NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Electrical and Electronic Engineering

GSM ARCHITECTURE

Graduation Project
EE- 400

Student: Adham Shweiki (990984)

Supervisor: Prof. Dr. Fakhreddin Mamedov

Lefkoşa -2003

ACKNOWLEDGEMENT

"First of all, I would like to say how grateful I am to my supervisor, Prof. Dr. Fakhreddin Mamedov, friends, parents, sisters, and brothers.

I would like to thank my supervisor Prof. Dr. Fakreddin Mamedov . Under his guidance, I successfully overcome many difficulties and learn a lot about Cellular and Global System for Mobile Comunications and Arcitecture of GSM. I asked him many questions in Communications, Telecommunication and GSM, he explained my questions patiently.

I could not have prepared this Project without the generous help of Mr. Cemal Kavalcıoğlu, I thank him for his invaluable and continual support.

I would like to express my gratitude to Prof. Dr. Şenol Bektaş because he helped me at each stage of my Undergraduate Education in Near East University.

I also wish to thank my advisor Assist. Prof. Dr. Kadri Bürüncük at my Undergraduate Education for his i6nvaluable advices, and for his patience and support.

Finally, I want to thank my father, my mother and my best friend Manaf, I could never have prepared this project without their endless support and encouragement."

ABSTRACT

GSM (Global System of Mobile Communication) has been well known as the world's most popular standard for new cellular radio and personal communication equipment throughout the world.

GSM was first introduced into the European market in 1991. By the end of 1993, several non European countries in South America, Asia, and Australia had adopted GSM and the technically equivalent offshots, DCS 1800, which supports Personal Communication Services (PCS) in the 1.8 GHz to 2.0 GHz radio bands recently created by the governments throughout the world. GSM's success has exceeded the expectations of virtually everyone, and it is now the world's most popular standard for new cellular radio and Personal Communication Equipment throughout the world. It is predicted that by the year 2001, there would be 500 million GSM subscribers worldwide.

A GSM PLMN cannot establish calls autonomously other than local calls between mobile subscribers. In most of the cases, the GSM PLMN depends upon the existing wireline networks to route the calls.

The GSM system architecture consists of three major interconnected subsystems that interact between themselves and with the users through certain network interfaces. The subsystems are the Base Station Subsystem (BSS), Network and Switching Subsystem (NSS), and The Operration Support Subsystem (OSS). The Mobile Station (MS) is also a subsystem, but is usually considered to be part of the BSS for architecture purposes. Equipment and Services are designed within GSM to support one or more of these specific subsystems.

The first subsystem named Base Station Subsystem (BSS), provides and manages radio transmission path between the mobile station and the mobile switching center. Second subsysten of GSM Architecture is Network and Switching Subsystem (NSS). This subsystem manages the switching functions of the system and allows the mobile switching centers to communicate with other networks. The last subsytem is known as Operation Support Subsystem (OSS). This subsystem's major functionality consists of supporting the operation and maintenance of GSM. It allows the system engineers to monitor, diagnose and troubleshoot all aspects of the GSM system. The above three basic subsystems built the GSM Architecture.

TABLE OF CONTENTS

INTRODUCTION

During the early 1980s, analog cellular telephone systems were experiencing rapid growth in Europe, particularly in Scandinavia and the United Kingdom, but also in France and Germany. GSM (Global System for Mobile Communications) is a European digital communications standard which provides full duplex data traffic to any device fitted with GSM capability, such as a phone, fax or pager, at a rate of 9600 bps using the TDMA communications scheme. Mobile phones may be thought of as cordless phones with elaborate portable and base units.The Radio Interface is the interface between the mobile stations and the fixed infrastructure. The GSM System Architecture consists of three major interconnected subsystems that interact between themselves and with the users through certain network interfaces. The Subsystems are the Base Station Subsystems (BSS), Network and Switching Subsystem (NSS), and the Operation Support Subsystem (OSS).

This project is aimed to examine GSM Architecture parts separately and demonstrate the GSM network functions tasks.

The project consists of the introduction, four chapters and conclusion.

The Chapter 1 introduces first History of GSM, then continues with Services provided by GSM. Finally the Chronology of communication and wireless systems up to 1982 and the developments of GSM from 1982 until Todays are also given.

Chapter 2 presents briefly overview of GSM (PLMN), channel and frame structure then we observed the objectives of GSM PLMN and tried to give the detailed services. then the structure of GSM channel and frame structure are described. Finally we represent GSM call flow scenarios.

Chapter 3 studies the GSM radio Interface in details, channel structure and coding, interleaving, ciphering, modulation, Discontinuous Transmission, timing advance, power control Discontinuous reception and finally Multipath and Equalization is also examined.

Chapter 4 is concerned to the GSM Architecture. This chapter is the most important aim of my Graduation Project. I illustrate the process of GSM Architecture and the GSM Functions in details.

1. INTRODUCTION TO CELLULAR AND GSM SYSTEMS

1.1 An overview of the GSM system

The Global System for Mobile communications is a digital cellular communications system. It was developed in order to create a common European mobile telephone standard but it has been rapidly accepted worldwide. GSM was designed to be compatible with ISDN services.

1.2 History of the cellular mobile radio and GSM

The idea of cell-based mobile radio systems appeared at Bell Laboratories (in USA) in the early 1970s. However, mobile cellular systems were not introduced for commercial use until the 1980s. During the early 1980s, analog cellular telephone systems experienced a very rapid growth in Europe, particularly in Scandinavia and the United Kingdom. Today cellular systems still represent one of the fastest growing telecommunications systems. But in the beginnings of cellular systems, each country developed its own system, which was an undesirable situation for the following reasons:

- The equipment was limited to operate only within the boundaries of each country.
- The market for each mobile equipment was limited.

In order to overcome these problems, the Conference of European Posts and Telecommunications (CEPT) formed, in 1982, the Groupe Spécial Mobile (GSM) in order to develop a pan-European mobile cellular radio system (the GSM acronym became later the acronym for Global System for Mobile communications). The standardized system had to meet certain criterias:

- Spectrum efficiency
- International roaming
- Low mobile and base stations costs
- Good subjective voice quality

- Compatibility with other systems such as ISDN (Integrated Services Digital Network)
- Ability to support new services

Unlike the existing cellular systems, which were developed using an analog technology, the GSM system was developed using a digital technology. In 1989 the responsability for the GSM specifications passed from the CEPT to the European Telecommunications Standards Institute (ETSI). The aim of the GSM specifications is to describe the functionality and the interface for each component of the system, and to provide guidance on the design of the system. These specifications will then standardize the system in order to guarantee the proper interworking between the different elements of the GSM system. In 1990, the phase I of the GSM specifications were published but the commercial use of GSM did not start until mid-1991.

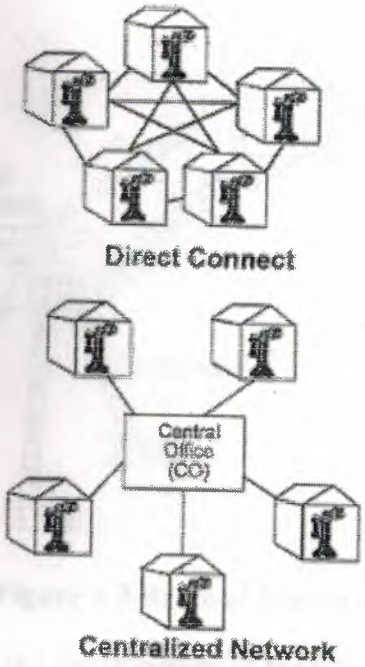


Figure 1.1 The old network public telephone

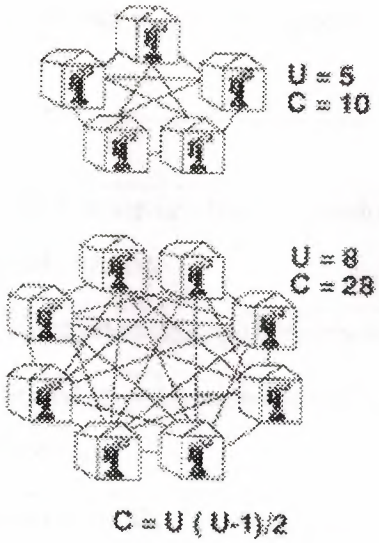


Figure 1.2 Public switched telephone network(PSTN)

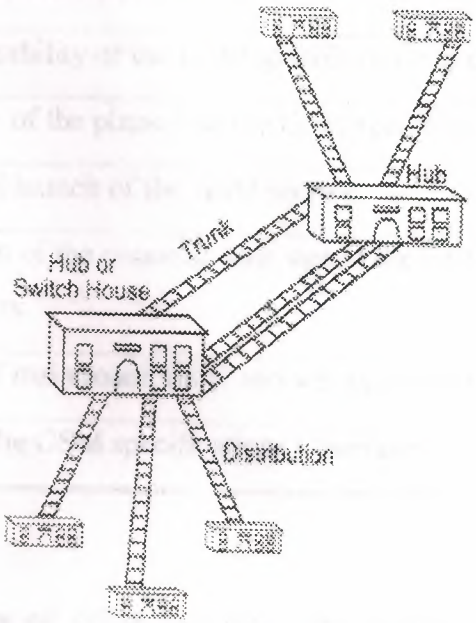


Figure 1.3 Railroad Network

The most important events in the development of the GSM system are presented in the table 1.1.

Table 1.1 Events in the development of GSM

Year	Events
1982	CEPT establishes a GSM group in order to develop the standards for a pan-European cellular mobile system
1985	Adoption of a list of recommendations to be generated by the group
1986	Field tests were performed in order to test the different radio techniques proposed for the air interface
1987	TDMA is chosen as access method (in fact, it will be used with FDMA) Initial Memorandum of Understanding (MoU) signed by telecommunication operators (representing 12 countries)
1988	Validation of the GSM system
1989	The responsability of the GSM specifications is passed to the ETSI
1990	Appearance of the phase 1 of the GSM specifications
1991	Commercial launch of the GSM service
1992	Enlargement of the countries that signed the GSM- MoU> Coverage of larger cities/airports
1993	Coverage of main roads GSM services start outside Europe
1995	Phase 2 of the GSM specifications Coverage of rural areas

From the evolution of GSM, it is clear that GSM is not anymore only a European standard. GSM networks are operationnal or planned in over 80 countries around the world. The rapid and increasing acceptance of the GSM system is illustrated with the following figures:

- 1.3 million GSM subscribers worldwide in the beginning of 1994.
- Over 5 million GSM subscribers worldwide in the beginning of 1995.
- Over 10 million GSM subscribers only in Europe by December 1995.

Since the appearance of GSM, other digital mobile systems have been developed. The table1.2 charts the different mobile cellular systems developed since the commercial launch of cellular systems.

Table 1.2 Mobile cellular systems

Year	Mobile Cellular System
1981	Nordic Mobile Telephony (NMT), 450
1983	American Mobile Phone System (AMPS)
1985	Total Access Communication System (TACS) Radiocom 2000 C-Netz
1986	Nordic Mobile Telephony (NMT), 900
1991	Global System for Mobile communications> North American Digital Cellular (NADC)
1992	Digital Cellular System (DCS) 1800
1994	Personal Digital Cellular (PDC) or Japanese Digital Cellular (JDC)
1995	Personal Communications Systems (PCS) 1900- Canada
1996	PCS-United States of America

I found an article about future cellular phones online with five sub-articles explaining five unique cellular phones from Samsung Electronics' website. All of those five different cellular phones were made with state of the art technologies. Some of the functions they feature are like TV, Internet, MP3 player, video transmission, and wrist cellular phone. The first cellular phone introduces was the TV phone. Samsung introduces a normal looking folding-type cellular phone with small TV built into it. This cellular phone uses a 1.8-inch high-resolution color LCD screen instead of normal screen with colors like green and black. This screen allows the user to view the TV using the antenna attached to the cellular phone and the earphone to view TV shows anywhere, and if someone calls, the TV simply turns off and the cellular phone turns into phone mode immediately. VHF and UHF reception is possible with the antenna on the cellular phone. And this TV phone allows you to watch TV for as long as 200 minutes on a single charge with it's high-capacity battery. Some specialty of this

cellular phone is that even with all those features, it only weighs 160 grams, and the TV operates on just 3 volts and gives same picture quality as any other portable TV using 9 volts. Before, using one antenna for TV and cellular phone seemed too difficult because of the interference between the TV and the phone's different frequency. However, Samsung made this possible with its newest technology they invented. Next cellular phone introduced was a Wireless Internet phone. This cellular phone has a charge 3-cm by 7-cm touch screen, which allows users to browse through the Internet, and send faxes. This phone has features like cellular phone, electronic notebook, PC data interface, character recognitions, and etc. This cellular phone's character recognition technology has 98% accuracy with Korean and 95% accuracy with English when written on the touch screen with a pen. This unit took Samsung's 110 researchers, $4.6 million, and 52 patents to develop. This Internet phone can also send e-mails, written documents or pictures through Internet just like a normal laptop computer. The third cellular phone introduced in this article was the MP3 Phone. This cellular phone plays music from its embedded memory of 32 MB in mp3 format, the most popular format of music for PC.

This cellular phone allows users to put mp3 files on it's embedded memory using computer, and also allows users to create their own mp3 files by recording their phone calls or other sounds. This phone has functions that other cellular phones have like, voice dialing, morning call, and etc. This phone also has a function that allows users to whisper on their cellular phone to the other person when they cannot raise their voice at that moment. This function amplifies sound coming from short distance so that the other caller can hear the user clearly. The fourth cellular phone shown was IMT-2000 cellular phone. This is a cellular phone that that has Base Station System, Mobile Switching Center, and other system hardware as well as hand sets for high-speed packet data and moving picture data transmission. This phone allows users to sent packet data at 144 Kbps, which is about 10 times faster than normal wireless handsets can. So users can send data, graphics, still pictures, and even moving pictures. Also this unit is designed to operate and 2 GHz, which is higher compared to other units with 1.9 GHz or 1.8 MHz. Last model from this article is the Watch Phone. Cellular phone that users wear was already invented in Japan and was used in 1996 Nagano Winter Olympics by some officials. However, those were not introduced to the public to buy. So the Samsung is the first company to introduce Watch Phone to the cellular phone market. This cellular phone has about 30 features just like other normal-sized cellular phones in South Korea.

Some features that this cellular phone has would be things like voice-activated dialing, phone directory, vibration, microphone, and LCD screen that displays the current mode that the user is in. This cellular phone is expected to be a big hit with the youth market because of its portability and other advantages. Some advantages can be that it is harder to lose or get stolen then normal cellular phones because it's worn on the users' wrist, and it stays out of the way for outdoor or indoor activities.

And the figure below shows the first cellular phone.

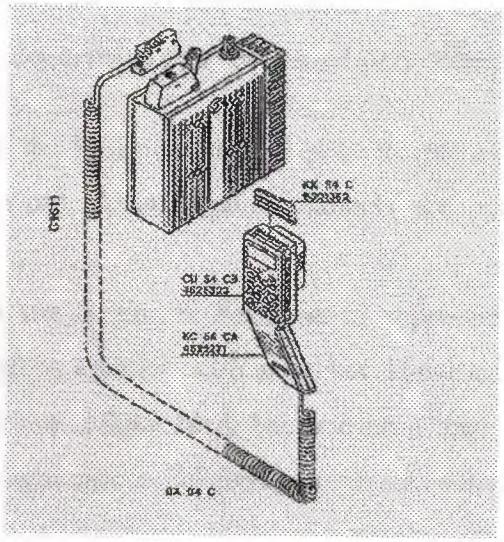


Figure 1.4 The frist cellular phone

1.3 The cellular structure

In a cellular system, the covering area of an operator is divided into cells. A cell corresponds to the covering area of one transmitter or a small collection of transmitters. The size of a cell is determined by the transmitter's power. The concept of cellular systems is the use of low power transmitters in order to enable the efficient reuse of the frequencies. In fact, if the transmitters used are very powerful, the frequencies can not be reused for hundred of kilometers as they are limited to the covering area of the transmitter. The frequency band allocated to a cellular mobile radio system is distributed over a group of cells and this distribution is repeated in all the covering area of an operator. The whole number of radio channels available can then be used in each group of cells that form the covering area of an operator. Frequencies used in a cell will be reused several cells away. The distance between the cells using the same frequency must be sufficient to avoid interference. The frequency reuse will increase considerably the capacity in number of users.

In order to work properly, a cellular system must verify the following two main conditions:

- The power level of a transmitter within a single cell must be limited in order to reduce the interference with the transmitters of neighboring cells. The interference will not produce any damage to the system if a distance of about 2.5 to 3 times the diameter of a cell is reserved between transmitters. The receiver filters must also be very performant.
- Neighboring cells can not share the same channels. In order to reduce the interference, the frequencies must be reused only within a certain pattern.

