed for the seamless transfer of a phone call from one cell to another. So that the call could continue uninterrupted as the caller traveled across numerous cells. Highly sophisticated computer 'switches' made that possible. As mobile users travel from cell to cell, their conversations are "handed off" between cells in order to maintain seamless service. Channels (frequencies) used in one cell can be reused in another cell some distance away. Cells can be added to accommodate growth, creating new cells in unsaved areas or overlaying cells in existing areas.

2.3 Elements of Cellular System

The equipment's which play a major role in the operation of cellular system are given as follows:

2.3.1 Mobile Station Terminal Equipment

The best known part of the cellular network is certainly the mobile station. Different types of stations are distinguished by power and application. Fixed mobile station are permanently installed in a car and may have a maximum allowed RF output power of up to 20W. Portable units (bag phones) can transmit up to 8W and hand portable units up to 2W. Hand portable units are becoming much smaller and are not much larger than analog units.

2.3.2 Subscriber Identity Module

The subscriber identity module (SIM) provides mobile equipment with an identity. Without a SIM, a mobile is not operational (except for emergency calls). The SIM is a smart card and has a computer and memory chip permanently installed in a plastic card the size of credit card. This has to be inserted into a reader in a mobile station before the mobile terminal can be used for its intended routine purposes. For very small hand potable phones, the credit card type is too large. There is, therefore, a small version of SIM, called the *plug-in* SIM.

Certain subscriber parameters are stores on the SIM card, together with personal data used by the subscriber, such as personal phone numbers. The SIM card identifies the subscriber to the network. Since only a SIM can personalize a phone, it is possible to travel abroad, taking only the SIM card, rent a mobile phone at the destination, and then use the phone (with the SIM card inserted) just as if it were a personal mobile phone at home. Anyone may reach a subscriber using a subscriber's home number. Every phone call, from wherever it is placed, is billed to subscriber's home account.

Short message received from the network may also be stored on the card. The recent introduction of larger memories and better microprocessors will make the SIM card even more flexible and powerful in the future, combining it with different services, such as credit and service cards.

To protect the SIM card from improper use, a security feature is built in. Before they can use the mobile, users have to enter a four digit *personal identification number* (PIN). The PIN is stored on the card. If the wrong PIN is entered three times in a row, the card blocks itself, and may only be unblocked with an eight digit personal unblocking key (PUK), which is also stored on the card.

2.3.3 Base Transceiver Station

The counterpart to a mobile station within a cellular network is the base station transceiver (BTS), which is the mobile's interface to the network. A BTS is usually located in the center of cell. The transmitting power of BTS determines the absolute cell size. A base station has between one and sixteen transceiver, each of which represents a separate RF channel.

2.3.4 Base Station Controller

The base station controller (BSC) monitors and controls several base station, the number of which depends on the manufacturer and can be between several hundreds of stations. The chief tasks of BSC are frequency administration, the control of a BTS, and exchange functions. The hardware of BSC may be located at the same site as the BTS, at its own standalone site, or at the site of mobile switching center (MSC). BSC and BTS together form a functional entity sometimes referred to as the *base station subsystem* (BSS).

2.3.5 Gateway Mobile Services Switching Center

The *gateway mobile services switching center* (GMSC) is the interface of the cellular network to the PSTN. It is a complete exchange, and with all its registers it is capable of routing calls from the fixed network- via the BSC and the BTS- to an individual mobile stations. The GMSC also provides the network with specific data about individual mobile stations. Depending on the network size, an operator might use several interfaces to fixed network, thus using several GMSCs or only one. If the traffic within cellular network requires more exchange capacity than the GMSCs can provide, additional mobile service switching center (MSC) might coexist with no access to the fixed network. If not otherwise explicitly distinguished from each other, the capabilities of the GMSC and the MSC are the same. A major difference between the two is that the MSC has no related home location register (HLR).

2.3.6 Operation and Maintenance Center

The operation and maintenance center (OMC) has access to both the (G) MSC and the BSC, handles error message coming from the network, and controls the traffic load of the BSC and the BTS. The OMC configures the BTS via the BSC and allows the operator to check the attached components of the system. As the cells become smaller and the number of base stations increases, it will not be possible in the future to check the individual stations on the regular basis for transceiver quality. Therefore it is important to put remote control of the maintenance in place to save costs, but still maintain the quality of the system. This is supported by better self-test functions in the BTS. The distribution of the maintenance tasks is treated differently by different manufacturers.

2.3.7 Home Location Register

The HLR stores the identity and user data of all the subscribers belonging to the area of related GMSC. These are permanent data such as the *International Mobile Subscriber Number* (IMSI), the *Authentication key*, the subscriber's permitted supplementary services and some temporary data.

The IMSI is permanently stored on the SIM card. The IMSI is one of the pieces of important information used to identify a subscriber within the GSM system. The first three digits of the IMSI identify the *mobile's country code* (MCC) and the next two digits are the *mobiles network code* (MNC). Up to ten additional digits of the *mobiles subscriber identification number* (MSIC) completes the IMSI.

The following IMSI:

262 02 454 275 1010

identifies a subscriber from Germany (MCC = 262), who is paying his or her monthly bill to the private operator d2 private (MNC = 02). The subscribers network identity number (MSIC) is 454 275 1010.

The number with which the subscriber may be reached from the public network is totally different from the IMSI, and starts with an area code of 0172, followed by a seven-digit subscriber number. The first digit of this subscriber number identify the subscriber related HLR. The number of digits used for this purpose is dependent on both the network size and the number of HLRs in the network. The IMSI is only used for internal network purposes.

2.3.8 Visitor Location Register

The VLR contains the relevant data of all mobiles currently located in a serving (G) MSC. The permanent data are the same as data found in the HLR; the temporary data differ slightly. E.g. the VLR contains the *temporary mobiles subscriber identity* (TMSI), which is used for limited periods of time to prevent the transmission of the IMSI via the air interface. The substitution of the TMSI for the IMSI serves to protect the subscriber from high-technology intruders and helps point to the location of the mobile station through the cell identity.

The subscriber's data are present at two locations (i.e. at VLR as well as at HLR).

The reason for storing two identical data at two different locations is given below:

1. It reduces the data traffic to HLR, because it is not necessary to ask for these data every time they are needed.
2. Another reason for storing at two locations is that each serves a different purpose. The HLR has to provide the GMSC with the necessary subscriber data when a call is coming from the public network. The VLR, on the other hand serves the opposite function, providing the host (G) MSC with the necessary subscriber data when a call is coming from a mobile station (e.g., during authentication).

2.3.9 Authentication Center

The *Authentication Center* (AC) is related to the HLR. It provides the HLR with different set of parameters to complete the authentication of a mobile station. The AC knows exactly which algorithm it has to use for a specific subscriber in order to calculate input values and issue the required results.

2.3.10 Equipment Identity Register

The *equipment identity register* (EIR) is an option up to the network operator to make use. The implementation of the EIR is a relatively new security feature of the GSM system. Within the EIR we find all the serial numbers of mobiles equipment that is either stolen or, due to some defect in their hardware, may not be used in a network. The *international mobile equipment identity* (IMEI) is not only the serial number of a certain mobile station, but it also reveals the manufacturer, the country of production, and type approval. The idea is to check the identity at each registration or call setup of any mobile station, and then, depending on its IMEI, admit or bar access of the mobile station to the system.

2.4 Cell Concept

The heart of the cellular system is made up of individual radio coverage areas called "cells." Each cell is a self-contained calling area. Within the cell, a cell site is strategically positioned as a base station for receiving, sending, and routing the transmitted radio signals of cellular phone calls.

Each base station consists of several transmitter/receivers (perhaps as many as 96 depending upon the antennas deployed), controllers, and an antenna array specifically designed for the requirements of the cell it serves. The antennas are mounted on towers or structures such as water towers or buildings, typically at heights from 50 to 200 ft.

There are two types of antennas. Sector antennas, which look like one by four-foot rectangular panels, serving an area of the cell shaped like a slice of pie, or omnidirectional antennas, which resemble poles ten to fifteen feet in length. Sector antennas are usually arranged in three triangular groups of three. Two of the three in each group are used to receive signals and one to transmit. When omnidirectional antennas are used some transmit and some receive signals.

The cell site's transmitter is low powered and does not reach much beyond that cell's boundaries. That makes it possible to reuse channels (frequencies) -- a given channel can be used at the same time in different cells, as long as the cells do not border one another, without causing signal interference. This is particularly valuable in urban areas where lots of cellular phones are in use at the same time.

Different possibilities of cell planning have been developed which can be categorise as given below:

2.4.1 Cell-splitting or Microcell Applications

As the number of subscriber grew larger, the density within the specified area became higher. The operators and radio engineers had to look for new capacity funds.

A rather basic idea was to split the existing space into smaller portions, thus multiplying the number of channels available (Fig. 2.1 & Fig. 2.2). Along with this simple scheme, the power levels used in these cells decreased, making it possible to reduce the size of batteries required for mobile stations.

2.4.2 Selective Cell

It dose not always make sense to have circular cells. Radio engineers designed cells with a wide verity of shapes, together with the required antennas, which are able to confine transmitted power within a particular area and exclude power from adjacent areas. The most common of these selective coverage schemes is the sectored cell, where coverage is confined to individual 120-deg sectors rather than the typical full 360-deg coverage. Such antennas may be located at the entrances of tunnels, on the edge of the valley, or at the ends of streets among skyscrapers.

2.4.3 Umbrella Cells

In this, power is transmitted at a higher power level than it is within the underlying microcells and at a different frequency. This means that when a mobile that is traveling at a high speed is detected as a fast mover, it can be handed off to the umbrella cell rather than tie up the network with a fast series of handoffs. Such a mobile can be detected from its propagation characteristics or distinguished by its excessive handoff demands. In this cell mobile can stay for a longer period of time, thus reducing the workload for the network.

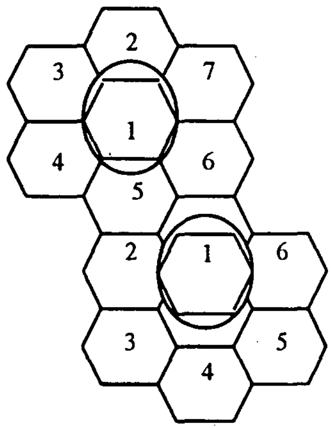


Fig.2.1 Cellular Structure

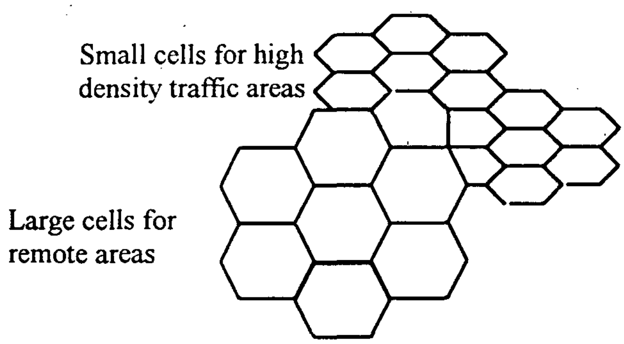


Fig.2.2 Cell Splitting And Microcells

3.1 GSM Architecture

A series of functions are required to support the services and facilities in the GSM PLMN (Public Land Mobile Network). The basic subsystems of GSM architecture are:

- Base Station Subsystem (BSS)
- Network and Switching Subsystem (NSS)
- Operational Subsystem (OSS)

The BSS provides and manages the transmissions paths between the mobile stations (MSs) and the NSS. This includes management of radio interface between MSs and the rest of the GSM system. The NSS has the responsibility of managing communications and connecting MSs. The NSS is not in direct contact with the MSs. Neither is the BSS in direct contact with external networks. The MS, BSS and the NSS form the operational part of the GSM system. The OSS provides the means for a service provider to control them. Figure 3.1 shows the model for the GSM system.