In order to exchange the information needed to maintain the communication links within the cellular network, several radio channels are reserved for the signaling information.

with cellular radio we use a simple hexagon to represent a complex object: the geographical area covered by cellular radio antennas. These areas are called cells. Using this shape let us picture the cellular idea, because on a map it only approximates the covered area. Why a hexagon and not a circle to represent cells?

Figure 1.5 Hexagon Cell

If we draw cells as circles we can't show the cells right next to each other. We get instead a confusing picture like that on the bottom right. Notice all the gaps between the circles? When showing a cellular system we want to depict an area totally covered by radio, without any gaps. Any cellular system will have gaps in coverage, but the hexagonal shape lets us more neatly visualize, in theory, how the system is laid out.

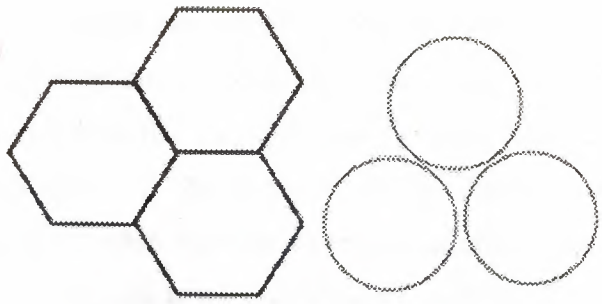


Figure 1.6 Hexagonal cell group

Notice the illustration below. The middle circles represent cell sites. This is where the base station radio equipment and their antennas are located. A cell site gives radio coverage to a cell. Do you understand the difference between these two terms? The cell site is a location or a point, the cell is a wide geographical area. Okay?

Most cells have been split into sectors or individual areas to make them more efficient and to let them to carry more calls. Antennas transmit inward to each cell. That's very important to remember. They cover a portion or a sector of each cell, not the whole thing. Antennas from other cell sites cover the other portions. The covered area, if you look closely, resembles a sort of rhomboid, as you'll see in the diagram after this one. The cell site equipment provides each sector with its own set of channels. In this example, just below , the cell site transmits and receives on three different sets of channels, one for each part or sector of the three cells it covers.

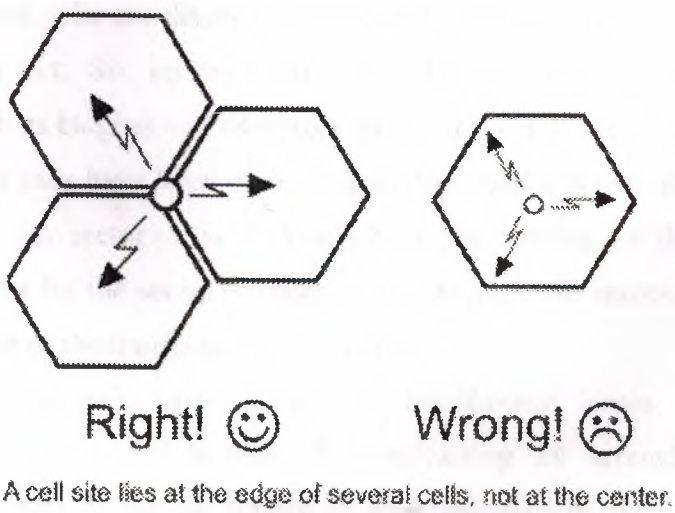


Figure 1.7 Effect in hexagonal cells

Is this discussion clear or still muddy? Skip ahead if you understand cells and sectors or come back if you get hung up on the terms at some later point. For most of us, let's go through this again, this time from another point of view. Mark provides the diagram and makes some key points here: "Most people see the cell as the blue hexagon, being defined by the tower in the center, with the antennae pointing in the directions indicated by the arrows. In reality, the cell is the red hexagon, with the towers at the corners, as you depict it above and I illustrate it below. The confusion comes from not realizing that a cell is a geographic area, not a point. We use the terms 'cell' (the coverage area) and 'cell site' (the base station location) interchangeably, but they are not the same thing."

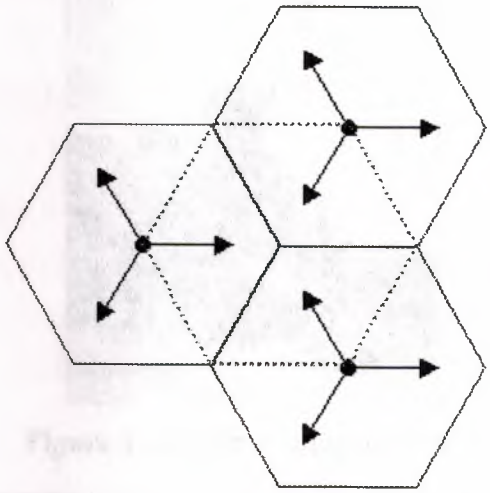


Figure 1.8 The reality hexagon cell

"These days most cells are divided into sectors. Typically three but you might see just two or rarely six. Six sectored sites have been touted as a Great Thing by manufacturers such as Hughes and Motorola who want to sell you more equipment. In practice six sectors sites have been more trouble than they're worth. So, typically, you have three antenna per sector or 'face'. You'll have one antenna for the voice transmit channel, one antenna for the set up or control channel, and two antennas to receive. Or you may duplex one of the transmits onto a receive.

By sectorising you gain better control of interference issues. That is, you're transmitting in one direction instead of broadcasting all around, like with an omnidirectional antenna, so you can tighten up your frequency re-use"

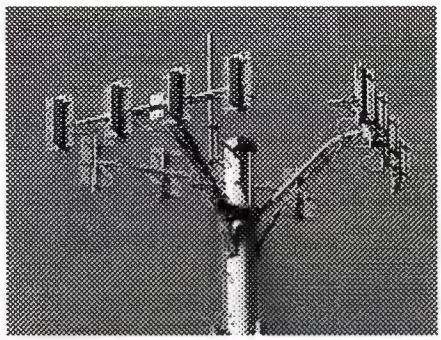


Figure 1.9 Transmitting antenna 1

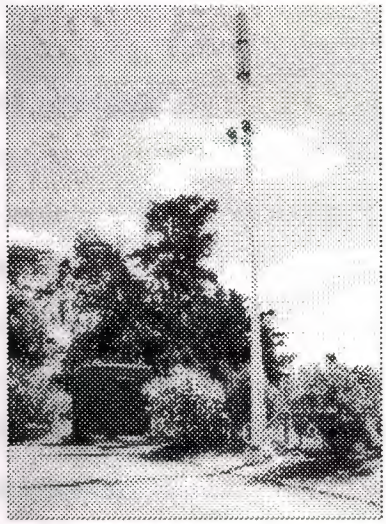


Figure 1.10 Transmitting antenna 2

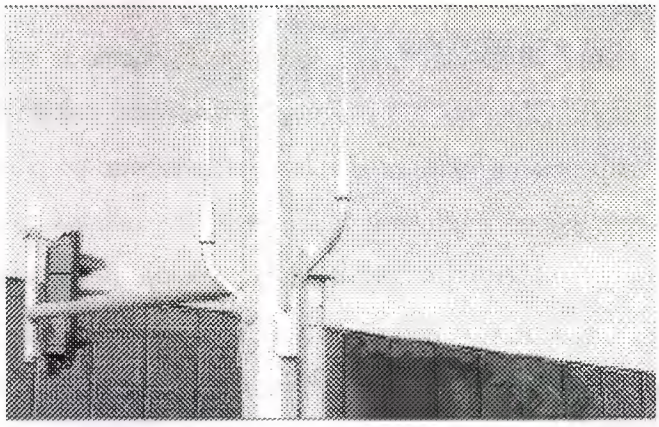


Figure 1.11 Transmitting antenna 3

"This is a large point of confusion with, I think, most RF or radio frequency engineers, so you'll see it written about incorrectly. While at AirTouch, I had the good fortune to work for a few months with a consultant who was retired from Bell Labs. He was one of the engineers who worked on cellular in the 60s and 70s. We had a few discussions on this at air touch and many of the engineers still didn't get it. And, of course, I had access

to Dr. Lee frequently during my years there. It doesn't get much more authoritative than the guys who developed the stuff! Jim Harless, a regular contributor, recently checked in regarding six sector cells. He agrees with Mark about the early days, that six sector cells in AMPS did not work out. He notes that "At Metawave (external link) I've been actively involved in converting some busy CDMA cells to 6-sector using our smart antenna platform. Although our technology is vendor specific, you can't use it with all equipment, it actually works quite well, regardless of the added number of pilots and increase in soft handoffs. In short, six sector simply allows carriers to populate the cell with more channel elements. Also, they are looking for improved cell performance, which we have been able to provide. By the way, I think the reason early CDMA papers had inflated capacity numbers were because they had six sector cells in mind." Mark says "I don't recall any discussion of anything like that. But Qualcomm knew next to nothing about a commercial mobile radio environment. They had been strictly military contractors. So they had a lot to learn, and I think they made some bad assumptions early on. I think they just underestimated the noise levels that would exist in the real world. I do know for sure that the 'other carrier jammer' problem caught them completely by surprise. That's what we encountered when mobiles would drive next to a competitors site and get knocked off the air. They had to re-design the phone.

1.4 Basic Theory and Operation

Cell phone theory is simple. Executing that theory is extremely complicated. Each cell site has a base station with a computerized 800 or 1900 megahertz transceiver and an antenna. This radio equipment provides coverage for an area that's usually two to ten miles in radius. Even smaller cell sites cover tunnels, subways and specific roadways. An area's size depends on, among other things, topography, population, and traffic. When you turn on your phone the mobile switch determines what cell will carry the call and assigns a vacant radio channel within that cell to take the conversation. It selects the cell to serve you by measuring signal strength, matching your mobile to the cell that has picked up When you turn on your phone the mobile switch determines what cell will carry the call and assigns a vacant radio channel within that cell to take the conversation. It selects the cell to serve you by measuring signal strength, matching your mobile to the cell that has picked up the strongest signal. Managing handoffs or handovers, that is, moving from cell to cell, is handled in a similar manner. The base station serving your call sends a hand-off request to the mobile switch after your signal

drops below a handover threshold. The cell site makes several scans to confirm this and then switches your call to the next cell. You may drive fifty miles, use 8 different cells and never once realize that your call has been transferred. At least, that is the goal. Let's look at some details of this amazing technology, starting with cellular's place in the radio spectrum and how it began. The FCC allocates frequency space in the United States for commercial and amateur radio services. Some of these assignments may be coordinated with the International Telecommunications Union but many are not. Much debate and discussion over many years placed cellular frequencies in the 800 megahertz band. By comparison, PCS or Personal Communication Services technology, still cellular radio, operates in the 1900 MHz band. The FCC also issues the necessary operating licenses to the different cellular providers. Although the Bell System had trialed cellular in early 1978 in Chicago, and worldwide deployment of AMPS began shortly thereafter, American commercial cellular development began in earnest only after AT&T's breakup in 1984. The United States government decided to license two carriers in each geographical area. One license went automatically to the local telephone companies, in telecom parlance, the local exchange carriers or LECs. The other went to an individual, a company or a group of investors who met a long list of requirements and who properly petitioned the FCC. And, perhaps most importantly, who won the cellular lottery. Since there were so many qualified applicants, operating licenses were ultimately granted by the luck of a draw, not by a spectrum auction as they are today.

The local telephone companies were called the wireline carriers. The others were the non-wireline carriers. Each company in each area took half the spectrum available. What's called the "A Band" and the "B Band." The nonwireline carriers usually got the A Band and the wireline carriers got the B band. There's no real advantage to having either one. It's important to remember, though, that depending on the technology used, one carrier might provide more connections than a competitor does with the same amount of spectrum. Mobiles transmit on certain frequencies, cellular base stations transmit on others. A and B refer to the carrier each frequency assignment has. A channel is made up of two frequencies, one to transmit on and one to receive.

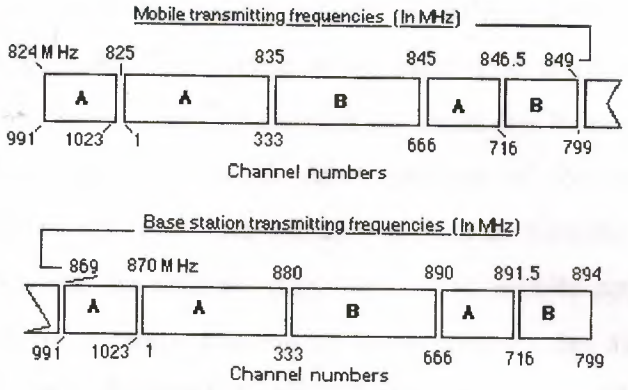


Figure 1.12 Mobile transmitting frequencies(in MHz)

The latter is responsible for the high voice quality and high signaling reliability of the Advanced Mobile Phone Service. In any given area, both the size of the cells and the distance between cells using the same group of channels determine the efficiency with which frequencies can be reused. When a system is newly installed in an area (when large cells are serving only a few customers), frequency reuse is unnecessary. Later, as the service grows, a dense system will have many small cells and many customers), a given channel in a large city could be serving customers in twenty or more nonadjacent cells simultaneously. The cellular plan permits staged growth. To progress from the early to the more mature configuration over a period of years, new cell sites can be added halfway between existing cell sites in stages. Such a combination of newer, smaller cells and original, larger cells .

One cellular system is the Western Electric AUTOPLEX-100. In this system, a mobile or portable unit in a given cell transmits to and receives from a cell site, or base station, on a channel assigned to that cell. In a mature system, these cell sites are located at alternate corners of each of the hexagonal cells. Directional antennas at each cell site point toward the centers of the cells, and each site is connected by standard land transmission facilities to a 1AESS switching system and system controller equipped for Advanced Mobile Phone Service operation (called a mobile telecommunications switching office, or MTSO). Start-up and small-city systems use a somewhat more conventional configuration with a single cell site at the center of each cell. The efficient use of frequencies that results from the cellular approach permits Advanced Mobile Phone Service customers to enjoy a level of service almost unknown with present

mobile telephone service. Grades of service of P(0.02) are anticipated,compared to today's all-too-common P(0.5) or worse. At the same time, the number of customers in a large city can be increased from a maximum of about one thousand for a conventional system to several hundred thousand. Also, because of the stored-program control capability of MTSOs equipped with the lAESS system, Custom Calling Services and man other features can be offered, some unique to mobile service. Other, smaller, switches provided by Western Electric or other vendors are also available to serve smaller cities and towns. System Operation: Unlike the MJ and MK systems, Advanced Mobile hone Service dedicates a special subset of the 333 allocated channels solely to signaling and control. Each mobile or portable unit is equipped with a frequency synthesizer (to generate any one of the 333 channels) and a high speed modem (10 kbps). When idle, a mobile unit chooses the "best control channel to listen to (by measuring signal strength) and reads the high-speed messages coming over this channel. The messages include the identities of called mobiles, local general control information, channel assignments for active mobiles and "filler" words to maintain synchronism. These data are made highly redundant to combat multi-path interference. A user is alerted to an incoming call when the mobile unit recognizes its identity code in the data message. From the user's standpoint, calls are initiated and received as they would be from any business or residence telephone. As a mobile unit engaged in a call moves away from a cell site and its signal weakens, the MTSO will automatically instruct it to tune to a different frequency, one assigned to the newly entered cell.

This is called handoff. The MTSO determines when handoff should occur by analyzing measurements of radio signal strength made by the present controlling cell site and by its neighbors. The returning instructions for handoff sent during a call must use the voice channel. The data regarding the new channel are sent rapidly (in about 50 milliseconds), and the entire retuning process takes only about 300 milliseconds. In addition to channel assignment, other MTSO functions include maintaining a list of busy (that is, off-hook) mobile units and paging mobile units for which incoming calls are intended. Regulatory Picture.The FCC intends cellular service to be regulated by competition, with two competing system providers in each large city: a wire-line carrier and a radio common carrier. To prevent any possible cross-subsidization or favoritism, the Bell operating companies must offer their cellular service through separate subsidiaries. These subsidiaries will be chiefly providers of service and, in fact, are

currently barred from leasing or selling mobile or portable equipment. Such equipment will be sold by nonaffiliated enterprises or by American Bell Inc.

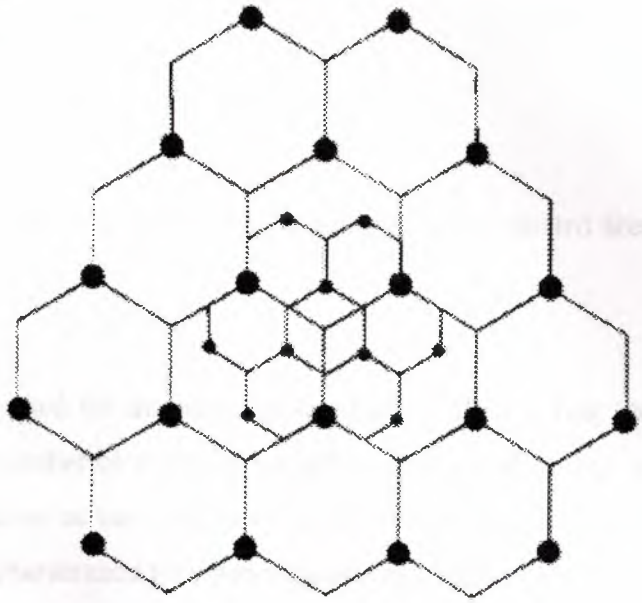


Figure 1.13 Cells splitting

1.5 Cellular coverage

1.5.1 Cluster

The cells are grouped into clusters. The number of cells in a cluster must be determined so that the cluster can be repeated continuously within the covering area of an operator. The typical clusters contain 4, 7, 12 or 21 cells. The number of cells in each cluster is very important. The smaller the number of cells per cluster is, the bigger the number of channels per cell will be. The capacity of each cell will be therefore increased. However a balance must be found in order to avoid the interference that could occur between neighboring clusters. This interference is produced by the small size of the clusters (the size of the cluster is defined by the number of cells per cluster). The total number of channels per cell depends on the number of available channels and the type of cluster used.

1.5.2 Types of cells

The density of population in a country is so varied that different types of cells are used:

- Macrocells
- Microcells
- Selective cells
- Umbrella cells

a) Macrocells

The macrocells are large cells for remote and sparsely populated areas.

b) Microcells

These cells are used for densely populated areas. By splitting the existing areas into smaller cells, the number of channels available is increased as well as the capacity of the cells. The power level of the transmitters used in these cells is then decreased, reducing the possibility of interference between neighboring cells.

c) Selective cells

It is not always useful to define a cell with a full coverage of 360 degrees. In some cases, cells with a particular shape and coverage are needed. These cells are called selective cells. A typical example of selective cells are the cells that may be located at the entrances of tunnels where a coverage of 360 degrees is not needed. In this case, a selective cell with a coverage of 120 degrees issused.

d) Umbrella cells

A freeway crossing very small cells produces an important number of handovers among the different small neighboring cells. In order to solve this problem, the concept of umbrella cells is introduced. An umbrella cell covers several microcells. The power level inside an umbrella cell is increased comparing to the power levels used in the microcells that form the umbrella cell.

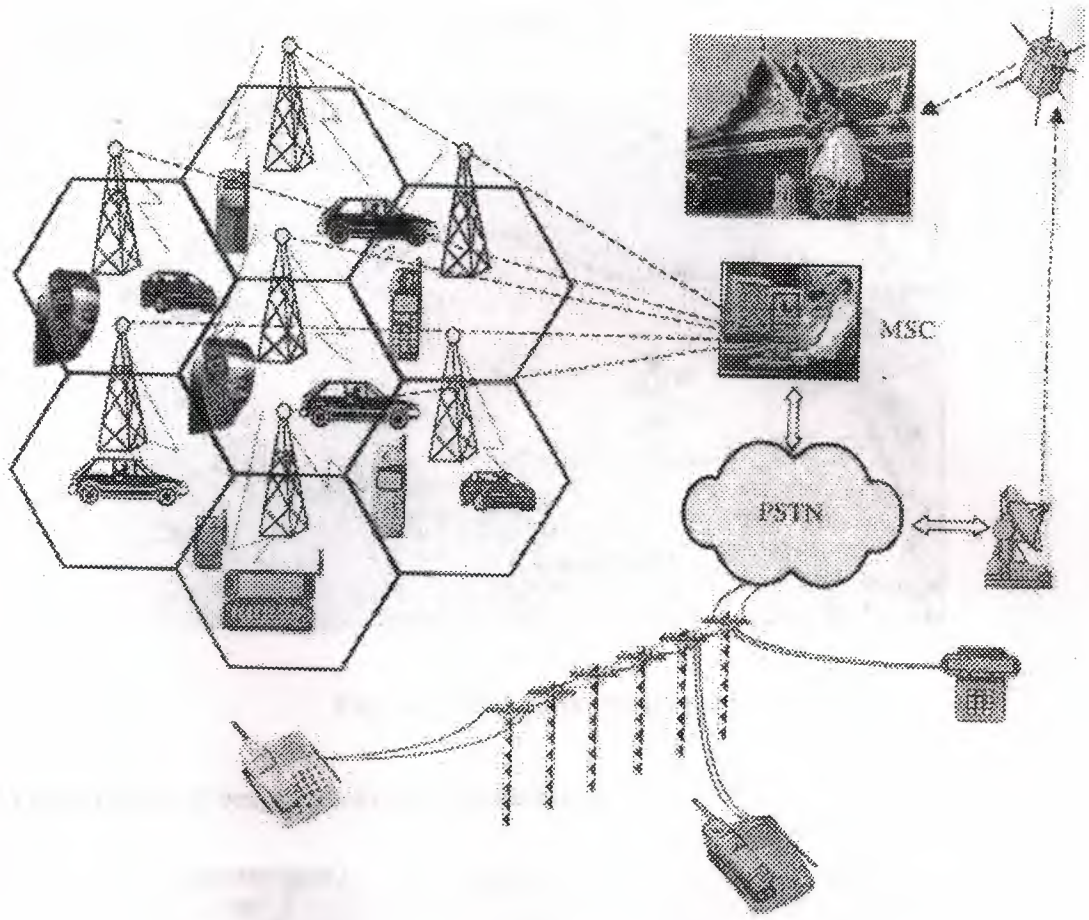


Figure 1.14 Cellular coverage network

When the speed of the mobile is too high, the mobile is handed off to the umbrella cell. The mobile will then stay longer in the same cell (in this case the umbrella cell). This will reduce the number of handovers and the work of the network. A too important number of handover demands and the propagation characteristics of a mobile can help to detect its high speed,The figure belows shows the coverage area maps in Turkey.

1. Aria comm. Company (coverage area map):

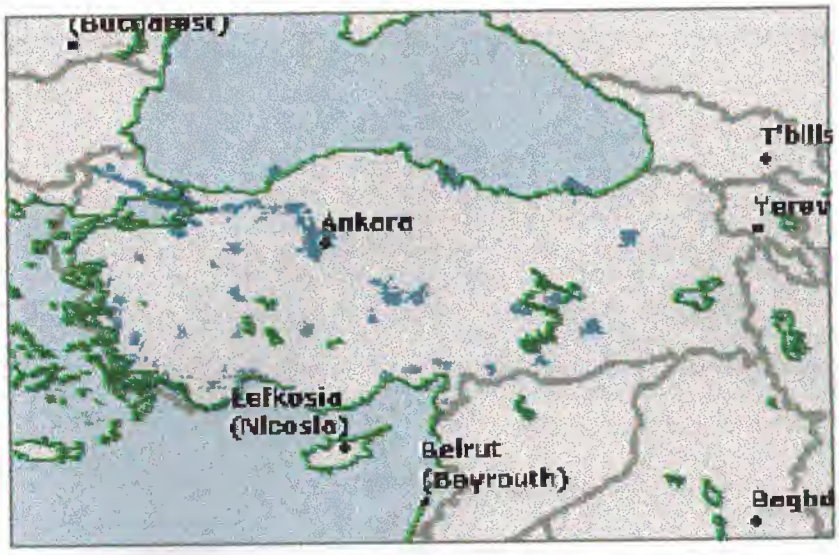


Figure 1.15 Aria coverage map

2. Aycell comm. Company(coverage area map)

Figure 1.16 Aycell coverage map

3. Telsim comm.company (coverage area map):

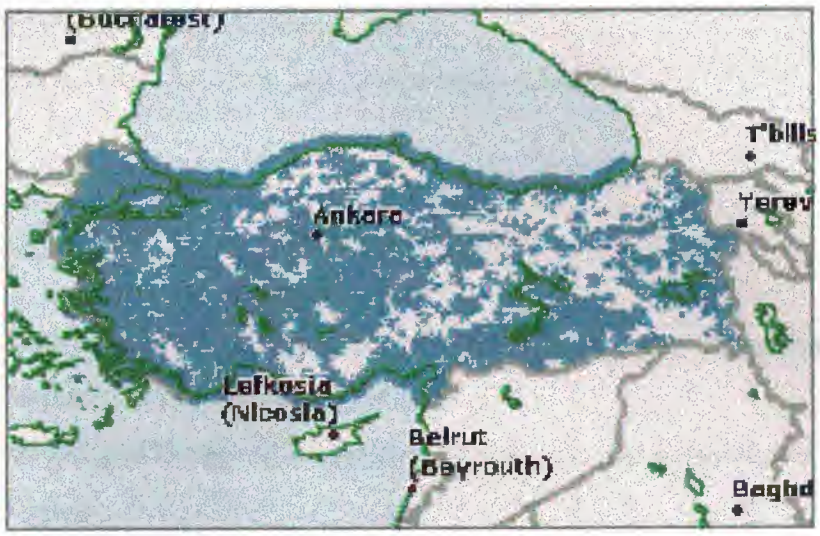


Figure 1.17 Telsim coverage map

4. Turkcell comm.company (coverage area map):

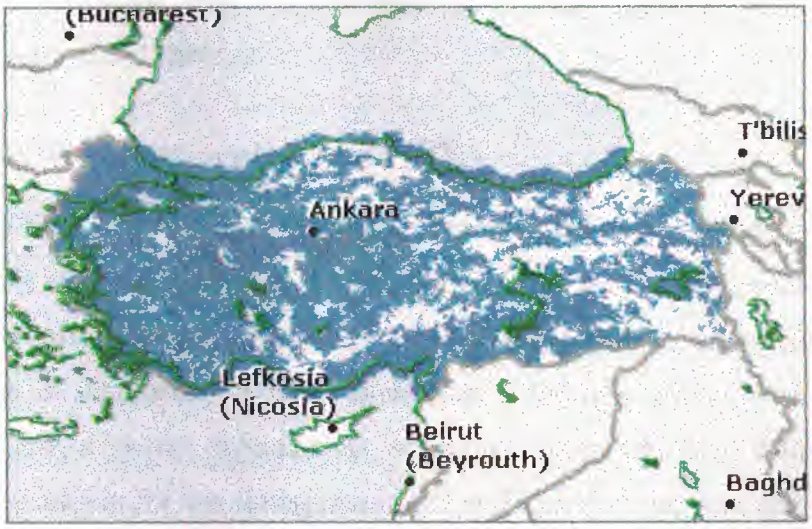


Figure 1.18 Turkcell coverage map

1.6 The GSM functions

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

- Transmission.

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

1.6.1 Transmission

The transmission function includes two sub-functions:

- The first one is related to the means needed for the transmission of user information.
- The second one is related to the means needed for the trasnmission of signaling information.

Not all the components of the GSM network are strongly related with the transmission functions. The MS, the BTS and the BSC, among others, are deeply concerned with transmission. But other components, such as the registers HLR, VLR or EIR, are only concerned with the transmission for their signaling needs with other components of the GSM network.

1.6.2 Radio Resources management (RR)

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 mobile station and the base station. However, as the RR function is also in charge of maintaining a connection even if the user moves from one cell to another, the MSC, in charge of handovers, is also concerned with the RR functions. The RR is also responsible for the management of the frequency spectrum and the reaction of the network to changing radio environment conditions. Some of the main RR procedures that assure its responsabilities are:

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

- Timing advance.

In this paragraph only the handover, which represents one of the most important responsabilities of the RR, is described.

a) Handover

The user movements can produce the need to change the channel or cell, specially when the quality of the communication is decreasing. This procedure of changing the resources is called handover. Four different types of handovers can be distinguished:

- Handover of channels in the same cell.
- Handover of cells controlled by the same BSC.
- Handover of cells belonging to the same MSC but controlled by different BSCs.
- Handover of cells controlled by different MSCs.

Handovers are mainly controlled by the MSC. However in order to avoid unnecessary signalling information, the first two types of handovers are managed by the concerned BSC (in this case, the MSC is only notified of the handover). The mobile station is the active participant in this procedure. In order to perform the handover, the mobile station controls continuously its own signal strengh and the signal strengh of the neighboring cells. The list of cells that must be monitored by the mobile station is given by the base station. The power measurements allow to decide which is the best cell in order to maintain the quality of the communication link. Two basic algorithms are used for the handover:

- The `minimum acceptable performance' algorithm. When the quality of the transmission decreases (i.e the signal is deteriorated), the power level of the mbbile is increased. This is done until the increase of the power level has no effect on the quality of the signal. When this happens, a handover is performed.
- The `power budget' algorithm. This algorithm performs a handover, instead of continuously increasing the power level, in order to obtain a good communication quality.

1.6.3 Mobility Management

The MM function is in charge of all the aspects related with the mobility of the user, specially the location management and the authentication and security.

1.6.4 Location management

When a mobile station is powered on, it performs a location update procedure by indicating its IMSI to the network. The first location update procedure is called the IMSI attach procedure.

The mobile station also performs location updating, in order to indicate its current location, when it moves to a new Location Area or a different PLMN. This location updating message is sent to the new MSC/VLR, which gives the location information to the subscriber's HLR. If the mobile station is authorized in the new MSC/VLR, the subscriber's HLR cancells the registration of the mobile station with the old MSC/VLR. A location updating is also performed periodically. If after the updating time period, the mobile station has not registered, it is then deregistered. When a mobile station is powered off, it performs an IMSI detach procedure in order to tell the network that it is no longer connected.

1.6.5 Authentication and security

The authentication procedure involves the SIM card and the Authentication Center. A secret key, stored in the SIM card and the AuC, and a ciphering algorithm called A3 are used in order to verify the authenticity of the user. The mobile station and the AuC compute a SRES using the secret key, the algorithm A3 and a random number 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. Another security procedure is to check the equipment identity. If the IMEI number of the mobile is authorized in the EIR, the mobile station is allowed to connect the network. In order to assure user confidentiality, the user is registered with a Temporary Mobile Subscriber Identity (TMSI) after its first location update procedure.

1.6.6 Communication Management (CM)

The CM function is responsible for:

- Call control.
- Supplementary Services management.
- Short Message Services management.

a) Call Control (CC)

The CC is responsible for call establishing, maintaining and releasing as well as for selecting the type of service. One of the most important functions of the CC is the call routing. In order to reach a mobile subscriber, a user diales the Mobile Subscriber ISDN (MSISDN) number which includes:

- a country code
- a national destination code identifying the subscriber's operator
- a code corresponding to the subscriber's HLR

The call is then passsed to the GMSC (if the call is originated from a fixed network) which knows the HLR corresponding to a certain MISDN number. The GMSC asks the HLR for information helping to the call routing. 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. Thanks to the MSRN number, the call is routed to subscriber's current MSC/VLR. In the subscriber's current LA, the mobile is paged.

b) Supplementary Services management

The mobile station and the HLR are the only components of the GSM network involved with this function.

c) Short Message Services management

In order to support these services, a GSM network is in contact with a Short Message Service Center through the two following interfaces:

- The SMS-GMSC for Mobile Terminating Short Messages (SMS-MT/PP). It has the same role as the GMSC.
- The SMS-IWMSC for Mobile Originating Short Messages (SMS-MO/PP).

1.6.7 Operation, Administration and Maintenance (OAM)

The OAM function allows the operator to monitor and control the system as well as to modify the configuration of the elements of the system. Not only the OSS is part of the OAM, also the BSS and NSS participate in its functions as it is shown in the following examples:

- The components of the BSS and NSS provide the operator with all the information it needs. This information is then passed to the OSS which is in charge of analize it and control the network.
- The self test tasks, usually incorporated in the components of the BSS and NSS, also contribute to the OAM functions.
- The BSC, in charge of controlling several BTSs, is another example of an OAM function performed outside the OSS.

2. GSM (PLMN), CHANNEL AND FRAME STRUCTURES

2.1 GSM Public Land Mobile Network (PLMN)

ETSI originally defined GSM as a European digital cellular telephony standard. GSM interfaces defined by ETSI lay the groundwork for a multivendor network approach to digital mobile communication. GSM offers users good voice quality, call privacy, and network security. Subscriber Identity Module (SIM) cards provide the security mechanism for GSM. SIM cards are like credit cards and identify the user to the GSM network. They can be used with any GSM handset, providing phone access, ensuring delivery of appropriate services to that user, and automatically billing the subscriber's network usage back to the home network.

Roaming agreements have been established between most GSM network providers in Europe, allowing subscribers to roam between networks and have access to same services no matter where they travel. Of major importance is GSM's potential for delivering enhanced services requiring multimedia communication: Voice, image, and data. Several mobile service providers offer free voice mailboxes and phone answering services to subscribers. The key to delivering enhanced services is Signaling System Number 7 (SS7), a robust set of protocol layers designed to provide fast, efficient, reliable transfer and delivery of signaling information across the signaling network and to support both switched-voice and nonvoice applications. With SS7 on the enhanced services platform and integrating mailbox parameters, subscribers can be notified about the number of stored messages in their mailboxes, time and source of last messages, message urgency, and type of message-voice or fax. Future applications such as fax store-and-forward and audiotext can also use the platform's voice-and data-handling capabilities.