In the GSM, interaction between the subsystems can be grouped into two main parts:

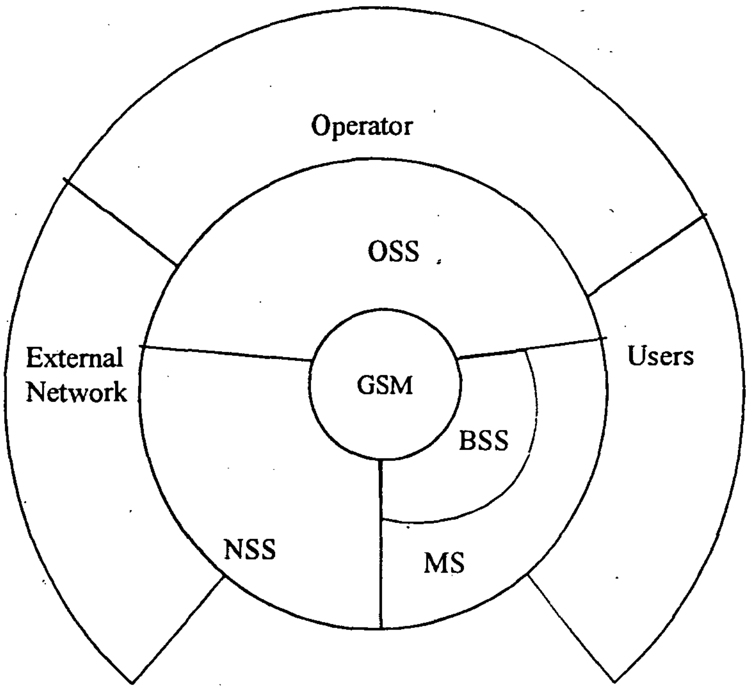
Operational part:

external network <->NSS <-> BSS <-> MS <-> user

Control part:

OSS <-> service provider

The operational part provides transmissions paths and establishes them. The control part interacts with the traffic-handling activity of the operational part by monitoring and modifying it to maintain or improve its functions.



BSS: Base Station Subsystem
NSS: Network and Switching Subsystem
OSS: Operational Subsystem
MS: Mobile Station

Fig.3.1 *Model of the GSM System*

3.2 *GSM Subsystem*

When the mobile unit is active (i.e. when a mobile phone is switched on), it registers with the appropriate BS, depending on its location, and its cell position is stored at the responsible MSC. When a call is set-up (when a user makes a call), the base station monitors the quality of the signal for the duration of the call, and reports that to the controlling MSC, which in turn makes decisions concerning the routing of the call.

When a cellular phone moves from one cell to the other, the BS will detect this from the signal power and inform the MSC of that. The MSC will then switch the control of the call to the BS of the new cell, where the phone is located. This is called handover . It normally takes up to 400ms, which is not noticeable for voice transmission.

A cellular phone user can only use his/her mobile within the covered area of the network. Roaming is the capacity of a cellular phone, registered on one system, to be able to enter and use other systems. Those other systems must be compatible to enable roaming (i.e. they must have the same type of networks). In Europe, the standard cellular network is called GSM (Global System for Mobile Communication). Incoming calls to GSM users are routed to them, irrespective of where they are, as long as they are within Europe.

3.3 *Mobile Station*

The MS consist of physical equipment used by the subscriber to access a PLMN for offered telecommunication services. Functionally the MS includes a Mobile Termination (MT) and, depending on the services it can support, various Terminal Equipment (TE) and combinations of TE and Terminal Adapter (TA) functions (TA acts as a gateway between the TE and MT).

(fig 3.2 and 3.3). Mainly there are three types of MS such as

- Vehicle-mounted station.
- Portable station.
- Handheld station.

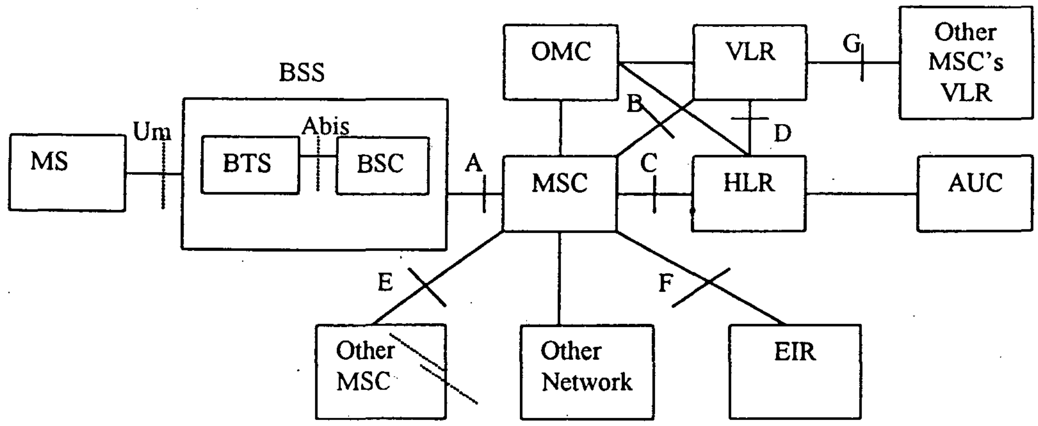
MSs come in five power classes that define maximum RF power level that the unit can transmit.

Table 9.4(same book) provides the maximum RF power for various classes. Vehicular and portable units can be either class I or class II, whereas handheld units can be class III, IV and V.

Basically, an MS can be divided into two parts.

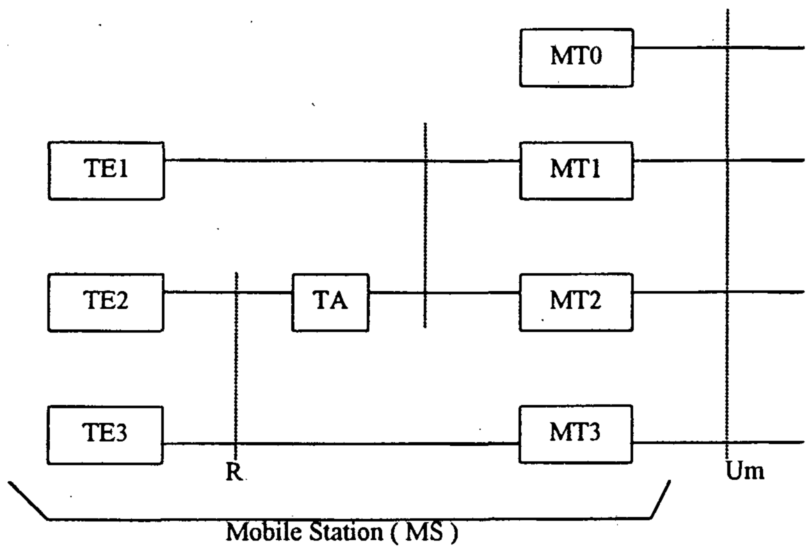
- The first part contains the hardware and software to support radio and man machine interface functions and is available at retail shops to buy or rent.
- The second part contains terminal/ user specific data in the form of a smart card (SIM card), which can effectively be considered a sort of logical terminal.

An MS has a number of identities, including the International Mobile Equipment Identity (IMEI), the International Mobile Subscriber Identity (IMSI), and the ISDN number.



MS : Mobile Station
BSS: Base Station Subsystem
BTS: Base Transceiver Station
BSC: Base Station Controller
MSC: Mobile Service Switching Center
OMC: Operations and Maintanance Center
HLR: Home Location Register
VLR: Visitor Location Register
EIR: Equipment Identity Register
AUC: Authentication Center

Fig.3.2 GSM Reference Model



MT: Mobile Termination
TE: Terminal Equipment
TA: Terminal Adapter

Fig.3.3 Functional Model of a Mobile Station

3.3.1 *Base station Subsystem*

The BSS is the physical equipment that provides the radio coverage to prescribed geographical areas, known as the cells. It contains the equipment required to communication with the MS. Functionally a BSS consists of: a control function carried out by the base station controller (BSC) and a transmitted function performed by base transceiver station (BTS). The BTS is the radio transmission equipment and covers each cell. A BSS can serve several cells because it can have multiple BTSs.

The BTS contains the Transponder Rate Adopter Unit (TRAU). In TRAU, the GSM specific speech encoding and decoding is carried out, as well as the rate adoption function for data. In certain situations TRAU is located between the BSC and the mobile service switching center (MSC) to gain an advantage of a more- compressed transmission between the BTS and the TRAU. Interface between the BTS and the BSC is Abis. The interface between the MS and BSS is air interface (Um).

3.3.2 *Networking and Switching Subsystem*

The NSS includes the main switching functions of the GSM, databases required for the subscribers, and mobility management. Its main role is to manage the communications between the GSM and other network users. Within the NSS, the switching functions are performed by the MSC. Subscriber information relevant to provisioning of services is kept in the Home Location Register (HLR). The other database in the NSS is the Visitor Location Register (VLR).

3.3.3 *Operation and Maintenance Subsystem (OMSS)*

The OMSS is responsible for handling system security based on validation of identities of various telecommunications entities. These functions are performed in AUthentication center (AUC) and Equipment Identity Register (EIR).

The AUC is accessed by the HLR to determine whether an MS will be granted service.

The EIR provides MS information used by the MSC. The EIR maintains a list of legitimate, fraudulent, or faulty MSs.

The OMSS is also in charge of remote operation and maintains of the PLMN. Functions are monitored and controlled in the OMSS. The OMSS may have one or more Network

Management Centers (NMCs) to centralize PLMN control.

The Operational and Maintenance Center (OMC) is the functional entity through which the service provider monitors and controls the system. The OMC provides a single point for the maintenance personnel to maintain the entire system. One OMC can serve multiple MSCs.

3.4 GSM Channel and Frame Structure

The bandwidth in the GSM is 25 MHz. The frequency band used for the uplink (i.e. transmission from the MS to the BS) is 890 to 915 MHz, whereas for the downlink (i.e. transmission from the BS to the MS) is 935 to 960 MHz. The GSM has 124 channels, each with a bandwidth of 200 kHz. For a given channel, the uplink (Fu) and downlink (Fd) frequency can be obtained from eqn (1) and (2), respectively:

$$Fu = 890.2 + 0.2\,(N-1)\ \text{MHz} \qquad (1)$$

$$Fd = 935.2 + 0.2\,(N-1)\ \text{MHz} \qquad (2)$$

where

$N = 1,2,.....,124.$

When the MS is assigned to an information channel, a radio channel and a timeslot are also assigned. Radio channels are assigned in frequency pairs- one for the uplink, Fu and other for the downlink, Fd. Each pair of radio channels supports upto eight simultaneous calls. Thus, the GSM can support upto 992 simultaneous users with rate speech coder. This will be doubled to 1,984 users with half-rate speech coder.

- ***Logical Channels***

In the GSM, there are three types of logical channels:

- Traffic channel (TCH).
- Control Channel (CCH).
- Cell Broadcast Channel (CBCH).

The TCHs are used to transmit user information (speech or data).

The CCHs are used to transmit control and signaling information.

The CBCH is used to broadcast user information from a service center to the MS listening in a given cell area. It is a unidirectional (downlink only), point-to-multipoint channel used for a short- information message service. Some special constraints are imposed on the design of the CBCH because of the requirement that this channel can be listened in parallel with Broadcast Control Channel (BCCH) information and paging message.

- *GSM Frame*

The GSM multiframe is 120 ms. It consists of 26 frames of 8 time slots. The structure of GSM hyperframe, superframe, multiframe, frame, and time slot is shown in figure- 9.6. A time slot carrier is 156.25 bits. The same format is used for the uplink and downlink transmission with various bursts types. In a normal bursts, two user information groups of 58 bits account for most of the transmission time in a time slot (57 bits carry user data, while the H bit is used to distinguish speech from other transmissions). Twenty six training (T) bits are used in the middle of the time slot. The time slot starts and ends with 3 tail bits. The time slot also contains 8.25 Guards (G) bits.

3.5 GSM Speech Processing

Two major tasks are involved in transmitting and receiving information over a digital radio link:

- Information Processing.
- Modulation Processing.

Information Processing deals with the prepration of basic information signals so that they are protected and converted into a form that a radio link can handle. Information Processing includes transcoding, channel coding, encrypting and multiplexing.

Modulation processing involves the physical prepration of the signal to carry information on a RF carrier.

Each digital radio link process in the transmitting path has its peer in the receiving path.(Fig. 3.4)

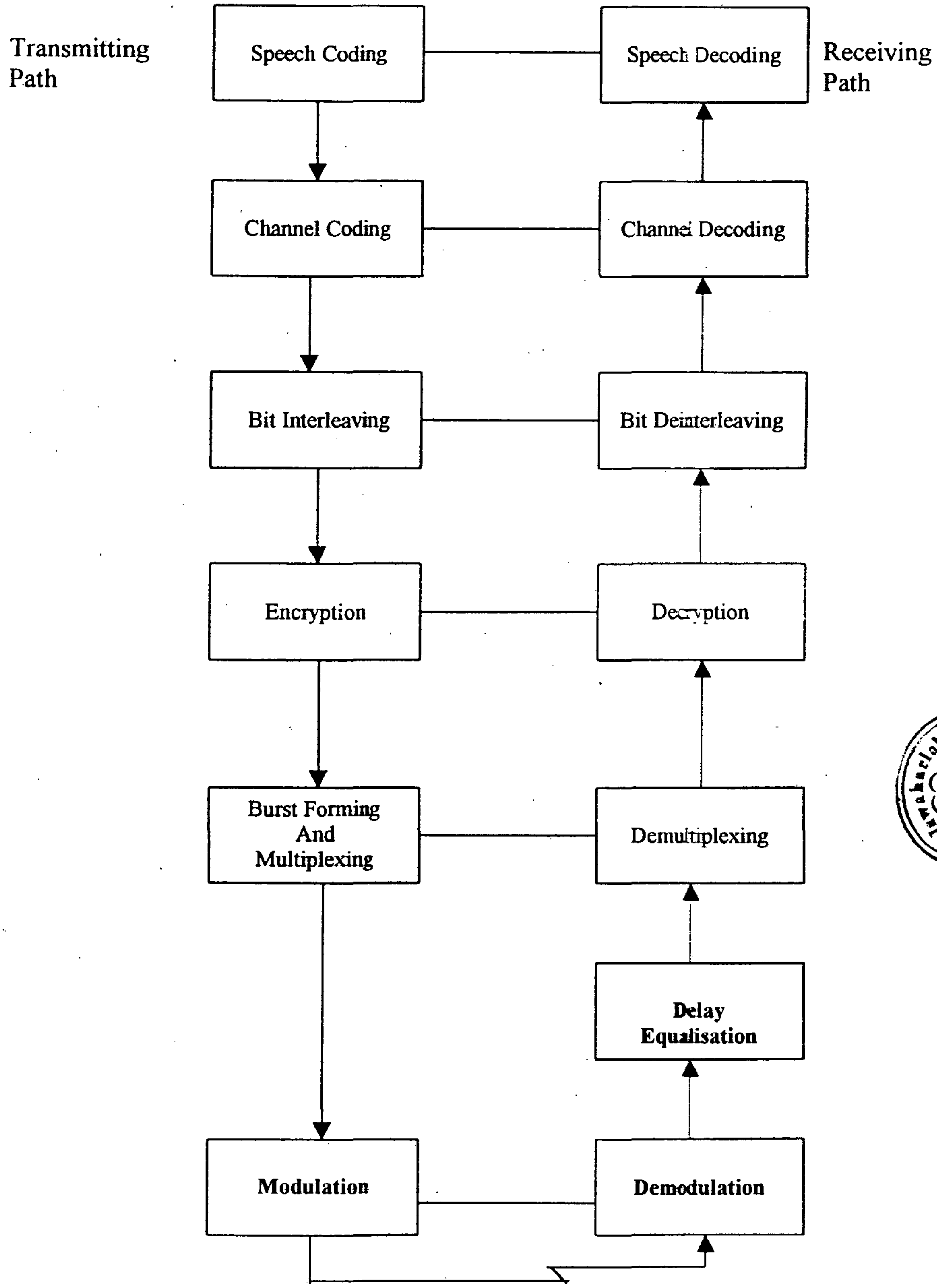


Fig. 3.4 *Digital Radio Link Process*

3.6 GSM Call Flow Scenarios

Here I discuss call flow scenarios used in the GSM. In this call flow scenario, MS enters the new MSC area and requires a location update procedure involving registration, authentication, ciphering and equipment validation.

Here the call flow scenarios involve the Call Origination (i.e., MS to land Call and MS to MS call), Call Termination (land to MS call), and handoff (i.e., inter-/intra-MSC).

3.6.1 Call Setup and Call Release

3.6.1.1 Call Setup with a Mobile

The procedure for a call setup for with a mobile station.

1. The MS sends a SETUP_REQ message to the MSC after it begins ciphering the radio channel. This message includes the dialed digits.
2. Upon receiving the SETUP_REQ message, THE MSC requests the VLR to supply the subscriber parameters necessary for handling the call. The message contains the called number and service indication.
3. The VLR checks for call-barring conditions. If the VLR determines the call cannot be processed, the VLR provides the reason to the MSC. In this case, we assume that the procedure is successful and the call can be processed. The VLR returns a message SUB_DATA_RESP to the MSC containing the service parameters for the subscriber.
4. The MSC sends a message to the MS that the call is proceeding.
5. The MSC allocates an available trunk to the BSS currently serving the MS. The MSC send a message to the BSS supplying it with the trunk number allocated and asks to assign a radio traffic channel for the MS.
6. The BSS allocates a radio channel and sends the information to the MS over SDCCH.
7. The MS tunes to the assigned radio channel and sends an acknowledgement to the BSS.
8. The BSS connects the radio traffic channel to the assigned trunk on the MSC and

deallocates the SDCCH. The BSS informs the MSC with a trunk and radio assignment complete message.

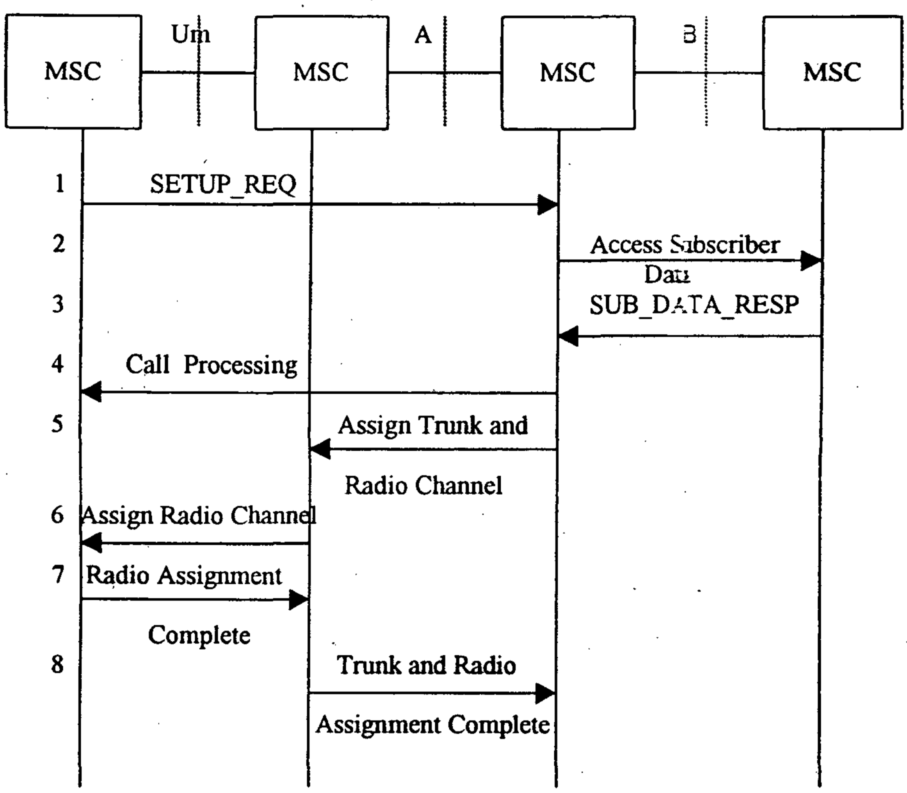


Fig3.5 ***Call Setup with a Mobile***

3.6.1.2 Call Setup with a Land Network

At this point a voice path is established between the MS and the MSC. The Ms user hears silence since the complete voice path is not yet established. The last phase involves the MSC establishing a voice path from the MSC to Public switched telephone network (PSTN).

1. The MSC sends the NET_SETUP message to the PSTN to request the call setup. This message includes the digits dialed by the MS and details of the trunk that will be used for the call.
2. The PSTN setup the call and notifies the MSC with a NET_ALERT message.
3. The MSC informs the MS that the destination number is being alerted. The MS hears the ringing tone from the destination local exchange through the established voice path.
4. When the destination party goes off hook, the PSTN informs the MSC.
5. The MSC informs the MS that the connection has been established.
6. The MS sends an acknowledgment to the MSC.