2.2 Objectives of a GSM PLMN

A GSM PLMN cannot establish calls autonomously other than local calls between mobile subscribers. In most of the cases, the GSM PLMN depends upon the existing wireline networks to route the calls. Most of the time the service provided to a subscriber is the combination of the access service by a GSM PLMN and the service by

some existing wireline network. Thus, the general objectives of a GSM PLMN with respect to service to a subscriber are:

- To provide the subscriber with a wide range of services and facilities, both voice and nonvoice, that are compatible with those offered by existing networks (e.g., PSTN, ISDN).
- To introduce a mobile RS that is compatible with ISDN.
- To provide certain services and facilities exclusive to mobile situations.
- To give compatibility of access to the GSM network for a mobile subscriber in a country that operates the GSM system.
- To provide facilities for automatic roaming, locating, and updating of mobile subscribers.
- To provide service to a wide range of mobile stations, including vehicle-mounted stations, portable stations, and handheld stations.
- To provide for efficient use of the frequency spectrum.
- To allow for a low-cost infrastructure, terminal, and service cost.

2.3 GSM PLMN Services

A telecommunication service supported by the GSM PLMN is defined as a group of communication capabilities that the service provider offers to the subscribers. The basic telecommunication services provided by the GSM PLMN are divided into three main groups: Bearer services, teleservices, and supplementary services.

2.3.1 Bearer Services

These services give the subscriber the capacity required to transmit appropriate signals between certain access points (i.e., user-network interfaces). The capabilities of the GSM bearer services are the following:

- Rate-adapted subrate information-circuit-switched asynchronous and synchronous duplex data, 300-9,600 bps.
- Access to Packet Assembler/Disassembler (PAD) functions-PAD access for asynchronous data, 300-9,600 bps.
- Access to X.25 public data networks-packet service for synchronous duplex data, 2,400-9,600 bps.
- Speech and data swapping during a call-alternate speech/data and speech followed by data.

- Modem selection-selection of 3.1-kHz audio service when interworking to an ISDN.
- Support of automatic request for retransmission (ARQ) technique for improved error rates-transparent mode (no ARQ) and nontransparent mode (with ARQ).

Table 2.1 provides a summary of these services and compares them with services available with ISDN.

2.3.2 Teleservices

These services provide the subscriber with necessary capabilities including terminal equipment functions to communicate with other subscribers. The GSM teleservices are:

- Speech transmission-Telephony, emergency call.
- Short Message Services-mobile terminating point-to-point, mobile-originating point-to-point, cell broadcast.

Table 2.1 A Comparison of Bearer Services Supported by GSM and ISDN

Service	GSM	ISDN
Data services	X	X
Alternate speech/data	X	X
Speech followed by data	X	X
Clear 3.1-kHz audio	X	X
Unrestricted digital information (UDI)	X	X
Packet Assembler/Disassembler (PAD)	X	
3.1-kHz external to PLMN	X	
Others		X

- Message handling and storage services.
- Videotex access.
- Teletex transmission.
- Facsimile transmission.

A summary of the teleservices is given in Table 2.2. A comparison is made between the GSM and ISDN teleservices.

2.3.3 Supplementary Services

These services modify or supplement basic telecommunications services and are offered together with or in association with basic telecommunications services. You should note that most of the supplementary services in GSM have been aligned with the North American supplementary services specified by ATSI. The GSM supplementary services are:

- **Number identification services:**
    1. Calling Number Identification Presentation (CNIP).
    2. Calling Number Identification Restriction (CNIR).
    3. Connected Number Identification Presentation (CNOP).
    4. Connected Number Identification Restriction (CNOR).
    5. Malicious Call Identification (MCI).
- **Calling Offering Services:**
    1. Call Forwarding Unconditional (CFU).
    2. Call Forwarding mobile Busy (CFB).
    3. Call Forwarding No Reply (CFNRy).
    4. Call Forwarding mobile Not Reachable (CFNRc).
    5. Call Transfer (CT).
    6. Mobile Access Hunting (MAH).

Table 2.2 A comparision of Teleservices Supported by GSM and ISDN

Service	GSM	ISDN
Circuit speech (telephony)	X	X
Emergency call	X	X
Short message point-to-point	X	X
Short message cell broadcast	X	X
Alternate speech/facsimile group 3	X	X
Automatic facsimile group 3 service	X	X
Voice-band modem (3.1-kHz audio)	X	X
Messaging teleservices	X	
Paging teleservices	X	
Others		X

- **Call Completion Services:**
    1. Call Waiting (CW).
    2. Call Holding (HOLD).
    3. Completion of Call to Busy Subscriber (CCBS).
- **Multiparty Services:**
    1. 3-Party service (3PTY).
    2. Conference Calling (CONF).
- **Community of Interest Services:**
    1. Closed User Group (CUG).
- **Charging Services:**
    1. Advice of Charge (AoC).
    2. Freephone Service (FPH).
    3. Reverse Charging (REVC).
- **Additional Information Transfer Service:**
    1. User-to-User Signaling (UUS).
- **Call Restrictions Services:**
    1. Barring All Originating Calls (BAOC).
    2. Barring Outgoing International Calls (BOIC).
    3. BOIC except Home Country (BOIC-exHC).
    4. Barring All Incoming Calls (BAIC).
    5. Barring Incoming Calls when Roaming (BIC-Roam).

The GSM system offers an opportinity to a subscriber of moving freely through countries where a GSM PLMN is operational. Agreements are required between the various service providers to guarantee access to service offered to subscribers.

2.4 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 (F_u) and downlink (F_d) frequency can be obtained from Eqs. (2.1) and (2.2), respectively:

$$F_u = 890.2 + 0.2\,(N\text{-}1)\ \text{MHz} \qquad (2.1)$$ where: N = 1, 2, ..., 124.

$$F_d = 935.2 + 0.2\,(N\text{-}1)\ \text{MHz} \qquad (2.2)$$

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, F_u and other for the downlink, F_d. Each pair of radio channels supports up to eight simultaneous calls (see Figure 2.1). Thus, the GSM can support up to 992 simultaneous users with the full-rate speech coder. This number will be doubled to 1,984 users with the half-rate speech coder.

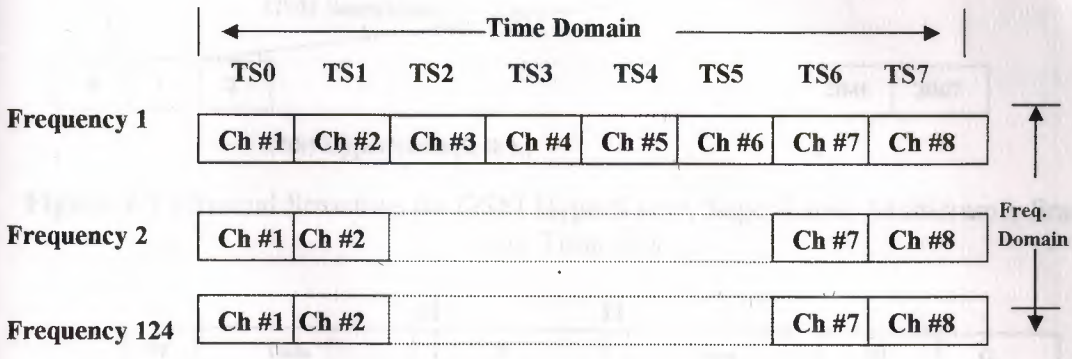


Figure 2.1 GSM FDMA/TDMA Structure

2.4.1 GSM Frame

The GSM multiframe is 120 ms. It consists of 26 frames of 8 time slots. The structure of a GSM hyperframe, superframe, multiframe, frame, and time slot is shown in Figure 2.2 A time slot carries 156.25 bits. The same format is used for the uplink and downlink transmission with various burst types as shown in Figure 2.3 In a normal burst, 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 Guard (G) bits.2

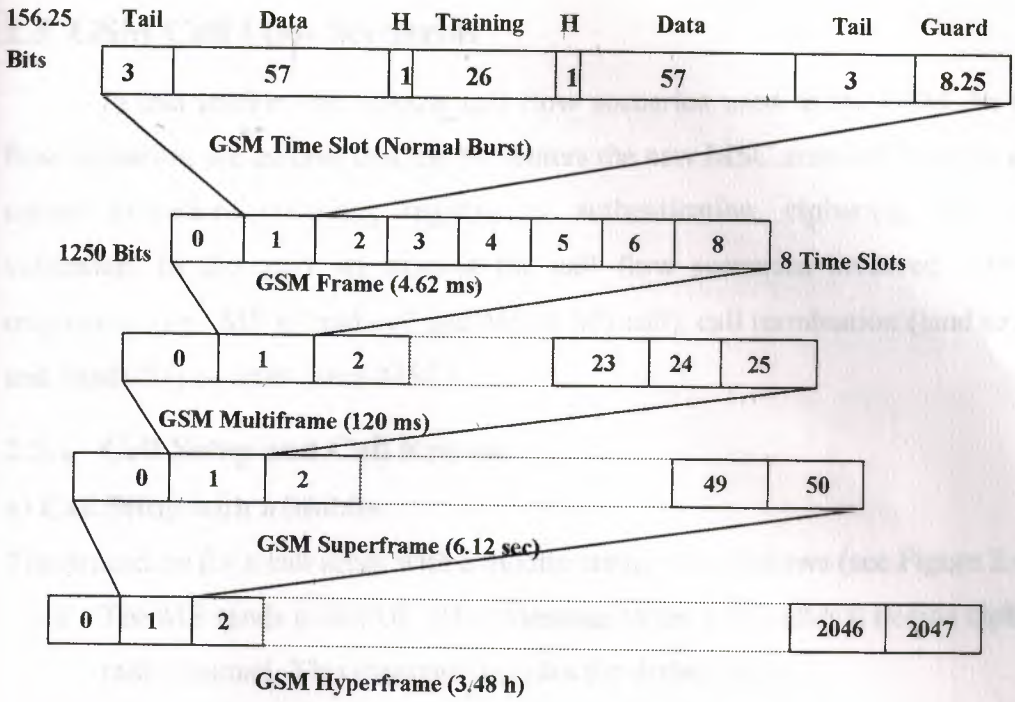
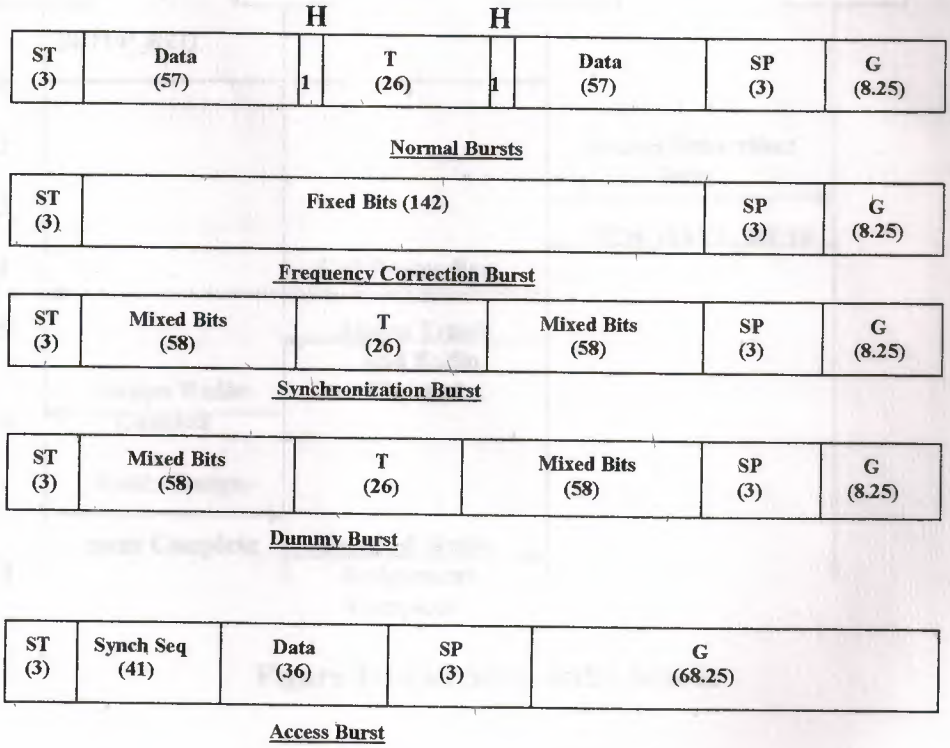


Figure 2.2 Physical Structure for GSM Hyperframe, Superframe, Multiframe, Frame, and Time Slot



ST: Start bits **T: Training bits**
SP: Stop bits **G: Guard time**
H: Stealing bit

Figure 2.3 GSM Time Slot Structure

2.5 GSM Call Flow Scenarios

In this section, we discuss call flow scenarios used in the GSM. In these call flow scenarios, we assume that the MS enters the new MSC area and requires a location update procedure involving registration, authentication, ciphering, and equipment validation. In this part we discuss the call flow scenarios involved with 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).

2.5.1 Call Setup and Call Release

a) Call Setup with a Mobile:

The procedure for a call setup with a mobile station is as follows (see Figure 2.4):

1. The MS sends a SETUP_REQ message to the MSC after it begins ciphering the radio channel. This message includes the dialed digits.

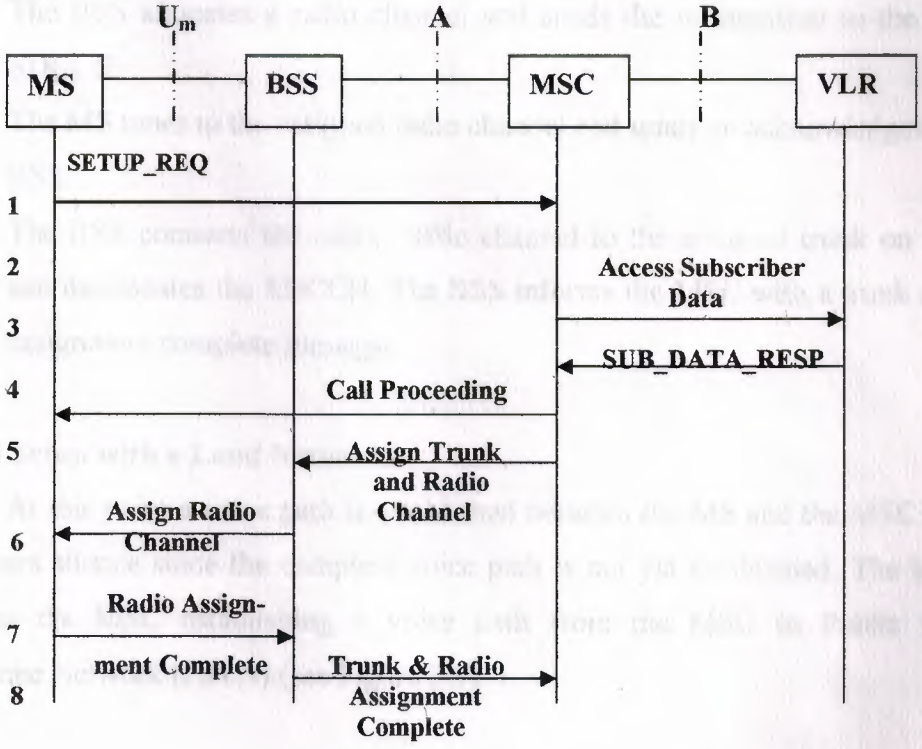


Figure 2.4 Call Setup with a Mobile

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 that 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 acknowledgment 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.

b) 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) (see Figure 2.5).

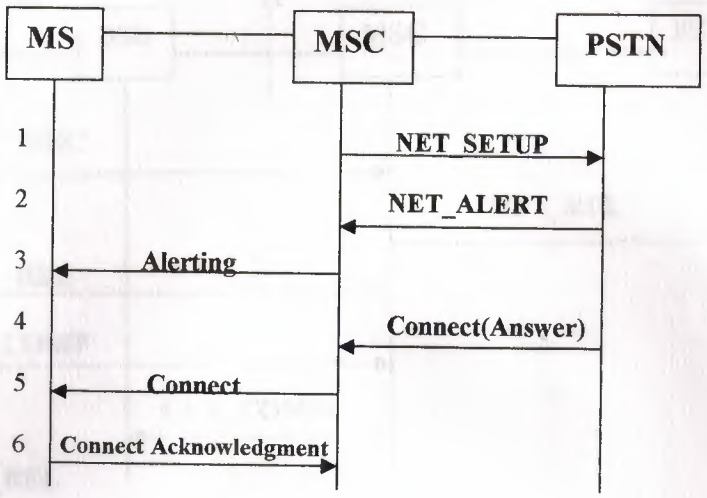


Figure 2.5 Call Setup with Land Network

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 sets up 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.

c) Call Release-Mobile Initiated:

Under normal conditions, there are two basic ways a call is terminated: Mobile initiated and network initiated. In this scenario, we assume that the mobile user initiates the release of the call (see Figure 2.6).