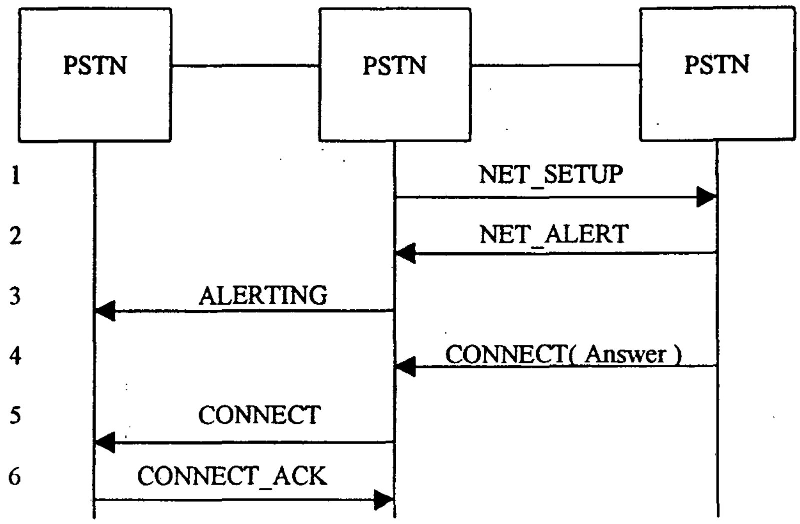


Fig.3.6 Call Setup with Land Network

3.6.1.3 Call Release - Mobile initiated

Under normal conditions, there are two basic ways a call is terminated:

- Mobile Initiated.
- Network Initiated.

In this scenario, the mobile user initiates the release of the call (see fig 9.14).

1. At the end of the call, the MS sends the CALL_DISC message to the MSC.
2. On receiving the CALL_DISC message, the MSC sends the NET_REL request message to the PSTN to release the call.
3. The MSC asks the MS to begin the clearing procedure using the CALL_REL message.
4. After the MS has performed its clearing procedure, it informs the MSC through the REL_COMP message.
5. The MSC then sends the CLR_COMM message to the BSS to ask it to release all the allocated dedicated resources for a given Signaling Connection Control Part (SCCP) connection.
6. The BSS sends the CHH_REL message to the MS to release the traffic channel.
7. The BSS sends an acknowledgement message CLR_COMP to the MSC informing it that all allocated dedicated resources have been released.

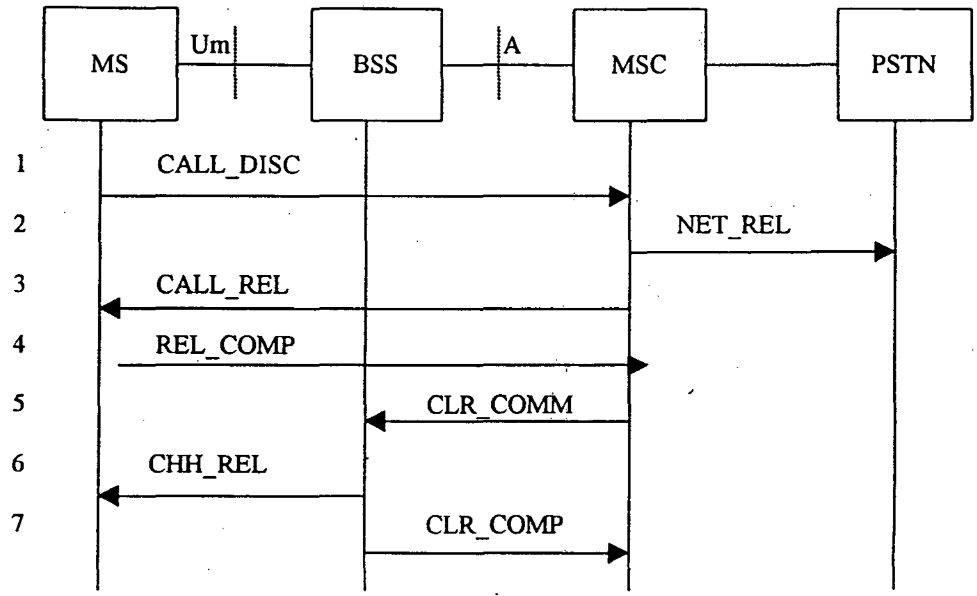


Fig.3.7 *Mobile to Land Call : Call Release – Mobile Initiated*

3.6.1.4 Routing analysis - Land to Mobile Call

In this scenario, the MS is already registered with the system and has been assigned a TMSI. In this situation MS is in its home system. A land subscriber dials the directory number of the Mobile subscriber.

1. The PSTN routs the call to the MSC assigned the directory number. The directory number in the INC_CALL message in mobile station ISDN Number (MSISDN).
2. The MSC sends the GET_ROUT message to the HLR to provide the routing information for the MSISDN.
3. The HLR returns the ROUT_INF message to the MSC. This message contains the Mobile Station Roaming Number (MSRN). If the MS is roaming within the servicing area of this MSC, the MSRN returned by the HLR will most likely be the same as the MSISDN. Here we assume that MS is not roaming.
4. The MSC informs its VLR about the incoming call using an INCO_CALL message that includes MSRN.
5. The VLR responds to the MSC through a PERM_PAGE message that specifies Location Area Specification (LAI) and TMSI of the MS. If the MS is barred from receiving the calls, the VLR informs the MSC that a call cannot be directed to the MS. The MSC would connect the incoming call to an appropriate announcement.

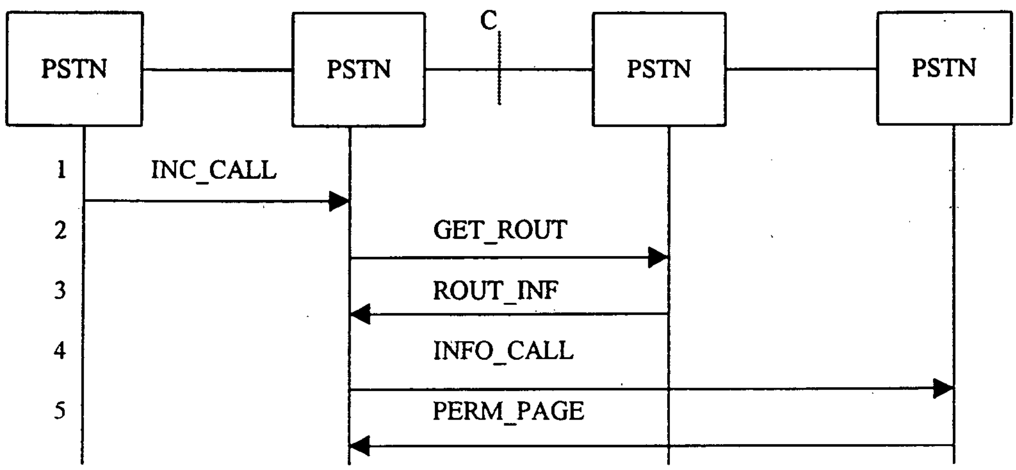


Fig.3.8 Land to Mobile Call – Routing Analysis

3.6.1.5 Paging - Land to Mobile Call

The following is the procedure for paging in a land to Mobile call.

1. The MSC uses the LAI provided by the VLR o determine which BSSs will page the MS. The MSC sends the PERM_PAGE message to each of the BSSs to perform the paging of the MS.
2. Each BSS broadcast the TMSI of the MS in the page message (PAGE_MESS) on the PCH.
3. When the MS hears its TMSI broadcast on the PCH, it responds to the BSS with a CHH_REQ message over common access channel, RACH.
4. On receiving the CHH_REQ message from the MS, the BSS allocates an SDCCH and sends the DSCH_ASS message to the MS over the AGCH. It is over the SDCCH that the MS communicates with the BSS and MSC until a TCH is assigned.
5. The MS sends a PAGE_RESP message to the BSS over the SDCCH. The message contains the MS's TMSI and LAI.
6. The BSS forwards the PAGE_RESP message to the MSC.
7. The MSC informs its VLR that the MS is responding to a page.

At this point the MS goes through authentication, Ciphering, Equipment validation, call setup, and call release procedures. If the MS has already gone through the authentication, ciphering, and equipment validation procedures, then only call setup and call release are carried out.

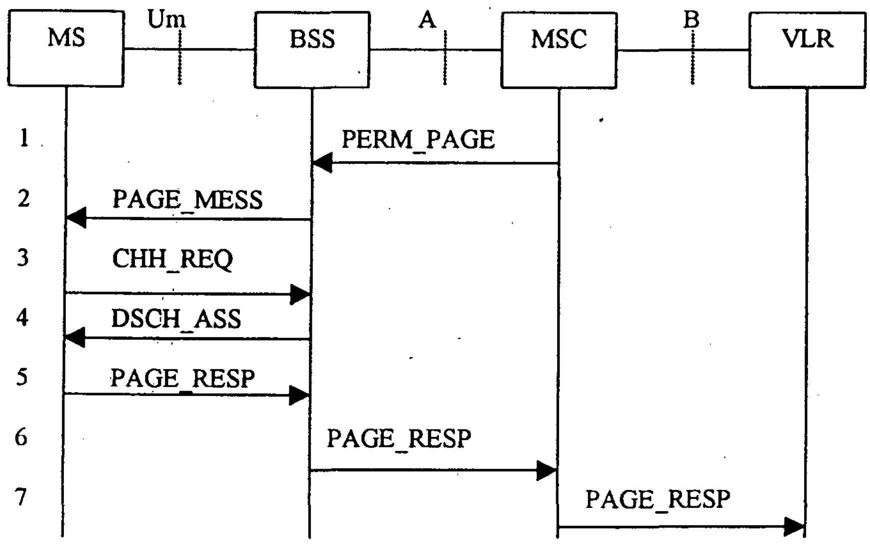


Fig.3.9 *PAGING – Land to Mobile Call*

3.6.2 Handoff

Basically there are two levels of handoffs:

- internal.
- external.

If the serving and target BTSs are located within the same BSS, the BSC for the BSS can perform a handoff without the involvement of the MSC. This type of handoff is referred to intra-BSS handoff. However, if the serving and target BTSs do not reside within the same BSS an external handoff is performed. In this of handoff the MSC coordinates the handoff and performs the switching tasks between the serving and target BTSs. The external handoff can be classified as: within the same MSC (i.e., intra-MSC) and between different MSCs (i.e., inter MSC)

3.6.2.1 Intra - MSC Handoff

When the MS determine that a handoff is required in an attempt to maintain the desired signal quality of the radio link, the following takes place.

1. The MS determines that a handoff is required. It sends the STRN_MEAS message to the serving BSS. This message contains the signal strength measurements.
2. The serving BSS sends a HAND_REQ message to thew MSC. This message contains a renk_ordered list of targets BSSs that are qualified to receive call.
3. The MSC reviews the global cell identity associated with the best candidate to determine if one of the BSSs that it controls is responsible for the cell area. In this scenario the MSC determines that the cell area is associated with the target BSS. To perform an intra-MSC handoff, two resources are required: a trunk between the MSC and the target BSS, and radio traffic channel in the new cell area. The MSC reserves a trunk and sends a HAND_REQ message to the target BSS. This message includes the desired cell area for handoff, the identity of the MSC-BSS trunk that was reserved, and the encryption key (Kc).
4. The target BSS selects and reserves the appropriate resources to support the handoff pending the connection execution. The target BSS sends an acknowledgment to the

MSC (HAND_REQ_ACK). The message contains the new radio channel identification.

5. The MSC sends the HAND_COMM message to the serving BSS. In this message the new radio channel identification supplied by the target BSS is included.
6. The serving BSS forwards the HAND_COMM message to the MS.
7. The MS returns to the new radio channel and sends the HAND_ACC message to the target BSS is included.
8. The target BSS sends the CHH_INFO message to the MS.
9. The target BSS informs the MSC when it begins detecting the Mobile handing over.
10. The target BSS and The MS exchange messages to synchronize/align the MS's transmission in the proper time slot. On completion, the MS sends the HAND_COMP message to the target BSS.
11. At this point the MSC switches the voice path to the target BSS. Once the MS and target BSS synchronize their transmission and establish a new signaling connection, the target BSS sends the MSC the HAND_COMP message to indicate that the handoff is successfully completed.
12. The MSC sends the REL_RCH message to the serving BSS to release the old radio traffic channel.
13. At this point the serving BSS frees up all the resources with the MS and sends the REL_RCH_COMP message to the MSC.

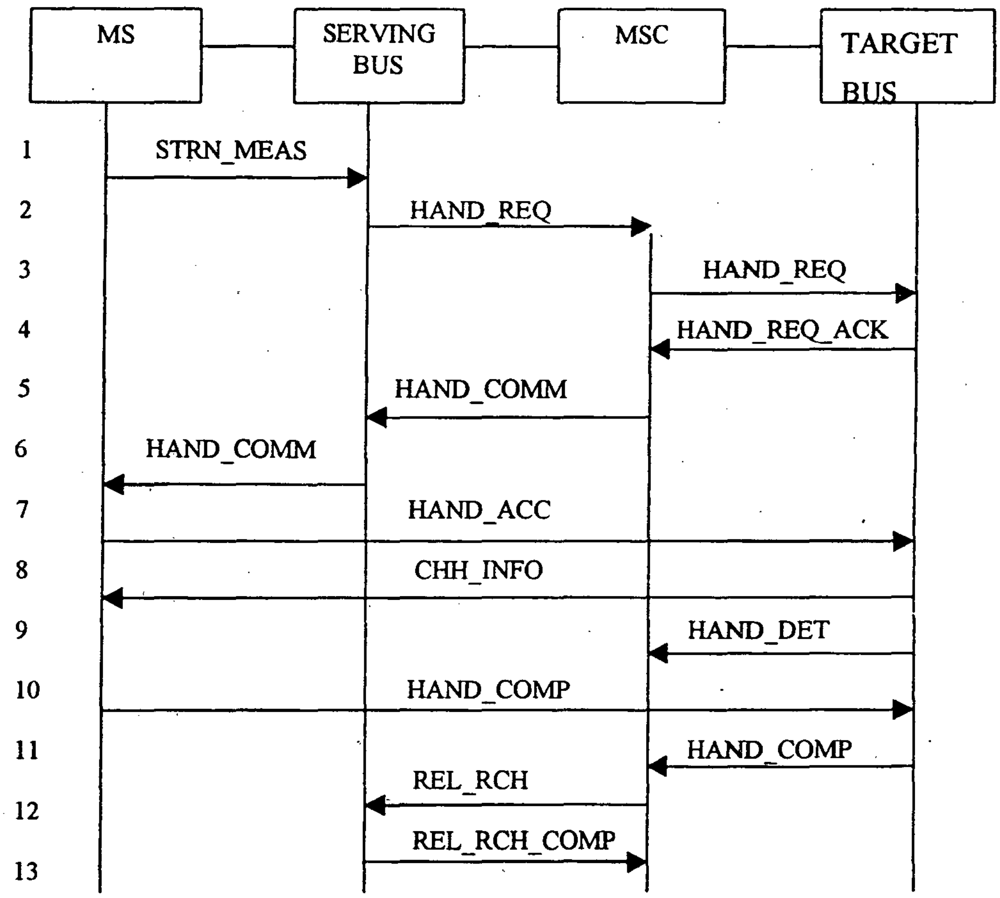


Fig.3.10 ***Intra – MSC Handoff***

3.6.2.2 Inter - MSC Handoff

In this, a call has already been established. The serving BSS is connected to the serving MSC and the target BSS to the target MSC. The inter-MSC handoff procedure is as follows :

1. Same as in the intra-MSC handoff (step 1).
2. Same as in the intra-MSC handoff (step 2).
3. When a call is handed over from the serving MSC to the target MSC via PSTN, the serving MSC sets up an inter-MSC voice connection by placing a call to the directory number that belongs to the target MSC. When the serving MSC places this call, the PSTN is unaware that a call is a handoff and follows the normal call routing procedures and delivers the call to the target MSC.
4. The target MSC sends a HAND_NUM message to its VLR to assign the TMSI.
5. The target VLR sends the TMSI in the HAND_NUM_COMP message.
6. Same as step 3 in the intra-MSC handoff.
7. Same as step 4 in the intra-MSC handoff.
8. The target MSC sends the HAND_PER_ACK message to the serving MSC indicating that it is ready for the handoff.
9. The serving MSC sends the NET_SETUP message to the target MSC to setup for the call.
10. The target MSC acknowledges this message with a SETUP_COMP message to the serving MSC.
11. Same as step 5 in the intra-MSC handoff.
12. Same as step 6 in the intra-MSC handoff.
13. Same as step 7 in the intra-MSC handoff.
14. Same as step 8 in the intra-MSC handoff.
15. Same as step 9 in the intra-MSC handoff.

16. Same as step 10 in the intra-MSC handoff.

17. Same as step 11 in the intra-MSC handoff.

18. At this point the handoff has been completed, the target MSC sends the SEND_ENDSIG message to the serving MSC.

19. The MS retunes to the new radio channel. A new voice path is setup between the MSS and the target BSS. The target MSC sends an answer message to the serving MSC.

20. Same as step 12 in the intra-MSC handoff.

21. Same as step 13 in the intra-MSC handoff.

22. The serving MSC sends the END_SIGNAL message to the target MSC.

23. The serving MSC releases the network resources and sends the NET_REL message to the target MSC,

24. The target MSC sends the REL_HAND_NUM message to its VLR to release the connection.

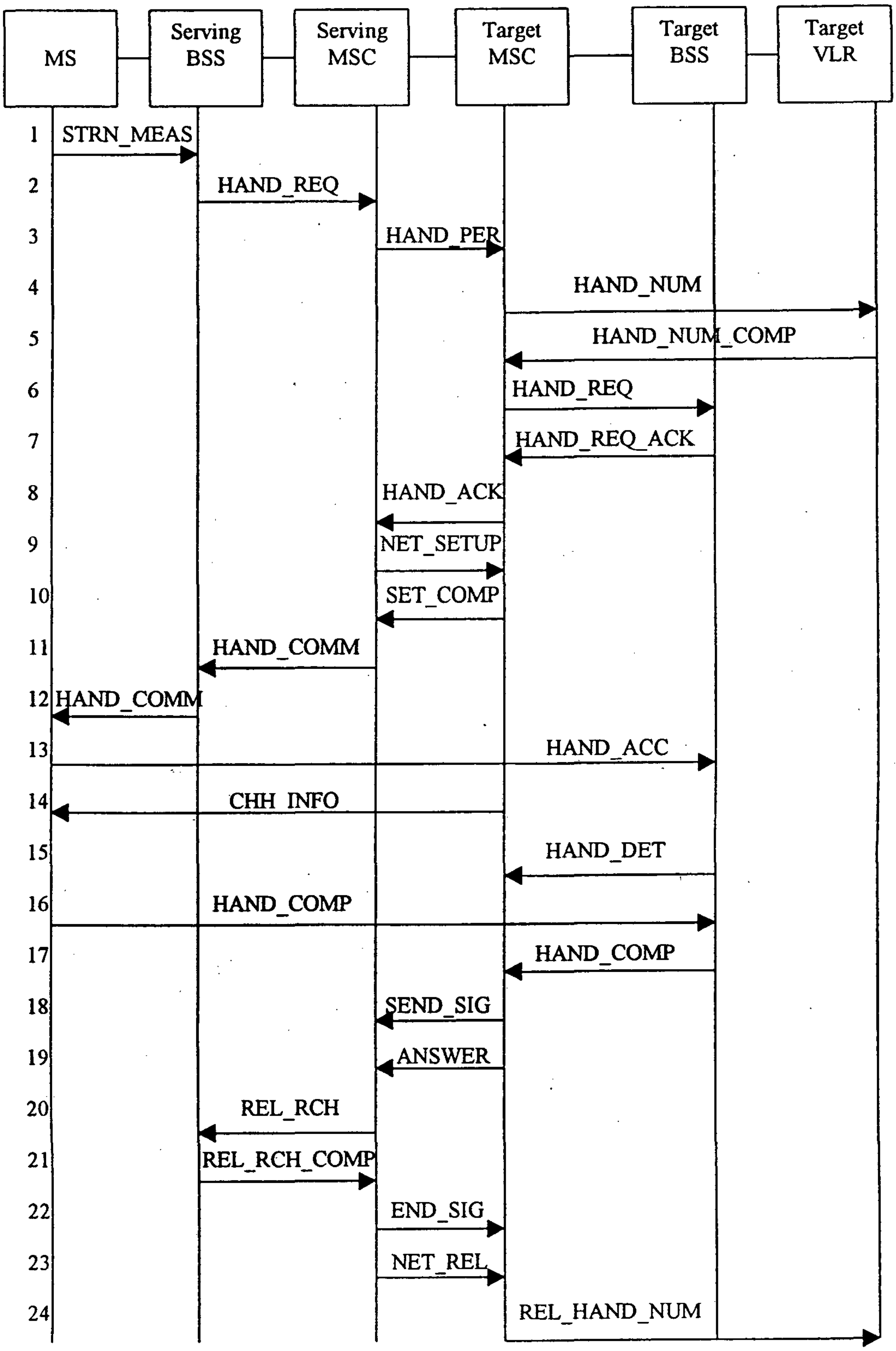


Fig.3.11 *Inter – MSC Handoff*

There are different types of Cellular Systems according to trunking. The concept of trunking is given below :

If the number of channels available for all the users of a radio system is less than the number of all possible users, then such a system is called a *Trunked radio system*.

Trunking is the process whereby users share a limited number of channels in some orderly way. Sharing channels, or providing channels than there are users who need them, works because we can be sure that the likelihood that everyone will want a channel at the same time is very low. The method of sharing channels is termed *access*; users ask for and are granted access to the trunked resource.

A Cellular phone system is a trunked radio system, because there are fewer channels than there are subscribers who could possibly want to use the system at the same time. Access is granted to multiple users of the system by dividing the system in to one or more of its operating domains:

- Frequency
- Time
- Space
- Code

4.1 Analog Cellular System

4.1.1 Basic Concept

The analog cellular system, called the Advanced Mobile Phone Service, (AMPS), consists of three basic elements: subscriber units (cellular phones) base stations, and a Mobile Telephone Switching Office (MTSO). Subscriber units communicate via radio signals to base stations, which convert radio signals for transfer to a central MTSO via land line or other link. The MTSO routes calls among subscriber units in the system or to the public Switched Telephone Network.

To serve more than 25,000,000 subscribers in the US with 864 cellular radio voice channels, each provider must reuse channels many times. In large cities like Los Angeles, as many as 40 subscribers may simultaneously use a single channel in one coverage area. Sharing a channel among so many subscribers would cause severe interference were it not for the fact that AMPS service areas are split into small zones of radio coverage, called cells. The cells are defined by the limited range of cellular radio transmissions. Cellular radios using the same channel do not interfere when they and the cells serving them are far enough apart. As a general rule, a radio channel used in a cell with a 1-mile diameter does not interfere with the same channel 4.6 miles away.