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 a NET_REL request message to the PSTN to release the call.
3. The MSC asks the MS to begin its clearing procedure using the CALL_REL message.

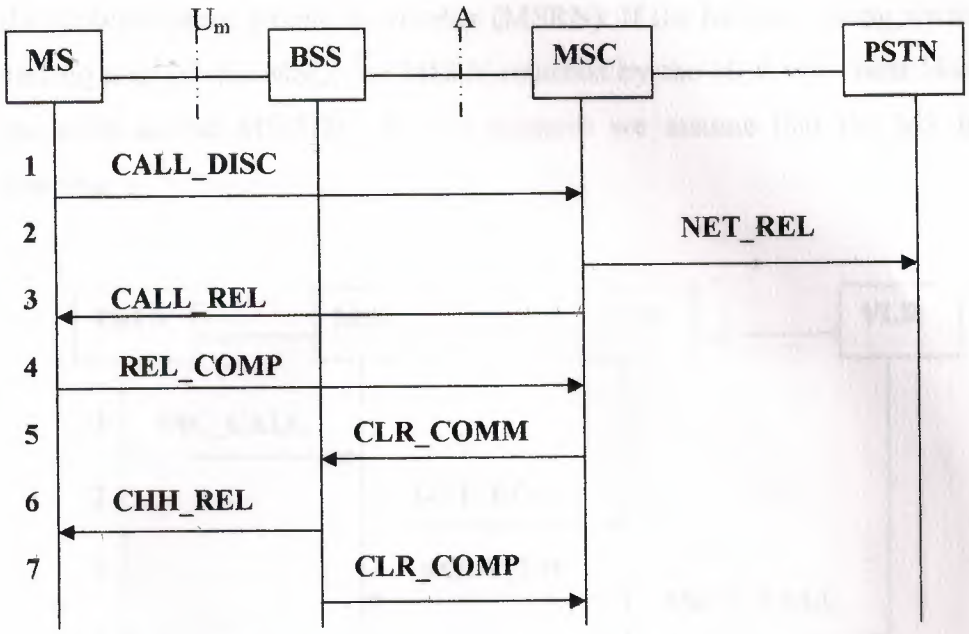


Figure 2.6 Mobile to Land Call: Call Release _ Mobile Initiated

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.

d) Routing Analysis_ Land to Mobile Call:

In this scenario we assume that the MS is already registered with the system and has been assigned a TMSI. We also assume that the MS is in its home system. A land subscriber dials the directory number of the mobile subscriber (see Figure 2.7).

1. The PSTN routes the call to the MSC assigned this directory number. The directory number in the INC_CALL message is the 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 serving area of this MSC, the MSRN returned by the HLR will most likely be the same as the MSISDN. In this scenario we assume that the MS is not roaming.

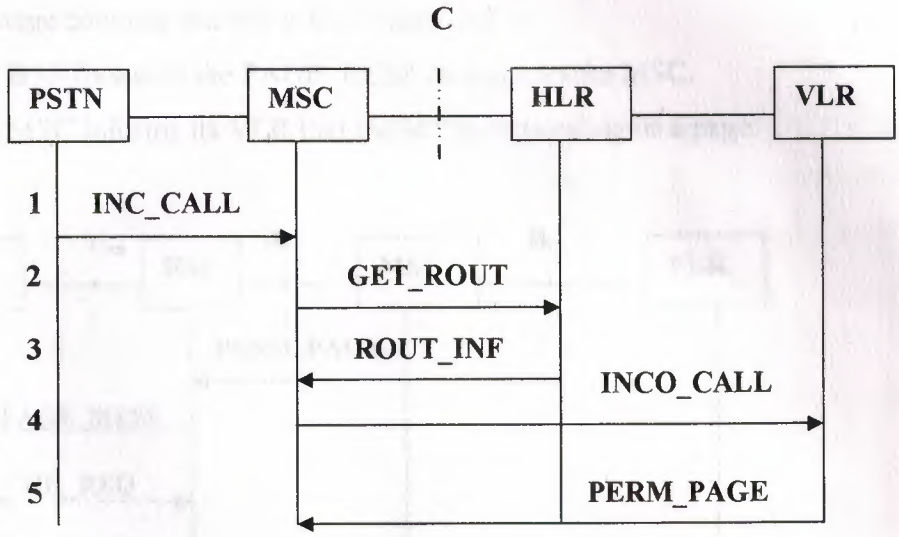


Figure 2.7 Land to Mobile Call_ Routing Analysis

4. The MSC informs its VLR about the incoming call using a INCO_CALL message that includes MSRN.
5. The VLR responds to the MSC through a PERM_PAGE message that specifies Location Area Identification (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.

e) Paging _ Land to Mobile Call:

The following is the procedure for paging in a land to mobile call (refer to Figure 2.8).

1. The MSC uses the LAI provided by the VLR to 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 broadcasts 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 the 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.

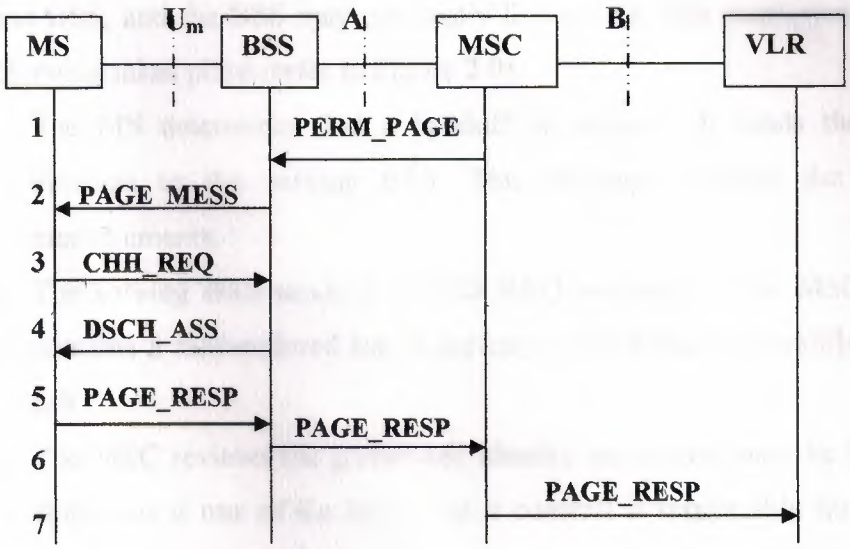


Figure 2.8 Paging _ Land to Mobile Call

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.

2.5.2 Handoff

Basically there are two levels of handoffs: Internal and 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

type of handoff the MSC coordinates the handoff and performs the switching tasks between the serving and target BTSs. The external handoffs can be classified as: Within the same MSC (i.e., intra-MSC) and between different MSCs (i.e., inter-MSC). In the following call flow scenarios we focus only upon the external hand-offs. We discuss the intra-MSC and inter-MSC handoff.

a) Intra-MSC Handoff:

When the MS determines that a handoff is required in an attempt to maintain the desired signal quality of the radio link (The signal quality is constantly monitored by the MS and BSS, and the BSS may optionally forward its own measurements to the MS), the following takes place (refer to Figure 2.9).

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 the MSC. This message contains a rank-ordered list of the target BSSs that are qualified to receive the 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 a 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 (K_c).
4. The target BSS selects and reserves the appropriate resources to support the handoff pending the connection execution. The target BSS sends an acknowledgement 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 retunes to the new radio channel and sends the HAND_ACC message. to the target BSS on the new radio channel.
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 resources with the MS and sends the REL_RCH_COMP message to the MSC.

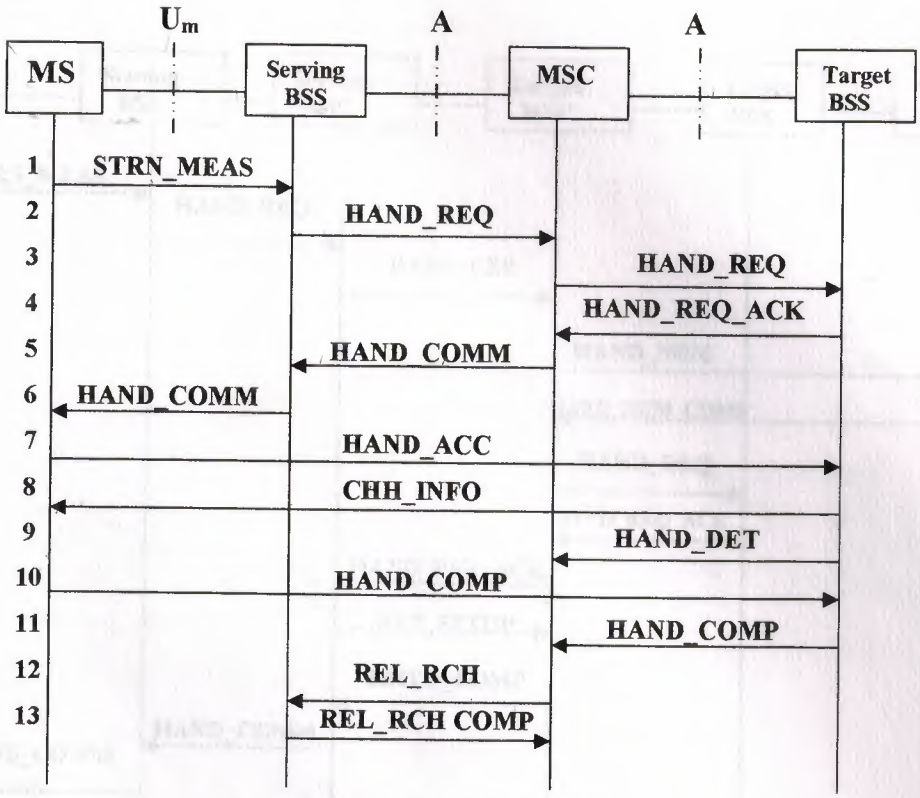


Figure 2.9 Intra-MSC Handoff

Note that GSM Recommendations require that the "open interval gap" during a handoff will not exceed 150 ms for 90% of the handoffs. The "open interval gap" starts when the MS retunes to the new radio channel and ends after synchronization without any loss in voice/data transmission in the BSS or MSC.

b) Inter-MSC Handoff:

In this scenario we assume that 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 (see Figure 2.10):

1. Same as in the intra-MSC handoff (step 1).
2. Same as in the intra-MSC handoff (step 2).

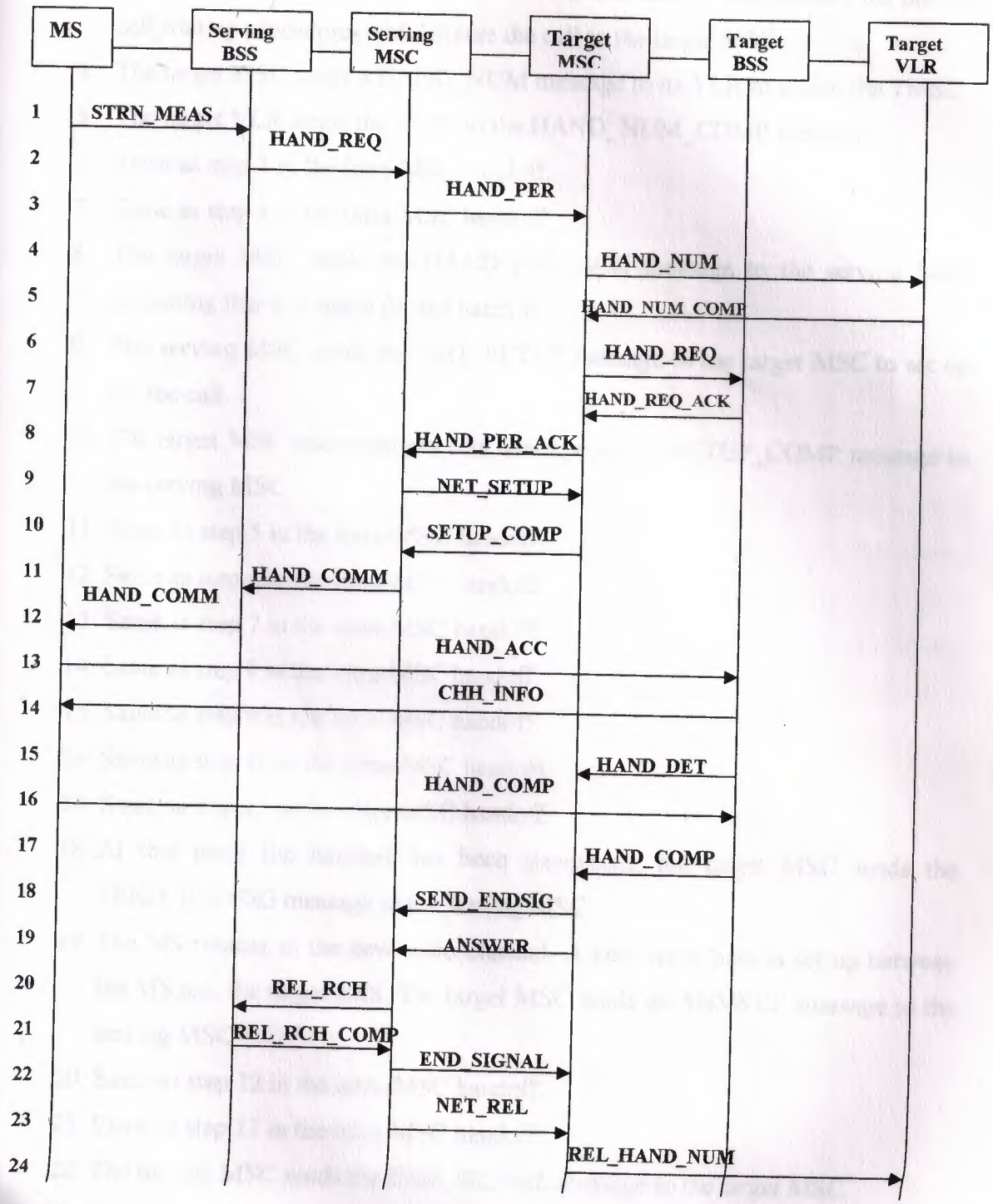


Figure 2.10 Inter-MSC Handoff

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 the 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 set up 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 set up between the MS 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.

2.6 MSC Performance

The MSC performance will meet the GSM Recommendations, Series 2.08 and 3.05. The reliability objectives of the MSC as per GSM Recommendations, Series 3.05 and 3.06 are:

- Cutoff call or call release failure rate probability: $P \leq 0.0002$.
- Probability of incorrect charging, misrouting, no tone, or other failures: $P \leq 0.0001$.
- Mean Accumulated Intrinsic Down Time (MAIDT) for one termination, or MAIDT (1) $\leq$ 30 minutes/year.
- Probability of losing HLR/VLR messages: $P \leq 0.0000001$.

The service availability of an MSC is expressed in terms of the frequency or duration of loss of service. The loss of service to particular circuits, groups of circuits, subsystems, or the complete MSC is determined by the faults in the MSC. The average cumulative duration of service denial due to faults affecting more than 50% of the circuits will not exceed three minutes during the first year of operation and two minutes during each subsequent year. On the average, a fault that causes more than 50% of the established calls to be disconnected prematurely will occur less than once a year.

3. GSM RADIO INTERFACE

3.1 Overview

The Radio interface is the interface between the mobile stations and the fixed infrastructure. It is one of the most important interfaces of the GSM system. One of the main objectives of GSM is roaming. Therefore, in order to obtain a complete compatibility between mobile stations and networks of different manufacturers and operators, the radio interface must be completely defined. The spectrum efficiency depends on the radio interface and the transmission, more particularly in aspects such as the capacity of the system and the techniques used in order to decrease the interference and to improve the frequency reuse scheme. The specification of the radio interface has then an important influence on the spectrum efficiency.

3.2 Frequency Allocation

Two frequency bands, of 25 MHz each one, have been allocated for the GSM system:

- The band 890-915 MHz has been allocated for the uplink direction (transmitting from the mobile station to the base station).
- The band 935-960 MHz has been allocated for the downlink direction (transmitting from the base station to the mobile station).

These bands were allocated by the ITU (International Telecom Union) who are responsible for allocating radio spectrum on an international basis. Although these bands were (and still are) used by analog systems in the early 1980's, the top 10 MHz were reserved for the already emerging GSM Network by the CEPT (European Conference of Posts and Telecommunications: translated from French). But not all the countries can use the whole GSM frequency bands. This is due principally to military reasons and to the existence of previous analog systems using part of the two 25 Mhz frequency bands.

3.3 Multiple Access Scheme

The multiple access scheme defines how different simultaneous communications, between different mobile stations situated in different cells, share the GSM radio spectrum. A mix of Frequency Division Multiple Access (FDMA) and Time Division Multiple Access (TDMA), combined with frequency hopping, has been adopted as the multiple access scheme for GSM.