4.1.2 Operational Mechanism

To keep track of channels being used, and to allocate frequencies among cells, a central Mobile Telephone Switching Office (MTSO) connects all the cells in a system. The MTSO also connects calls between the cells and the landline network, and it coordinates the transfer of calls from cell to cell as subscribers travel through the system. For outgoing calls, AMPS cellular systems use the following process to assign radio channels and connect calls:

1. The subscriber dials and presses SEND. The phone sends a message asking the nearest cell to serve an outgoing call.
2. The nearest cell informs the MTSO of the request.
3. The MTSO assigns radio channels for the call to the cellular radio and serving cell.
4. The MTSO places the call on the landline network. The cell and MTSO maintain the connection between the cellular phone and landline network throughout the call.
5. As the subscriber moves between cells, the MTSO transfers calls from one cell to another, a process called "Handoff".

The AMPS system uses a similar procedure for incoming calls. The MTSO receives the call and directs the cells to send a radio message paging the cellular phone being called. If the receiving phone is on, it responds by requesting access to the system. The system goes through steps 2 and 3, the phone rings, and the call is connected as in step 4.

4.2 TDMA Cellular System

4.2.1 Basic concept

Digital technologies such as Time Division Multiple Access (TDMA) systems build upon the AMPS framework, using the subscriber unit, base stations, and MTSO in a similar way. However, TDMA adds capacity to the system by letting multiple users share a radio channel without interference or sacrifice of voice quality.

4.2.2 Operational Mechanism

TDMA technology makes it possible to serve several subscribers on each radio channel by converting speech sounds to a stream of digital information. The voice is sampled and compressed by a voice coder. The resulting 8,000 bit per second represent the voice.

The speech data is compressed into bursts only a third as long as the original audio signal. The encoding, transmission, and decoding are nearly instantaneous, so the remaining time is left for other subscribers.

To share the airtime on a radio channel among multiple subscribers, each subscriber sends and receives bursts at separate times. The times are allocated as slots of one 150th second, and assigned among three subscribers. Subscriber's communications are timed precisely to assigned slots. A digital phone receives the digital information and expands it to a full data stream. The expanded data is decoded to reproduce the original voice signal.

4.2.3 *Advantages*

- ***Authentication***

The process that enables your cellular phones and cellular service providers to confirm the identity of any phone placing or receiving a call, and inhibiting fraudulent use of the system.

- *Calling Number ID*

Allows the phone number of the incoming call to be displayed, so you will know who is calling you.

- *Message Waiting Indicator*

Notifies you if there is a voice message.

- *Dual Mode*

A TDMA Phone contains both analog and digital transceivers. If digital service is available, it operates in digital mode; if not it can operate in analog mode. Some manufactures phones can make this change automatically.

- *Voice Privacy*

Digital transmissions are inherently private because scanners are not equipped to decode or time-align with the digital bursts. Digital transmissions are easily encrypted to make eavesdropping nearly impossible.

- *Longer Talk-Time*

In digital mode, TDMA phones are idle between bursts, consuming less power than analog phones. In digital mode, subscribers can talk nearly twice as long without a battery change.

4.3 CDMA Digital Cellular System

4.3.1 Basic concept

Code Division Multiple Access (CDMA) Systems, first deployed in 1995, are also "dual mode", offering subscribers both digital and AMPS service. Like other digital systems, CDMA serves multiple users on a single radio channel.

4.3.2 Operational Mechanism

Technically CDMA differs from TDMA in three important ways:

- CDMA radio channels are about 6 times wider.
- The system assigns each subscriber a unique pseudo-random noise (PN) code; subscriber units then enhance signals carrying the assigned code, leaving the other signals inaudible.

- Theoretically, CDMA offers potential to serve more users per channel than TDMA or AMPS.

However, the 20-fold increase in system capacity is approximate. No fixed subscriber capacity can be assigned to CDMA systems, because their capacity depends upon the ability to control the power levels of the phone. Because of the power levels, fewer subscribers can be served. The next illustration attempts to show how the coding system works, and why the system is sensitive to excess data and power levels.

The bits sent along each communications path are assigned a unique code (for example, the squares and circles in the diagram). To be sure that enough information gets through to accurately describe the voice, each coded bit is repeated many times. These redundant bits are then mixed into a radio channel with bits from other communications paths. To decode this mixture of coded signals, the system might direct receiver 1 to enhance only bits coded with squares, 2 to enhance only circles, 3 to enhance only black squares. Each bit is repeated many times, so even though some bits are always lost to interference, enough usually get through to keep the signal clear. To accommodate heavy traffic, CDMA systems can vary the speech coding rate and accept higher bit error rates, but eventually, if too much data crowd the channel, too much is lost, and users notice deteriorating signal quality. However, this can be made up for by the increased number of channels available with CDMA systems.

CDMA handoffs differ slightly from other analog and digital technologies, because it allows the subscriber unit to simultaneously monitor and communicate with multiple cells, making handoffs much less noticeable.

4.3.3 Advantages

- ***Authentication***

The process that enables your cellular phones and cellular service providers to confirm the identity of any phone placing or receiving a call, and inhibiting fraudulent use of the system.

- ***Calling Number ID***

Allows the phone number of the incoming call to be displayed, so you will know who is calling you.

- *Message Waiting Indicator*

Notifies you if there is a voice message.

- *Dual Mode*

A CDMA phone contains both analog and digital transceivers. If digital service is available, it operates in digital mode; if not it can operate in analog mode. Some phone manufacturers' phones can make this change automatically.

- *Voice Privacy*

Digital transmissions are inherently private because scanners are not equipped to decode or time-align with the digital bursts. Digital transmissions are easily encrypted to make eavesdropping nearly impossible.

- *Longer Talk-Time*

In digital mode, CDMA phones are idle between bursts, consuming less power than analog phones. In digital mode, subscribers can talk nearly twice as long without a battery change.

4.4 GSM-PCS Cellular System

The Global System for Mobile Communications (GSM) has only recently begun to be deployed in North America. Recently, APC, 1-2-1 of Canada, Pacific Bell Mobile Services, DCR Communications, and others are using the GSM PCS 1900 system.

4.4.1 Basic Concept

GSM is a TDMA digital system that converts voice and access information to digital data, and communicates those data in bursts during brief time slots allocated to multiple subscribers sharing a radio channel. Like other digital technologies, GSM encodes, transmits, and decodes bursts in a fraction of the time required to produce the sound, using only a fraction of the airtime on a radio channel. In GSM systems, 8 subscribers can share the time on the channel. GSM uses radio frequencies about three times as efficiently as TDMA. GSM voice compression differs slightly from that of Digital Control Channel (DCC), using more bits to represent a voice signal, and compressing voice information fivefold. Also unlike DCC, GSM has no control channel, using only one type of 200kHz-traffic channel for voice and access. GSM phones can select cell sites and channels when initiating a call or during a call, and they assist handoff by measuring channel quality of nearby cell sites. GSM's digital format allows advanced encryption techniques, strongly securing calls against eavesdropping.

4.4.2 Operational Mechanism

GSM phones are about as complex as DCC phones and high global demand has made them relatively expensive compared with other digital technologies. Nevertheless, infrastructure costs are low because more subscribers can simultaneously use the radio channels in each cell site.

GSM phones use a removable Subscriber Identity Module (SIM) card containing the phone number, secret key, user's personal portfolio of services, and authentication algorithm for validation. Future SIM cards will provide inter-network access to services and billing to the subscriber. These SIM cards will work in phones on non-GSM mobile networks and in wired phones, providing convenient inter-network roaming.

The GSM standard also supports a Short Message Service (SMS), which allows mobile phones to receive short text messages. GSM phones can be used like a modem and linked to a PC to communicate data and fax messages at speeds up to 9.6 kbs. GSM standards include capabilities for services such as call forwarding, call waiting, call holding, multi-party calls, and closed user groups.

The radio accessed network is inherently less secure than a fixed network. This comes from the possibility to listen to and to emit radio waves from anywhere, without tampering with operator's equipment. To correct a little this state of affair, several types of security functions have been introduced in GSM in order to protect the network against fraudulent access and to ensure subscriber privacy. These functions include:

- authentication of the subscriber, to prevent access of unregistered users.
- radio path ciphering, in particular ciphering of all subscriber information to prevent third-party tapping.
- subscriber identity protection, to prevent subscriber location disclosure.

In following paragraphs, I have discussed Registration, Authentication and Ciphering.

5.1 Registration

After a mobile station is switched on it scans the whole GSM frequency in order to detect the presence of a network in least amount of time. When the network is detected, the mobile station reads the system information on the forward, or as it is called in GSM, the base channel. With this information, the mobile station is able to determine it's current position within the network. If the current location is not the same as it was last switched off, a registration procedure takes place.

First the Mobile station requests a channel from the network, which will be assigned by the base station. Before the channel is actually assigned to the Um interface, the BSC has to activate a channel on the BTS, which has to acknowledge the activation to the BSC in return. Now that the mobile station is connected to the infrastructure, the mobile station tells the system that it wants to perform a location update. This wish is passed on, via the BSC, to the (G)MSC, which, being very stubborn and bureaucratic, requires an authentication of the mobile station before taking any further action. Upon the receipt of correct parameters, the (G)msc accepts the mobile, via the BSC and the BTS, into its new location, and -if this option is used in the network - assigns a temporary identity (TMSI), which the mobile station also has to acknowledge. When this procedure is finished, the channel is released from the BSC via the BTS.

5.2 Authentication

The authentication procedure checks the validity of subscriber's SIM card, and whether they are permitted in a particular network. The authentication is based on the authentication algorithm, a3, which is stored on the SIM card and in the AC.

The A3 algorithm uses two input parameters: one is the authentication key, Ki, which is stored only on the SIM card and in the network. The second value, the randomly generated number (RAND), is transmitted to the mobile station on the Um interface. The mobile station passes the RAND to the SIM card where it is used as an input value for the A3 algorithm. The result, SRES, is returned - via the Um interface from the mobile station - to the network where the value of SRES is compared with the calculated value from the AC. A set of authentication parameters (RAND and SRES) is stored in the HLR and VLR for use by the AC. One important point of this security feature is that the relevant parameters (A3 and Ki) are stored in secure places and are never transmitted on the UM interface.

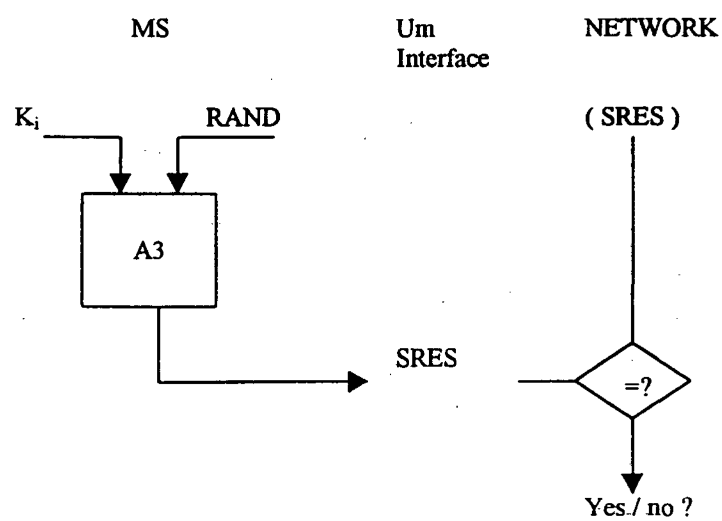


Fig. 5.1 Principle of Authentication

5.3 Ciphering

Digital transmission is suitable for the ciphering of data, because bit streams merely have to be scrambled with a certain method known only to both sides of the air interface. The GSM system uses such a ciphering method to protect signaling and user data. In order to ensure that the ciphered data from one side can be deciphered on the other side, a reversible algorithm is used. This means that if the ciphering algorithm, A5, is used to encipher a data stream, the same algorithm is used to decipher this stream and get back the original stream.

In the current system, only one algorithm A5/1 is used for both entities (i.e., for ciphering and deciphering both). But this algorithm feels difficult to export the GSM system other than COCOM states (the Eastern European states restricted from access to certain Western technologies).

To make exporting easier, a new algorithm A5/2 is developed, which is used for these former non-COCOM countries. Both algorithms can coexist in a network that's why Western European networks support both algorithms.

Having only two algorithms for ciphering could make the life of professional eavesdroppers relatively easy. The algorithm, therefore, require a specific key, Kc. This key is calculated from a random number, RAND delivered from the network. This the same number that was used for authentication procedure. The only difference is that a different algorithm, A8, is used to produce the ciphering key. The A8 algorithm is stored on the SIM card. The mobile equipment does not know anything about the security related algorithm A3 and A8. This Kc key issued by the A8 algorithm is then used with the ciphering algorithm, A5/1 or A5/2, to encipher or decipher the data. The A5 algorithm is implemented in the mobile station whether it is A5/1 or A5/2.

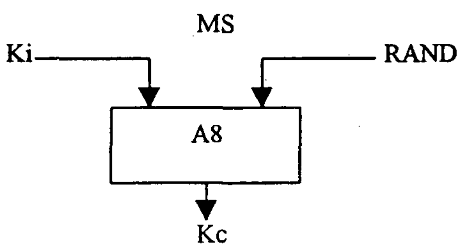


Fig. 5.2 Calculation of the Ciphering Key

To start the ciphering procedure, the network commands the mobile station to start ciphering with a specific ciphering sequence. From this time onward, the Mobile station transmits ciphered data, where even the acknowledgment that ciphering is being used is already transmitted with enciphered data.

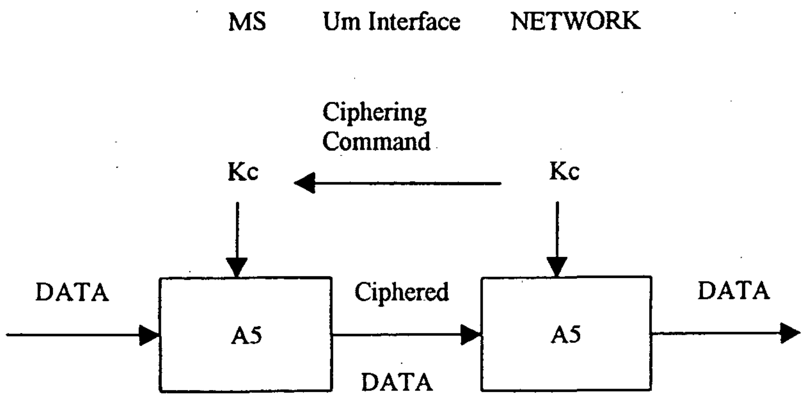


Fig.5.3 Start and Execution of Ciphering.

Chapter – 6

Proposed Approach for Optimal Cell Size

6.1 Multitier Wireless Cellular System

The Cellular System for the next generation of wireless multimedia networks will rely on cells that are smaller than those used today. In particular, in the proposed micro cellular systems, the cell radius can shrink down to as small as 50 m (0.5 MI - a 10 MI radius range for today's macro cellular system). Smaller cell radii are also possible for system with smaller coverage, such as pico and nano cells in a local area environment. The different parameters on which the sizes of cell rely are described below:

1.The size of cells is closely related to the expected speed of mobiles that the system is to support (i.e., the faster the mobiles move, the larger the cell should be), to keep the complexity of handoffs at a manageable level.

2. The cell size is also dependent on the expected system load; that is, the larger the system load the smaller the cell should be. Smaller cells result in channel being reused a greater number of times (greater extent of concurrency) and thus greater total system capacity.

3. Finally, the cell size is also depends on the required quality of service (QoS) level; for example, the probability of call blocking, of call dropping, or of call completion.

In general, the more stringent the QoS, the smaller the cells need to be, since smaller cells increase the total system capacity. However, smaller cells translate to more base stations, and hence higher costs.

When there are multiple mobility classes, it is useful to consider cell splitting, which results in a multitier system. For example, in a two tier system, one tier consists of smaller cells (called microcells or tier 2 cells), which are used by low-mobility users, and the other of larger cells (called macrocells or tier 1 cells), used by high mobility users.

In my project, I employ the multitier idea to show how to optimize the cell size with differing traffic requirements and mobile characteristics. Specifically I try to find out an optimal cell size considering following parameters:

- Total number of channels.

- The area to be covered.

- The average speed of mobiles in a tier.

- The call arrival and duration statistics for each tier.

- The constraints on the Quality of services (QoS).

Now my project approach is as follows:

- First I discuss my network model.

- Next I define my Optimization problem.

- At last, but not least, provide an algorithm for its solution.

6.2 Proposed Network Model

The assumptions, which I considered for network model, are as follows.

For each tier, the total area of the system (coverage area) is partitioned into cells. All cells of the same tier are of equal size. The network resources are also partitioned among the network tiers. Channels allocated to a particular tier are then reused based on the reused factor determined for the mobiles of that tier (i.e., within each tier, channels are divided into channel sets). One such set is then allocated to each cell of that tier. I use fixed channel allocation (FCA) for the allocation of channels both among the tiers and within a tier.

In this project, I have addressed only connection-oriented traffic (i.e., my work does not cover the connectionless case), and referred 'Call' as an association between a mobile and some other entity within the network. A call can be used to convey digital data, analog traffic, or digitized analog traffic and requires allocation of the wireless resources.

Each tier is identified by several parameters:

* Call arrival rate.

* Call duration time.

* Call data rate.

* Average speed of mobiles.

* Performance factor.

* QoS factors.

The performance factor (e.g., bit error rate) determines the channel reuse plan. The QoS factors used in this work are dropping probability and blocking probability. A call (more specifically an arriving call) is being denied service due to lack of wireless resources. The blocking probability refers to that arrived call. The calls, which are in progress, are being terminated during the handoff process. It happens due to unavailability of wireless resources in the new cell. The dropping probability refers to those terminated call accounts. Among these factors, call dropping is more serious than call blocking. As a consequence, network specification call for dropping probability is not much greater than blocking probability.

The assumptions, which I considered regarding traffic modeling and system architecture, are as follows:

1. The traffic generation is specially uniformly distributed.

2. Call arrival follows a Poisson process. The special and time distribution of call arrivals are the same over all cells in a given tier, but can be different from tier to tier.

3. Call duration for a given tier is exponentially distributed and may vary from tier to tier.

4. Handoffs and new calls are served from the same pool of available channels.

5. The speed of each class of mobiles is constant for each tier.

6. New call arrivals and call terminations are independent of the handoff traffic.

In this project, I formulate the cell optimization problem as the minimization of the total system cost and calculate the design parameters of each tier. The system cost is composed of the cost of the base stations and interconnection of the base stations to the mobile switching center. The cost of base station consists of the equipment (electronics, tower, antennas, etc.), real estate (including the zoning rights to place wireless transmission equipment), installation costs, and operating, administrative, and maintenance costs. In general, the total system cost is roughly proportional to the number of base stations. The total system cost is the sum of the costs of all the tiers. I further assume that all base stations of a specific tier are of equal cost.

6.3 Notations for Optimal Design

Notation :

A	Total area to be covered
S	Number of tiers
C	Total number of available network channels
C_i	Number of channels allocated to tier i
N_i	Number of channels allocated to tier i cell
f_i	Number of tier i cells in the frequency reuse cluster
m_i	Number of tier i cells contained in a tier (i - 1) cell. Tier 0 defines the total coverage area; m_1 defines total number of tier 1 cells.
R_i	Radius of a tier i cell(meters).
V_i	Average speed of tier i mobile users(meters per second).
λ_i^0	Number of tier i calls initiated per unit time per unit area, calls/(seconds . meter^2).
λ_i	Call initiation rat e in a tier i cell.
$1/\mu_i$	Average call duration of a tier i cell.
h_i	Mean number of handoffs.
γ_i	The relative cost of a tier i base station to the cost of a tier S base station($\gamma_S \equiv 1$).
$P_B(i)$	Actual blocking probability for a tier i cell.
$P_D(i)$	Actual dropping probability for a tier i cell.
$P_B^{max}(i)$	The maximum acceptable blocking probability for tier i calls.
$P_D^{max}(i)$	The maximum acceptable dropping probability for tier i calls.
$P_L(i)$	Loss probability of tier i.
PLT	Overall system loss probability, weighted by the amount of traffic of each tier.
PLT_{max}	The maximum acceptable weighted system loss probability.
TSC	Total system cost.
TSC_{max}	Maximum allowable total system cost.

6.4 *Definition of the Optimization Problem*

The objective of the work described in this project is to minimize the cost of multitier infrastructure. In this model, I assume that the major part of total system cost is the cost of Base station deployment, which in this model is proportional to the total number of base stations. The total number of base stations is directly depends on the total number of cells which results after cell splitting.