It is hoped that eventually the GSM network will use the entire bandwidth. It is apparent from this that the bandwidth you use on a day-to-day basis to operate your mobile phone is limited. It would seem that only a certain number of users can operate on the bandwidth simultaneously. However GSM has devised a method to maximize the bandwidth available. They use a combination of Time and Frequency Division Multiple Access (TDMA/FDMA).

a) **FDMA:** Using FDMA, a frequency is assigned to a user. So the larger the number of users in a FDMA system, the larger the number of available frequencies must be. The limited available radio spectrum and the fact that a user will not free its assigned frequency until he does not need it anymore, explain why the number of users in a FDMA system can be "quickly" limited.

This is the division of the bandwidth in to 124 carrier frequencies each of 200 kHz. At least one of these is assigned to each base station.

b) **TDMA:** TDMA allows several users to share the same channel. Each of the users, sharing the common channel, is assigned their own burst within a group of bursts called a frame. Usually TDMA is used with a FDMA structure.

The carrier frequencies are then divided again into 8 time slots. This prevents mobiles from transmitting and receiving calls at the same time as they are allocated separate time slots

In GSM, a 25 Mhz frequency band is divided, using a FDMA scheme, into 124 carrier frequencies spaced one from each other by a 200 kHz frequency band. Normally a 25 Mhz frequency band can provide 125 carrier frequencies but the first carrier frequency is used as a guard band between GSM and other services working on lower frequencies. Each carrier frequency is then divided in time using a TDMA scheme. This scheme splits the radio channel, with a width of 200 kHz, into 8 bursts. A burst is the unit of time in a TDMA system, and it lasts approximately 0.577 ms. A TDMA frame is formed with 8 bursts and lasts, consequently, 4.615 ms. Each of the eight bursts, that form a TDMA frame, are then assigned to a single user.

3.4 Channel Structure

A channel corresponds to the recurrence of one burst every frame. It is defined by its frequency and the position of its corresponding burst within a TDMA frame. In GSM there are two types of channels:

- The traffic channels used to transport speech and data information.
- The control channels used for network management messages and some channel maintenance tasks.

Since radio spectrum is a limited resource shared by all users, a method must be devised to divide up the bandwidth among as many users as possible. The method chosen by GSM is a combination of Time- and Frequency-Division Multiple Access (TDMA/FDMA). The FDMA part involves the division by frequency of the (maximum) 25 MHz bandwidth into 124 carrier frequencies spaced 200 kHz apart. One or more carrier frequencies are assigned to each base station. Each of these carrier frequencies is then divided in time, using a TDMA scheme. The fundamental unit of time in this TDMA scheme is called a burst period and it lasts 15/26 ms (or approx. 0.577 ms). Eight burst periods are grouped into a TDMA frame (120/26 ms, or approx. 4.615 ms), which forms the basic unit for the definition of logical channels. One physical channel is one burst period per TDMA frame. The number and position of their corresponding burst periods define channels. All these definitions are cyclic, and the entire pattern repeats approximately every 3 hours. Channels can be divided into dedicated channels, which are allocated to a mobile station, and common channels, which are used by mobile stations in idle mode.

3.4.1 Traffic Channels

A traffic channel (TCH) is used to carry speech and data traffic. Traffic channels are defined using a 26-frame multi frame, or group of 26 TDMA frames. The length of a 26-frame multi frame is 120 ms, which is how the length of a burst period is defined (120 ms divided by 26 frames divided by 8 burst periods per frame). Out of the 26 frames, 24 are used for traffic, 1 is used for the Slow Associated Control Channel (SACCH) and 1 is currently unused (see Figure 3.1). TCHs for the uplink and downlink are separated in time by 3 burst periods, so that the mobile station does not have to transmit and receive simultaneously, thus simplifying the electronics. In addition to

these full-rate TCHs, there are also half-rate TCHs defined, although they are not yet implemented.

Half-rate TCHs will effectively double the capacity of a system once half-rate speech coders are specified (i.e., speech coding at around 7 kbps, instead of 13 kbps). Eighth-rate TCHs are also specified, and are used for signaling. In the recommendations, they are called Stand-alone Dedicated Control Channels (SDCCH). Full-rate traffic channels (TCH/F) are defined using a group of 26 TDMA frames called a 26-Multiframe. The 26-Multiframe lasts consequently 120 ms. In this 26-Multiframe structure; the traffic channels for the downlink and uplink are separated by 3 bursts. As a consequence, the mobiles will not need to transmit and receive at the same time, which simplifies considerably the electronics of the system. The frames that form the 26-Multiframe structure have different functions:

- 24 frames are reserved to traffic.
- 1 frame is used for the Slow Associated Control Channel (SACCH).
- The last frame is unused. This idle frame allows the mobile station to perform other functions, such as measuring the signal strength of neighboring cells.

Half-rate traffic channels (TCH/H), which double the capacity of the system, are also grouped in a 26-Multiframe but the internal structure is different.

3.4.2 Control Channels

According to their functions, four different classes of control channels are defined:

- Broadcast channels.
- Common control channels.
- Dedicated control channels.
- Associated control channels.

Common channels can be accessed both by idle mode and dedicated mode mobiles. Idle mode mobiles to exchange the signalling information required to change to dedicated mode use the common channels. Mobiles already in dedicated mode monitor the surrounding base stations for handover and other information. The common channels are defined within a 51-frame multiframe, so that dedicated mobiles using the 26-frame multiframe TCH structure can still monitor control channels. The common channels include:

a) Broadcast Control Channel (BCCH)

The base station, to provide the mobile station with the sufficient information it needs to synchronize with the network, uses the BCH channels. Three different types of BCHs can be distinguished:

- The Broadcast Control Channel (BCCH), which gives to the mobile station the parameters needed in order to identify and access the network.
- The Synchronization Channel (SCH), which gives to the mobile station the training sequence needed in order to demodulate the information transmitted by the base station.
- The Frequency-Correction Channel (FCCH), which supplies the mobile station with the frequency reference of the system in order to synchronize it with the network Continually broadcasts, on the downlink, information including base station identity, frequency allocations, and frequency-hopping sequences.

b) Common Control Channels (CCCH)

The CCCH channels help to establish the calls from the mobile station or the network. Three different types of CCCH can be defined:

- The Paging Channel (PCH). It is used to alert the mobile station of an incoming call.
- The Random Access Channel (RACH), which is used by the mobile station to request access to the network.
- The Access Grant Channel (AGCH). The base station, to inform the mobile station about which channel it should use, uses it. This channel is the answer of a base station to a RACH from the mobile station.

c) Frequency Correction Channel (FCCH) and Synchronization Channel (SCH)

Used to synchronize the mobile to the time slot structure of a cell by defining the boundaries of burst periods, and the time slot numbering. Every cell in a GSM network broadcasts exactly one FCCH and one SCH, which are by definition on time slot number 0 (within a TDMA frame).

d) Dedicated Control Channels (DCCH)

The DCCH channels are used for message exchange between several mobiles or a mobile and the network. Two different types of DCCH can be defined:

- The Standalone Dedicated Control Channel (SDCCH), which is used in order to exchange signaling information in the downlink and uplink directions.

- The Slow Associated Control Channel (SACCH). It is used for channel maintenance and channel control.

e) Associated Control Channels

The Fast Associated Control Channels (FACCH) replace all or part of a traffic channel when urgent signaling information must be transmitted. The FACCH channels carry the same information as the SDCCH channels.

f) Random Access Channel (RACH)

Slotted Aloha channel used by the mobile to request access to the network.

g) Paging Channel (PCH)

Used to alert the mobile station of an incoming call.

h) Access Grant Channel (AGCH)

Used to allocate an SDCCH to a mobile for signaling (in order to obtain a dedicated channel), following a request on the RACH.

3.4.3 Burst Structure

There are four different types of bursts used for transmission in GSM. The normal burst is used to carry data and most signaling. It has a total length of 156.25 bits, made up of two 57 bit information bits, a 26 bit training sequence used for equalization, 1 stealing bit for each information block (used for FACCH), 3 tail bits at each end, and an 8.25 bit guard sequence, as shown in Figure 3.1. The 156.25 bits are transmitted in 0.577 ms, giving a gross bit rate of 270.833 kbps. The F burst, used on the FCCH, and the S burst, used on the SCH, have the same length as a normal burst, but a different internal structure, which differentiates them from normal bursts (thus allowing synchronization). The access burst is shorter than the normal burst, and is used only on the RACH. As it has been stated before, the burst is the unit in time of a TDMA system. Four different types of bursts can be distinguished in GSM:

- The frequency-correction burst is used on the FCCH. It has the same length as the normal burst but a different structure.
- The synchronization burst is used on the SCH. It has the same length as the normal burst but a different structure.
- The random access burst is used on the RACH and is shorter than the normal burst.
- The normal burst is used to carry speech or data information. It lasts approximately 0.577 ms and has a length of 156.25 bits.

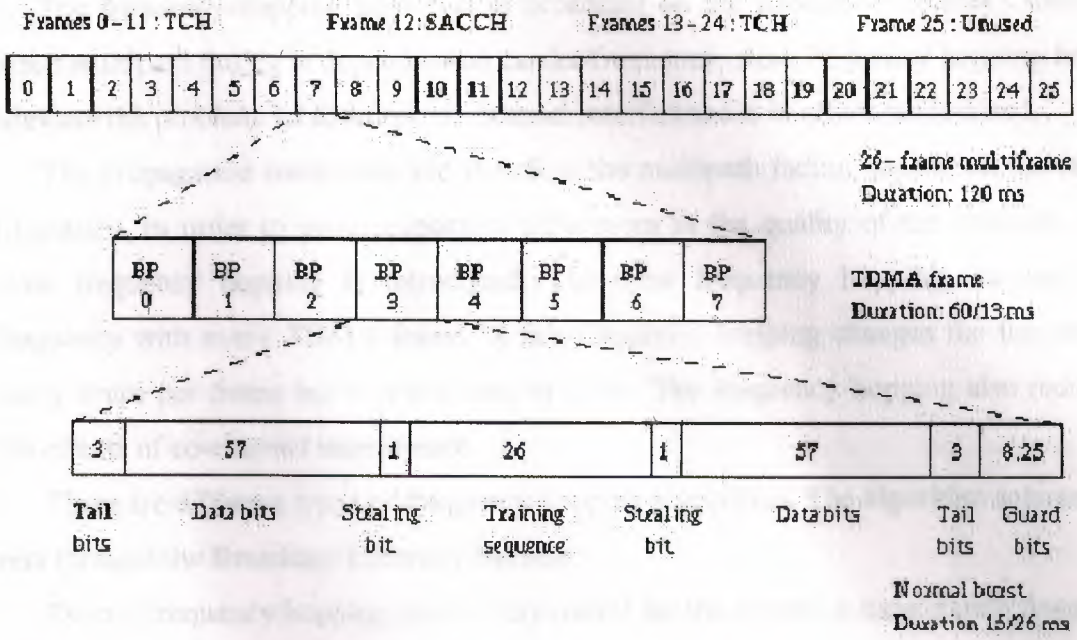


Figure 3.1 Structure of the 26-Multiframe, the TDMA frame and the normal burst

The tail bits (T) are a group of three bits set to zero and placed at the beginning and the end of a burst. They are used to cover the periods of ramping up and down of the mobile's power. The coded data bits correspond to two groups, of 57 bits each, containing signaling or user data.

The stealing flags (S) indicate, to the receiver, whether the information carried by a burst corresponds to traffic or signaling data. The training sequence has a length of 26 bits. It is used to synchronize the receiver with the incoming information, avoiding then the negative effects produced by a multipath propagation. The guard period (GP), with a length of 8.25 bits, is used to avoid a possible overlap of two mobiles during the ramping time.

3.4.4 Frequency Hopping

The mobile station already has to be frequency agile, meaning it can move between a transmit, receive, and monitor time slot within one TDMA frame, which normally are on different frequencies. GSM makes use of this inherent frequency agility to implement slow frequency hopping, where the mobile and BTS transmit each TDMA frame on a different carrier frequency.

The frequency-hopping algorithm is broadcast on the Broadcast Control Channel. Since multipath fading is dependent on carrier frequency, slow frequency hopping helps alleviate the problem. In addition, co-channel interference is in effect randomized.

The propagation conditions and therefore the multipath fading depend on the radio frequency. In order to avoid important differences in the quality of the channels, the slow frequency hopping is introduced. The slow frequency hopping changes the frequency with every TDMA frame. A fast frequency hopping changes the frequency many times per frame but it is not used in GSM. The frequency hopping also reduces the effects of co-channel interference.

There are different types of frequency hopping algorithms. The algorithm selected is sent through the Broadcast Control Channels.

Even if frequency hopping can be very useful for the system, a base station does not have to support it necessarily On the other hand, a mobile station has to accept frequency hopping when a base station decides to use it.

3.5 From Source Information to Radio Waves

The figure 3.2 presents the different operations that have to be performed in order to pass from the speech source to radio waves and vice versa. If the source of information is data and not speech, the speech coding will not be performed.

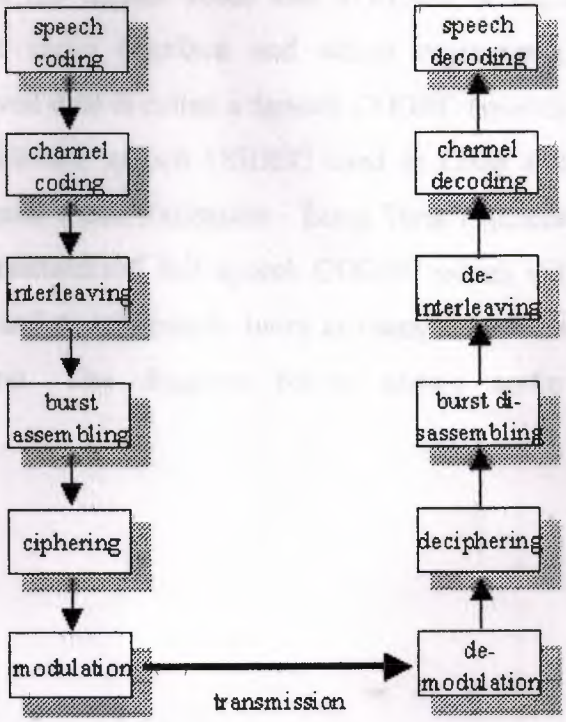


Figure 3.2 From speech source to radio waves

3.5.1 Speech Coding

The transmission of speech is, at the moment, the most important service of a mobile cellular system. The GSM speech coder, which will transform the analog signal (voice) into a digital representation, has to meet the following criterias:

- A good speech quality, at least as good as the one obtained with previous cellular systems.
- To reduce the redundancy in the sounds of the voice. This reduction is essential due to the limited capacity of transmission of a radio channel.
- The speech coder must not be very complex because complexity is equivalent to high costs.

The final choice for the GSM speech coder is a coder named RPE-LTP (Regular Pulse Excitation Long-Term Prediction). This coder uses the information from previous samples (this information does not change very quickly) in order to predict the current sample. The speech signal is divided into blocks of 20 ms. These blocks are then passed to the speech coder, which has a rate of 13 kbps, in order to obtain blocks of 260 bits. Obviously the most important aspect of the GSM Network is speech transmission. Although other services are now offered, voice telephony is still the most popular service available and hence generates the most revenue for the various companies. The device that transforms the human voice into a stream of digital data, suitable for transmission over the radio interface and which regenerates an audible analog representation of received data is called a Speech CODEC (speech transcoder or speech coder/decoder). The full-rate speech CODEC used in GSM is known as RPE-LTP, which stands for "Regular Pulse Excitation - Long Term Prediction". It is hoped there will eventually be a standardized full speech CODEC which will half the amount of data to be transmitted and so will enable twice as many customers to use the same slot in the TDMA frame. The diagram below shows audio signal processing

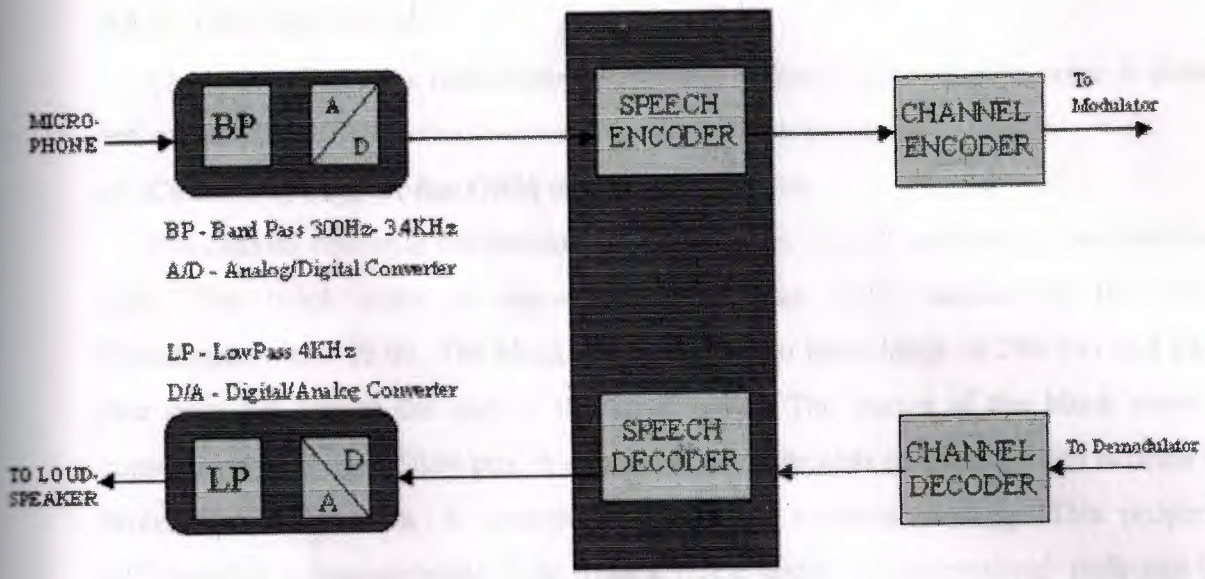


Figure 3.3 Audio Signal Processing

GSM is a digital system, so speech which is inherently analog, has to be digitized. The method employed by ISDN, and by current telephone systems for multiplexing voice lines over high-speed trunks and optical fiber lines, is Pulse Coded Modulation (PCM). The output stream from PCM is 64 kbps, too high a rate to be feasible over a radio link. The 64 kbps signal, although simple to implement, contains much redundancy. The GSM group studied several speech coding algorithms on the basis of subjective speech quality and complexity (which is related to cost, processing delay, and power consumption once implemented) before arriving at the choice of a Regular Pulse Excited Linear Predictive Coder (RPE-LPC) with a Long Term Predictor loop. Basically, information from previous samples, which does not change.

Very quickly, is used to predict the current sample. The coefficients of the linear combination of the previous samples, plus an encoded form of the residual, the difference between the predicted and actual sample, represent the signal. Speech is divided into 20 millisecond samples, each of which is encoded as 260 bits, giving a total bit rate of 13 kbps. This is the so-called Full-Rate speech coding. Recently, some North American GSM1900 operators have implemented an Enhanced Full-Rate (EFR) speech-coding algorithm. This is said to provide improved speech quality using the existing 13 kbps bit rate.

3.5.2 Channel coding

Channel coding adds redundancy bits to the original information in order to detect and correct, if possible, errors occurred during the transmission.

a) Channel coding for the GSM data TCH channels

The channel coding is performed using two codes: a block code and a convolutional code. The block code corresponds to the block code defined in the GSM Recommendations 05.03. The block code receives an input block of 240 bits and adds four zero tail bits at the end of the input block. The output of the block code is consequently a block of 244 bits. A convolutional code adds redundancy bits in order to protect the information. A convolutional encoder contains memory. This property differentiates a convolutional code from a block code. A convolutional code can be defined by three variables: n, k and K. The value n corresponds to the number of bits at the output of the encoder, k to the number of bits at the input of the block and K to the memory of the encoder. The ratio, R, of the code is defined as follows: R = k/n. Let's consider a convolutional code with the following values: k is equal to 1, n to 2 and K to 5. This convolutional code uses then a rate of R = 1/2 and a delay of K = 5, which

Means that it will add a redundant bit for each input bit. The convolutional code uses 5 consecutive bits in order to compute the redundancy bit. As the convolutional code is a 1/2 rate convolutional code, a block of 488 bits is generated. These 488 bits are punctured in order to produce a block of 456 bits. Thirty-two bits, obtained as follows, are not transmitted:

$$C\,(11 + 15\,j) \text{ for } j = 0, 1, \ldots, 31$$

The block of 456 bits produced by the convolutional code is then passed to the interleaver.

b) Channel coding for the GSM speech channels

Before applying the channel coding, the 260 bits of a GSM speech frame are divided in three different classes according to their function and importance. The most important class is the class Ia containing 50 bits. Next in importance is the class Ib, which contains 132 bits. The least important is the class II, which contains the remaining 78 bits. The different classes are coded differently. First of all, the class Ia bits are block-coded. Three parity bits, used for error detection, are added to the 50 class Ia bits. The resultant 53 bits are added to the class Ib bits. Four zero bits are added to this block of 185 bits (50+3+132). A convolutional code, with r = 1/2 and K = 5, is then

applied, obtaining an output block of 378 bits. The class II bits are added, without any protection, to the output block of the convolutional coder. An output block of 456 bits is finally obtained.

c) Channel coding for the GSM control channels

In GSM the signaling information is just contained in 184 bits. Forty parity bits, obtained using a fire code, and four zero bits are added to the 184 bits before applying the convolutional code (r = 1/2 and K = 5). The output of the convolutional code is then a block of 456 bits, which does not need to be punctured.

Electromagnetic interference can disrupt encoded speech and data transmitted over the GSM Network. Because of this this complicated encoding and block interleaving is used to protect the Network. Speech and data rates use different algorithms. Radio emissions too can cause interference if they occur outside of the allotted bandwidth and must be strictly controlled to allow for both GSM and older analog systems to co-exist. Because of natural and man-made electromagnetic interference, the encoded speech or data signal transmitted over the radio interface must be protected from errors. GSM uses convolutional encoding and block interleaving to achieve this protection. The exact algorithms used differ for speech and for different data rates. The method used for speech blocks will be described below. Recall that the speech coder produces a 260-bit block for every 20 ms speech sample. From subjective testing, it was found that some bits of this block were more important for perceived speech quality than others. The bits are thus divided into three classes:

- **Class Ia** 50 bits - most sensitive to bit errors.
- **Class Ib** 132 bits - moderately sensitive to bit errors.
- **Class II** 78 bits - least sensitive to bit errors.

Class Ia bits have a 3 bit Cyclic Redundancy Code added for error detection. If an error is detected, the frame is judged too damaged to be comprehensible and it is discarded. It is replaced by a slightly attenuated version of the previous correctly received frame. These 53 bits, together with the 132 Class Ib bits and a 4-bit tail sequence (a total of 189 bits), are input into a 1/2 rate convolutional encoder of constraint length 4. Each input bit is encoded as two output bits, based on a combination of the previous 4 input bits. The convolutional encoder thus outputs 378 bits, to which are added the 78 remaining Class II bits, which are unprotected. Thus every 20 ms speech sample is encoded as 456 bits, giving a bit rate of 22.8 kbps. To further protect

against the burst errors common to the radio interface, each sample is interleaved. The 456 bits output by the convolutional encoder are divided into 8 blocks of 57 bits, and these blocks are transmitted in eight consecutive time-slot bursts. Since each time-slot burst can carry two 57-bit blocks, each burst carries traffic from two different speech samples. Recall that each time-slot burst is transmitted at a gross bit rate of 270.833 kbps. This digital signal is modulated onto the analog carrier frequency using Gaussian-filtered Minimum Shift Keying (GMSK). GMSK was selected over other modulation schemes as a compromise between spectral efficiency, complexity of the transmitter, and limited spurious emissions. The complexity of the transmitter is related to power consumption, which should be minimized for the mobile station. The spurious radio emissions, outside of the allotted bandwidth, must be strictly controlled so as to limit adjacent channel interference, and allow for the co-existence of GSM and the older analog systems (at least for the time being).

3.5.3 Interleaving

An interleaving rearranges a group of bits in a particular way. It is used in combination with FEC codes in order to improve the performance of the error correction mechanisms. The interleaving decreases the possibility of losing whole bursts during the transmission, by dispersing the errors. Being the errors less concentrated, it is then easier to correct them.

a) Interleaving for the GSM control channels

A burst in GSM transmits two blocks of 57 data bits each. Therefore the 456 bits corresponding to the output of the channel coder fit into four bursts (4x114 = 456). The 456 bits are divided into eight blocks of 57 bits. The first block of 57 bits contains the bit numbers (0, 8, 16,....., 448), the second one the bit numbers (1, 9, 17, ...,449), etc. The last block of 57 bits will then contain the bit numbers (7, 15,....., 455). The first four blocks of 57 bits are placed in the even-numbered bits of four bursts. The other four blocks of 57 bits are placed in the odd-numbered bits of the same four bursts. Therefore the interleaving depth of the GSM interleaving for control channels is four and a new data block starts every four bursts. The interleaver for control channels is called a block rectangular interleaver.

b) Interleaving for the GSM speech Channels

The block of 456 bits, obtained after the channel coding, is then divided in eight blocks of 57 bits in the same way as it is explained in the previous paragraph. But these

eight blocks of 57 bits are distributed differently. The first four blocks of 57 bits are placed in the even-numbered bits of four consecutive bursts. The other four blocks of 57 bits are placed in the odd-numbered bits of the next four bursts.

The interleaving depth of the GSM interleaving for speech channels is then eight. A new data block also starts every four bursts. The interleaver for speech channels is called a block diagonal interleaver.

c) Interleaving for the GSM data TCH channels

A particular interleaving scheme, with an interleaving depth equal to 22, is applied to the block of 456 bits obtained after the channel coding. The block is divided into 16 blocks of 24 bits each, 2 blocks of 18 bits each, 2 blocks of 12 bits each and 2 blocks of 6 bits each. It is spread over 22 bursts in the following way:

- The first and the twenty-second bursts carry one block of 6 bits each.
- The second and the twenty-first bursts carry one block of 12 bits each.
- The third and the twentieth bursts carry one block of 18 bits each.
- From the fourth to the nineteenth burst, a block of 24 bits is placed in each burst.

A burst will then carry information from five or six consecutive data blocks. The data blocks are said to be interleaved diagonally. A new data block starts every four bursts.

3.5.4 Burst Assembling

The burst assembling procedure is in charge of grouping the bits into bursts. Section 3.4.3. presents the different bursts structures and describes in detail the structure of the normal burst.

3.5.5 Ciphering

Ciphering is used to protect signaling and user data. First of all, a ciphering key is computed using the algorithm A8 stored on the SIM card, the subscriber key and a random number delivered by the network (this random number is the same as the one used for the authentication procedure). Secondly, a 114-bit sequence is produced using the ciphering key, an algorithm called A5 and the burst numbers. This bit sequence is then XORed with the two 57 bit blocks of data included in a normal burst. In order to decipher correctly, the receiver has to use the same algorithm A5 for the deciphering procedure.

3.5.6 Modulation

The modulation chosen for the GSM system is the Gaussian Minimum Shift Keying (GMSK). The aim of this section is not to describe precisely the GMSK modulation as it is too long and it implies the presentation of too many mathematical concepts. Therefore, only brief aspects of the GMSK modulation are presented in this section. The GMSK modulation has been chosen as a compromise between spectrum efficiency, complexity and low spurious radiations (that reduce the possibilities of adjacent channel interference). The GMSK modulation has a rate of 270 5/6 kbauds and a BT product equal to 0.3. Figure 3.4. presents the principle of a GMSK modulator.

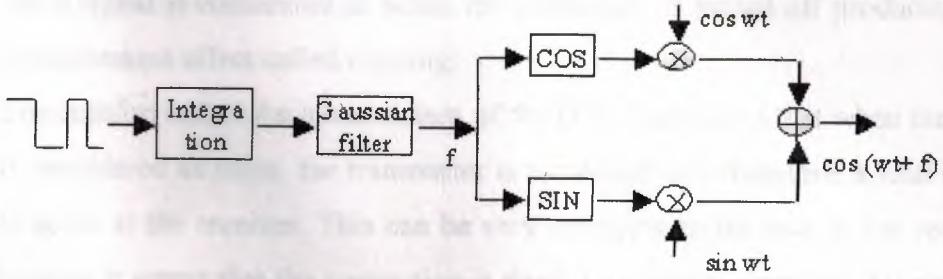


Figure 3.4 GMSK Modulator

3.6 Discontinuous Transmission (Dtx)

Minimizing co-channel interference is a goal in any cellular system, since it allows better service for a given cell size, or the use of smaller cells, thus increasing the overall capacity of the system. Discontinuous transmission (DTX) is a method that takes advantage of the fact that a person speaks less that 40 percent of the time in normal conversation, by turning the transmitter off during silence periods. An added benefit of DTX is that power is conserved at the mobile unit. The most important component of DTX is, of course, Voice Activity Detection. It must distinguish between voice and noise inputs, a task that is not as trivial as it appears, considering background noise. If a voice signal is misinterpreted as noise, the transmitter is turned off and a very annoying effect called clipping is heard at the receiving end. If, on the other hand, noise is misinterpreted as a voice signal too often, the efficiency of DTX is dramatically decreased. Another factor to consider is that when the transmitter is turned off, there is total silence heard at the receiving end, due to the digital nature of GSM. To assure the receiver that the connection is not dead, comfort noise is created at the receiving end by trying to match the characteristics of the transmitting end's background noise. This is

another aspect of GSM that could have been included as one of the requirements of the GSM speech coder. The function of the DTX is to suspend the radio transmission during the silence periods. This can become quite interesting if we take into consideration the fact that a person speaks less than 40 or 50 percent during a conversation. The DTX helps then to reduce interference between different cells and to increase the capacity of the system. It also extends the life of a mobile's battery. The DTX function is performed thanks to two main features:

- The Voice Activity Detection (VAD), which has to determine whether the sound represents speech or noise, even if the background noise is very important. If the voice signal is considered as noise, the transmitter is turned off producing then, an unpleasant effect called clipping.
- The comfort noise. An inconvenient of the DTX function is that when the signal is considered as noise, the transmitter is turned off and therefore, a total silence is heard at the receiver. This can be very annoying to the user at the reception because it seems that the connection is dead. In order to overcome this problem, the receiver creates a minimum of background noise called comfort noise. The comfort noise eliminates the impression that the connection is dead.

3.7 Timing Advance

The timing of the bursts transmissions is very important. Mobiles are at different distances from the base stations. Their delay depends, consequently, on their distance. The aim of the timing advance is that the signals coming from the different mobile stations arrive to the base station at the right time. The base station measures the timing delay of the mobile stations. If the bursts corresponding to a mobile station arrive too late and overlap with other bursts, the base station tells, this mobile, to advance the transmission of its bursts.

3.8 Power Control

There are five classes of mobile stations defined, according to their peak transmitter power, rated at 20, 8, 5, 2, and 0.8 watts. To minimize co-channel interference and to conserve power, both the mobiles and the Base Transceiver Stations operate at the lowest power level that will maintain an acceptable signal quality. Power levels can be stepped up or down in steps of 2 dB from the peak power for the class down to a minimum of 13 dBm (20 milli watts). The mobile station measures the signal strength

or signal quality (based on the Bit Error Ratio), and passes the information to the Base Station Controller, which ultimately decides if and when the power level should be changed. Power control should be handled carefully, since there is the possibility of instability. This arises from having mobiles in co-channel cells alternatingly increase their power in response to increased co-channel interference caused by the other mobile increasing its power. This in unlikely to occur in practice but it is (or was as of 1991) under study. At the same time the base stations perform the timing measurements, they also perform measurements on the power level of the different mobile stations. These power levels are adjusted so that the power is nearly the same for each burst. A base station also controls its power level. The mobile station measures the strength and the quality of the signal between itself and the base station. If the mobile station does not receive correctly the signal, the base station changes its power level.

3.9 Discontinuous Reception

Another method used to conserve power at the mobile station is discontinuous reception. The paging channel, used by the base station to signal an incoming call, is structured into sub-channels. Each mobile station needs to listen only to its own sub-channel. In the time between successive paging sub-channels, the mobile can go into sleep mode, when almost no power is used. It is a method used to conserve the mobile station's power. The paging channel is divided into sub channels corresponding to single mobile stations. Each mobile station will then only 'listen' to its sub channel and will stay in the sleep mode during the other sub channels of the paging channel.

3.10 Multipath and Equalization

At the GSM frequency bands, radio waves reflect from buildings, cars, hills, etc. So not only the 'right' signal (the output signal of the emitter) is received by an antenna, but also many reflected signals, which corrupt the information, with different phases. An equalizer is in charge of extracting the 'right' signal from the received signal. It estimates the channel impulse response of the GSM system and then constructs an inverse filter. The receiver knows which training sequence it must wait for. The equalizer will then, comparing the received training sequence with the training sequence it was expecting, compute the coefficients of the channel impulse response. In order to extract the 'right' signal, the received signal is passed through the inverse filter. At the 900 MHz range, radio waves bounce off everything - buildings, hills, cars, airplanes,

etc. Thus many reflected signals, each with a different phase, can reach an antenna. Equalization is used to extract the desired signal from the unwanted reflections. It works by finding out how a known transmitted signal is modified by multipath fading, and constructing an inverse filter to extract the rest of the desired signal. This known signal is the 26-bit training sequence transmitted in the middle of every time-slot burst. The actual implementation of the equalizer is not specified in the GSM specifications.