Thus, the total system cost, TSC, is

Thus the total system cost, TSC is

$$TSC = m_1(\gamma_1 + m_2(\gamma_2 + m_3(\ldots))) = \sum_{i=1}^{S} \gamma_i \prod_{j=1}^{i} m_j, \quad S \geq 1 \qquad (1)$$

In the above equation, I assume that cells are split in an arbitrary manner; that is, the location of tier i base stations is independent of the location of base stations of the other tiers. In some cases, a more structured splitting may be used. Thus if a base station already exists in a cell for tier i, the cost of placing an additional base station for a higher tier is negligible. Thus, for example, in case a of two-tier network the total cost can be reduced by the cost of tier 2 base stations. In such a case, the total cost can be given accurately by following formula

$$TSC = \sum_{i=1}^{S} \gamma_i \left(\gamma_1 \prod_{j=1}^{i} m_j - \prod_{j=1}^{i-1} m_j \right) = \gamma_1 m_1 + \sum_{i=2}^{S} \gamma (m_i - 1) \prod_{j=1}^{i-1} m_j, \quad S \geq 1 \qquad (2)$$

Reiterating some of the assumptions stated earlier, I assume that the set of all the available channels to tier i, Ci, is equally divided among the fi cells in the frequency reuse cluster, leading to no channel sharing between the cells. Also there is no channel sharing among the tiers. Furthermore, I assume that no channels are put aside for handling handoffs (i.e., allocation of channels for handoff requests and for new calls initiated within the cells are handled from the same pool of available channels in the cell). Thus the blocking and dropping probabilities are equal, and I called probability of loss, $P_L(1)$;

i.e.

$$\begin{aligned} \forall\, i,\ P_L(i) &= P_B(i) \\ &= P_D(i) \text{ and } P_L^{max}(i) \\ &= \min[P_B^{max}(i), P_D^{max}(i)] \end{aligned}$$

The overall system loss probability, PLT is given by :

$$\text{PLT} = \frac{\sum_{i=1}^{S} P_L(i)\lambda_i^0}{\sum_{i=1}^{S} \lambda_i^0} \qquad (3)$$

My main objective is to determine optimal cell size, when total system cost, TSC is minimum and total number of channels is atmost C, subject to following QoS constraints:

$\text{PLT} \le \text{PLT}_{max}$ and $\overline{P_L} \le \overline{P_L^{max}}$

In other words i am trying to determine m_i, for minimising TSC such that

$$\sum_{i=1}^{S} C_i \le C \text{ and } \text{PLT} \le \text{PLT}_{max} \text{ and } \overline{P_L} \le \overline{P_L^{max}} \qquad (4)$$

6.5 Proposed Solution of the Optimization Problem

The average number of handoffs, h_i, that a call of tier i will undergo during its lifetime is

$$h_i = \frac{(3+2\sqrt{3})V_i}{9\mu_i R_i}, \quad i = 1,2,\ldots,S \qquad (5)$$

Now, assuming that there are total of M_i cells in tier I ($M_i = \prod_{j=1}^{i} m_j$).

So, the total average number of handoffs per second in all the cells is $h_i \lambda_i Mi$.

The total arrival rate of handoff and initial calls in all tier i cells is $\lambda_i M_i(h_i+1)$ and average total (handoffs plus initial calls) rate per cell is

$$\lambda_i^{total} = \lambda_i(h_i+1) \qquad (6)$$

While in developing equation (6), I used assumption 6, together with the fact that the residual length of handed - off calls continuesto be exponentially distributed.

Thus, the total arrival process to a cell is still Markovian with the average rate of λ_i^{total}.

Since the area of hexagon with radius R is $3\sqrt{3}/2\,R^2$.

Thus

$$\lambda_i = \lambda_i^0 \frac{3\sqrt{3}}{2} R_i^2 \qquad (7)$$

Hence,

$$\lambda_i^{total} = \lambda_i^0 R_i \frac{\left[\left(2+\sqrt{3}\right)V_i + 3\sqrt{3}\mu_i R_i\right]}{2\mu_i} \qquad (8)$$

The average call termination rate is,

$$\mu_i^{total} = \mu_i\left(1+9h_i\right) \qquad (9)$$

$$P_L(i) = \frac{\left(\lambda_i^{total} / \mu_i^{total}\right)^{N_i} / N_i!}{\sum_{j=0}^{C_i} \left(\lambda_i^{total} / \mu_i^{total}\right)^j / j!} \qquad (10)$$

$$= \frac{\{[\lambda_i(1+h_i)]/[\mu_i(1+9h_i)]\}^{N_i} / N_i!}{\sum_{j=0}^{C_i} \{[\lambda_i(1+h_i)]/[\mu_i(1+9h_i)]\}^j / j!}, \quad i = 1,2,\ldots\ldots S$$

where λ_i^{total} and μ_i^{total} are given by equation 8 and 9 respectively.

λ_i and h_i by equations 7 and 5 respectively, and

$$N_i = \left\lfloor \frac{C_i}{f_i} \right\rfloor, \quad i = 1,2\ldots\ldots S \qquad (11)$$

Now assuming S = 2

then in the cost function in equation 2 simplifies to

$$TSC = \gamma_1 m_1 + \gamma_2 m_1 (m_2 - 1) \qquad (12)$$

Now, expressing m_1, m_2 *and* R_2 as a function of area A and tier 1 cell radius R_1.

Therefore

$$m_1 = \left\lceil \frac{A}{\text{Area of tier 1 cell}} \right\rceil = \left\lceil \frac{2\sqrt{3}A}{9R_1^2} \right\rceil \qquad (13)$$

Since both tier 1 and tier 2 cells are hexagonally shaped and tier 2 cells are obtained by suitably splitting the tier 1 cells. Each tier 1 cell will contain k layers of tier 2 cells.

From the geometry of a hexagon, the number of tier 2 cells in a tier 1 cell is given by

$$m_2 = 1+6+\ldots\ldots+6k = 1+3k(k+1), \quad k = 0,1,\ldots\ldots \qquad (14)$$

where (k+1) denotes the number of "circular layers" in the cell splitting.

Also the number of tier 2 cell is given by

$$R_2 = \frac{R_1}{\sqrt{m_2}} \qquad (15)$$

Thus, the optimization problem can be solved by equation (10) –(15) given above.

6.6 *Algorithm for Optimal Design*

By above problem definition, It is described that I have to find the optimal values of R_1, R_2, C_1, C_2, m_1 and m_2 . I assumed that the required optimal values are R_1^*, R_2^*, C_1^*, C_2^*, m_1^* and m_2^* . The parameters m_1, m_2, C_1 and C_2 are integers, while R_1 and R_2 are continuous variable.

Therefore,

I have to consider a discrete subset of the possible values of R_1 for which

$$R_1 = \sqrt{\frac{2\sqrt{3}A}{9\iota}}$$

where $\iota = m_{min1}, \ldots\ldots, m_{max1}$.

m_{min1} and m_{max1} are the lower and upper bounds of the tier 1 cell in the system. Thus

R_1 can assume one of $m_{max1} - m_{min1} + 1$ values.

The lower bound m_{min1} is assumed to be equal to 1.

While the upper bound, m_{max1} is estimated from TSC_{max} in the following way

$$m_{max1} = \left\lceil \frac{TSC_{max}}{\gamma_1} \right\rceil \qquad (16)$$

The procedure, which I used to find the optimal design parameters, is given below:

$$\mathrm{TSC}^{*} = \mathrm{TSC}$$

$$\mathrm{m}_{\max 1} = \left\lceil \frac{\mathrm{TSC}_{\max}}{\gamma_1} \right\rceil$$

$$a_1 = \frac{3\sqrt{2}}{2}\lambda_1^0$$

$$a_2 = \frac{3\sqrt{3}}{2}\lambda_2^0$$

$$b_1 = \frac{3+2\sqrt{3}}{9\mu_1}V_1$$

$$b_2 = \frac{3+2\sqrt{3}}{9\mu_2}V_2$$

$$c = \sqrt{\frac{2\sqrt{3}A}{9}}$$

while $(\mathrm{m}_{\min 1} \le m_1 \le m_{\max 1})$do

$$\mathrm{R}_1 = \frac{c}{\sqrt{m_1}}$$

$$\lambda_1 = a_1 R_1^2$$

$$h_1 = b_1 / R_1$$

while $\left(1 \le C_1 \le C\right)$ do

$$N_1 = \left\lfloor \frac{C_1}{f_1} \right\rfloor$$

$$N_2 = \left\lfloor \frac{C - C_1}{f_2} \right\rfloor$$

$$P_L(1) = \frac{\{[\lambda_1(1+h_1)]/[\mu_1(1+9h_1)]\}^{N_1} / N_1!}{\sum_{j=0}^{N_1} \{[\lambda_1(1+h_1)]/[\mu_1(1+9h_1)]\}^{j} / j!}$$

for $(k = 1;; k++)$

$m_2 = 1 + 3k(k+1)$

$TSC = \gamma_1 . m_1 + \gamma_2 . m_1 . (m_2 - 1)$

if (TSC $\ge$ TSC*) then break

$R_2 = R_1 / \sqrt{m_2}$

$\lambda_2 = a_2 R_2^2$

$h_2 = b_2 / R_2$

$$P_L(2) = \frac{\{[\lambda_2(1+h_2)]/[\mu_2(1+9h_2)]\}^{N2_1} / N_2!}{\sum_{j=0}^{N_{12}} \{[\lambda_2(1+h_2)]/[\mu_2(1+9h_2)]\}^{j} / j!}$$

$$PLT = \frac{\lambda_1^0 P_L(1) + \lambda_2^0 P_L(2)}{\lambda_1^0 + \lambda_2^0}$$

if $\left(\left(PLT < PLT_{max}\right) \text{and} \left(P_L(1) < P_L^{max}(1)\right)\right)$

and $\left(P_L(2) < P_L^{max}(2)\right)$ then break

end for

if $(TSC < TSC^{*})$ then

$\hat{k} = k$

$m_1^* = m_1$

$m_2^* = m_2$

$R_1^* = R_1$

$R_2^* = R_1 / \sqrt{m_2}$

$C_1^* = C_1$

$C_2^* = C - C_1$

end if

end while

end while

Hence, the outputs of the above algorithm are :

$TSC^*, m_1^*, m_2^*, R_1^*, R_2^*, C_1^*, C_2^*$.

Chapter 7

Conclusion

Present work is a modest attempt to determine the optimal cell size for a Multitier Wireless Cellular System. Basically, I have considered the optimal design of a Multitier System to minimize the total system cost. Due to that, I defined system cost as being primary composed of the cost of cell sites (i.e. the base stations) and proposed a procedure to determine the cell sizes for each tier. Since my objective is to find the optimal cell size, keeping the minimum total system cost. Therefore, I also find the portion of the total no channels assigned to each tier and the total system cost along with The cell size.

Any system designer to estimate the total system cost, the required number of cells for each tier and the partition of system channels among the tiers can use my proposed algorithm.

The procedure given by me can help the Mobile users in purchasing their cellular system.

Before purchase, they may compare the system specifications with the specification proposed by my procedure.

1. K.Sohraby, "Impact of Mobility in Linear Cellular Arrays on the Performance of Cellular and PCS networks", Proc. IEEE MILCOM '94 Fort Monmouth, NJ, , Oct. 2-5, 1994.
2. Z. J. Haas, J. H. Winters, and D. S. Johnson, "Additional Results on the Capacity Bounds in Cellular System", Proc. GLOBECOM '94.
3. R. Guerin," Channel Occupancy Time Distribution in Cellular Radio System", IEEE Trans. Vehic. Tech., vol. VT-35, no. 3, Aug. 1987.
4. Siegmund M. Redl, Matthias K. Weber and Malcom W. Oliphant,"AN INTRODUCTION TO GSM", Artech House, Boston, London 95.
5. Vijay K. Garg and Joseph E. Wilkes,"WIRELESS AND PERSONAL COMMUNICATIONS SYSTEMS" ,Third Edition, Printice HALL PTR.
6. Michel MOULY and Marie-Bernadette PAUTET," The GSM System for Mobile Communications", Published by Auther's Company, Cell & Sys. Correspondence.
7. JOHN WALKER," MOBILE INFORMATION SYSTEMS" Published by Artech House, Boston, London.
8. Andrew S. Tannenbaum," COMPUTER NETWORKS " Third Edition, Printice Hall Inc.
9. Dimitri Bertsekas and Robert Gallager," DATA NETWORKS " Second Edition, Printice Hall Inc.