4. GSM ARCHITECTURE

4.1 Overview

The increasing demand for data services leads to the internet growing and the World Wide Web has grown from 130 mostly educational sites in mid-1993 to 650,000 largely commercial sites at the beginning of 1997. There are now estimated to be well in excess of 50 million individual subscribers with Internet access. This development can be divided into two periods. First generation wireless networks evolve from specialized proprietary protocols or national standards. Wireless voice and data networks operate independently or, at best, are loosely coupled. Over the last decade a second-generation fully digital mobile communication network, now called the Global System for Mobil communications (GSM), with integrated voice and data capabilities has been created and deployed. GSM has three spectral variants: GSM 900, DCS1800 and PCS 1900 operating respectively in the 900MHz, 1.8 GHz and 1.9 GHz bands. GSM has matured to be adopted by around 200 operators in 100 countries. The success of GSM has produced a market led evolution. The GSM system was originally deployed in phase 1 as a basic voice and circuit data service and then additional supplementary services were added in the pre-planned phase 2. GSM is now in "phase 2+", which allows for the ongoing introduction of new services and which should eventually migrate to a third generation system known as the Universal Mobile Telecommunications System (UMTS). A rich collection of new data services is currently being defined under phase 2+. These services when combined with existing data services will provide greater choices and improved bandwidth. The GSM system architecture consists of three major interconnected subsystems that interact between themselves and with the users through certain network interfaces. The subsystems are the Base Station Subsystem (BSS), Network and Switching Subsystem (NSS), and the Operation Support subsystem (OSS). The Mobile Station (MS) is also a subsystem, but is usually considered to be part of the BSS for architecture purposes. Equipment and services are designed within GSM to support one or more of these specific subsystems.

- The BSS provides and manages radio transmission paths between the mobile stations and the Mobile Switching Center (MSC). It also manages the radio

interface. Each BSS consists of many Base Station Controllers (BSCs) which connect the MS to the NSS via the MSCs.

- The NSS manages the switching functions of the system and allows the MSCs to communicate with other networks such as the PSTN and ISDN.
- The OSS supports the operation and maintenance of GSM and allows system engineers to monitor, diagnose, and troubleshoot all aspects of the GSM system. This subsystem interacts with the other GSM subsystems, and is provided solely for the staff of the GSM operating company, which provides service facilities for the network.

One goal of the GSM is to achieve separation between the NSS and BSS, so that other wireless technologies could be used, such as digital enhanced cordless telecommunications (DECT) and the satellite systems. The GSM air interface between the mobile stations and other subsystems of GSM combines both time division multiple access (TDMA) and frequency division multiple access (FDMA) with optional frequency hopping.

4.2 Architecture Of The GSM Network

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 4.1

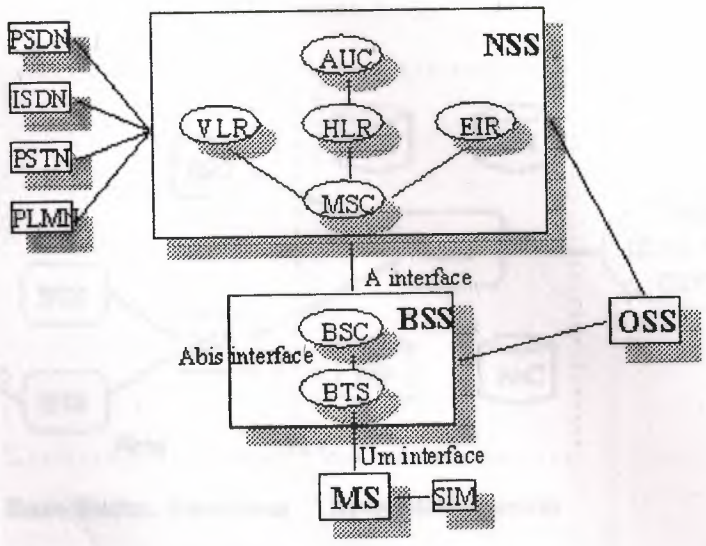


Figure 4.1 Architecture of the GSM network

A GSM network is composed of several functional entities, whose functions and interfaces are specified. Figure 4.1 shows the layout of a generic GSM network. The GSM network can be divided into three broad parts. The subscriber carries the Mobile Station. The Base Station Subsystem controls the radio link with the Mobile Station. The Network Subsystem, the main part of which is the Mobile services Switching Center (MSC), performs the switching of calls between the mobile users, and between mobile and fixed network users. The MSC also handles the mobility management operations. Not shown is the Operations and Maintenance Center, which oversees the proper operation and setup of the network. The Mobile Station and the Base Station Subsystem communicate across the U_m interface, also known as the air interface or radio link. The Base Station Subsystem communicates with the Mobile Services Switching Center across the A interface. GSM provides recommendations, not requirements. The GSM specifications define the functions and interface requirements.

In detail but do not address the hardware. The reason for this is to limit the designers as little as possible but still to make it possible for the operators to buy equipment from different suppliers. The GSM network is divided into three major systems: the switching system (SS), the base station system (BSS), and the operation and support system (OSS). The basic GSM network elements are shown in Figure 4.2

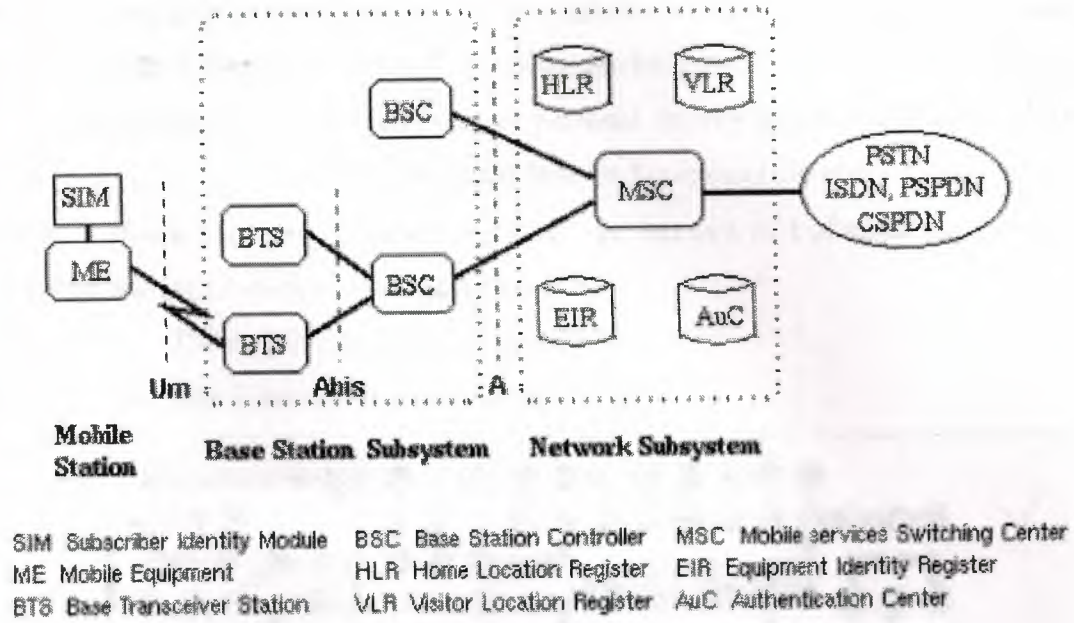


Figure 4.2 General architecture of a GSM network

4.2.1 Mobile Station

The mobile station (MS) consists of the mobile equipment (the terminal) and a smart card called the Subscriber Identity Module (SIM). The SIM provides personal mobility, so that the user can have access to subscribed services irrespective of a specific terminal. By inserting the SIM card into another GSM terminal, the user is able to receive calls at that terminal, make calls from that terminal, and receive other subscribed services.

The International Mobile Equipment Identity (IMEI) uniquely identifies the mobile equipment. The SIM card contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication, and other information.

The IMEI and the IMSI are independent, thereby allowing personal mobility. The SIM card may be protected against unauthorized use by a password or personal identity number.

The mobile station is the formal name for what represents, for most people, their actual cell-phone and a smart card called the Subscriber Identity Module (SIM). Other examples of mobile stations are car-phones and transportable units.

The SIM card can be regarded as separate from the actual terminal as a user can insert the card into another terminal, receive calls from there, and reap the full access of other subscribed services. The SIM card provides for greater security and renders theft futile as it may contain a user password or personal identity number. The terminal itself is uniquely identified by the International Mobile Equipment Identity (IMEI), which is similar in idea as the unique number a printer, say, has as a part of a computer network. A Mobile Station consists of two main elements:

- The mobile equipment or terminal.
- The Subscriber Identity Module (SIM).

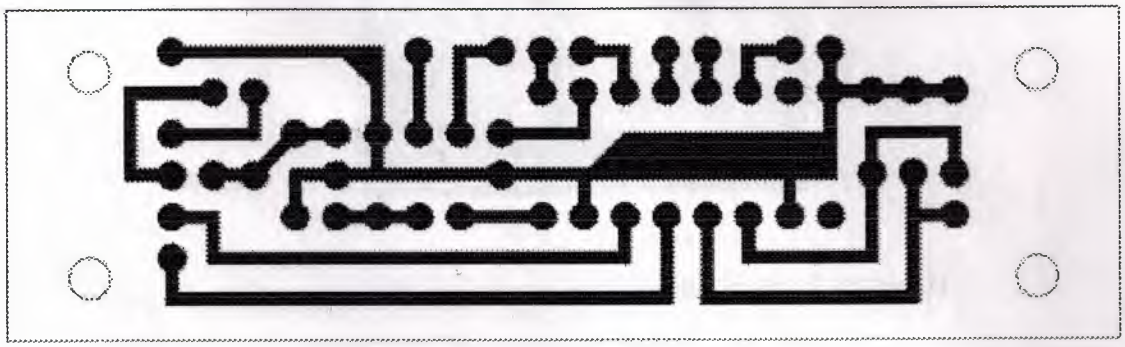


Figure 4.3 Mobile equipment (internal board)

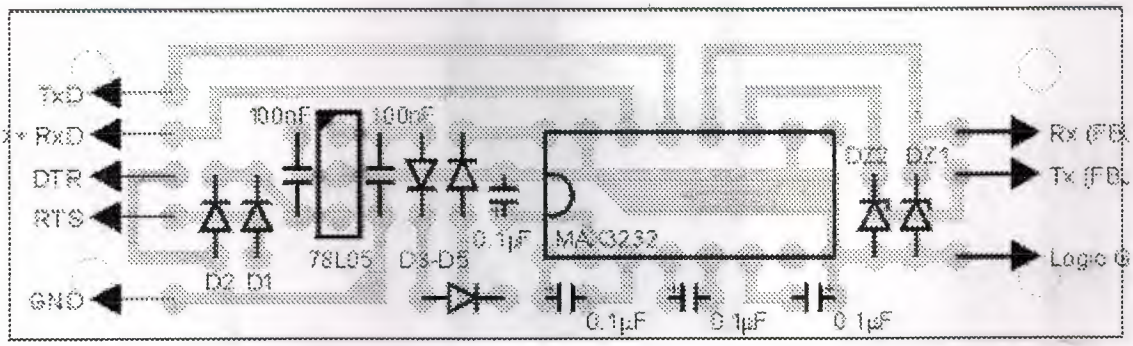


Figure 4.4 Mobile equipment (conn. cct)

a) The Terminal

There are different types of terminals distinguished principally by their power and application:

- The `fixed' terminals are the ones installed in cars. Their maximum allowed output power is 20 W.
- The GSM portable terminals can also be installed in vehicles. Their maximum allowed output power is 8W.

- The handhels terminals have experienced the biggest success thanks to thei weight and volume, which are continuously decreasing. These terminals can emit up to 2 W. The evolution of technologies allows to decrease the maximum allowed power to 0.8 W.

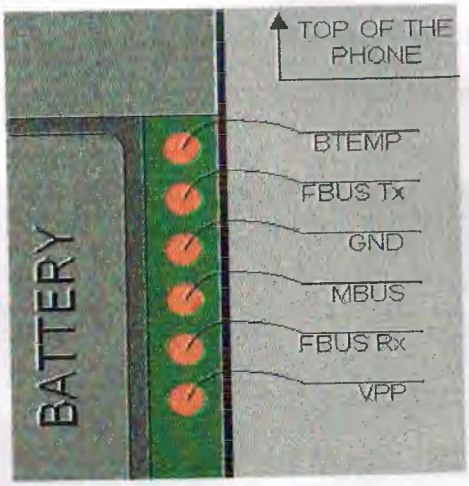


Figure 4.5 Mobile phone equipment (internal terminal)

Figure 4.6 Front view terminal

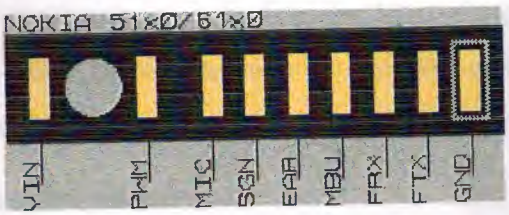


Figure 4.7 Side view terminal

b) The SIM

The SIM is a smart card that identifies the terminal. By inserting the SIM card into the terminal, the user can have access to all the subscribed services. Without the SIM card, the terminal is not operational. A four-digit Personal Identification Number (PIN) protects the SIM card. In order to identify the subscriber to the system, the SIM card contains some parameters of the user such as its International Mobile Subscriber

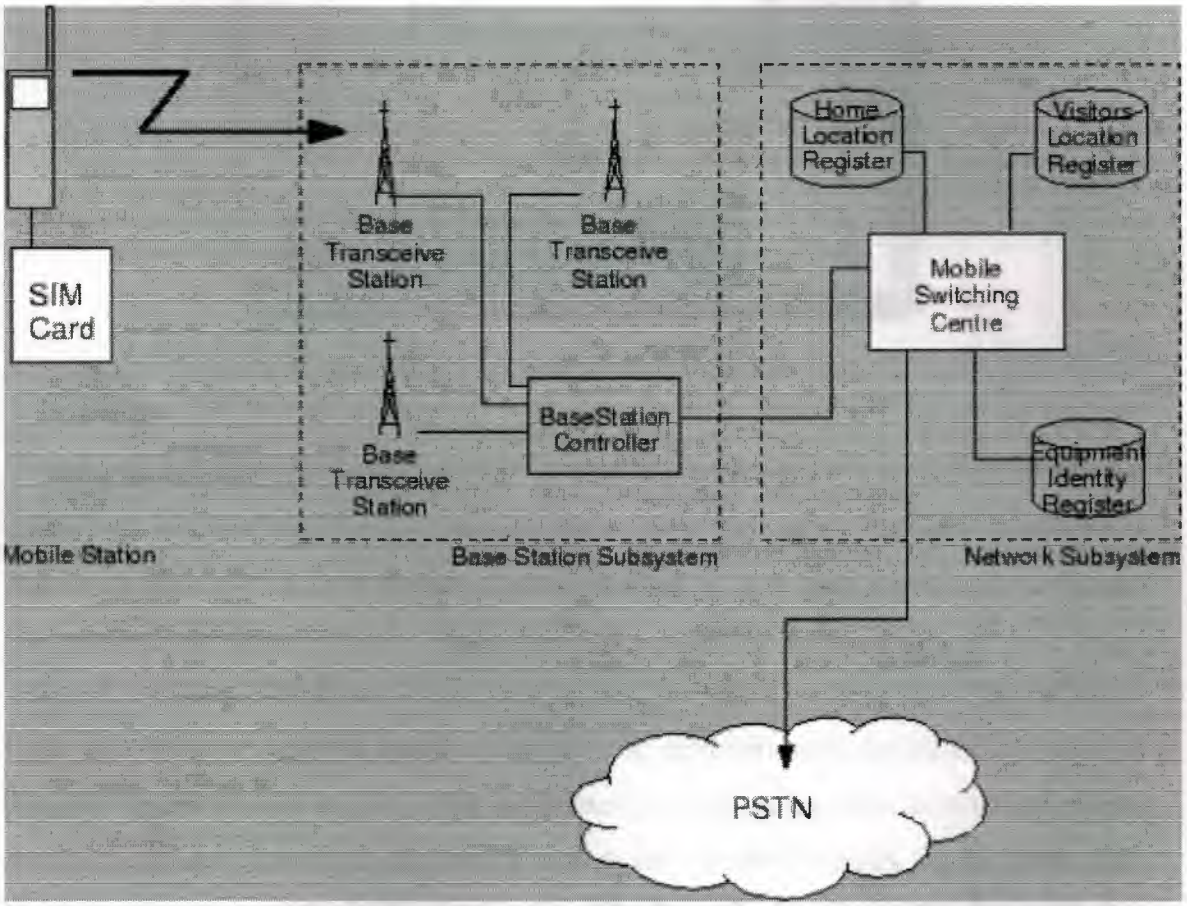


Figure 4.8 Overview of a GSM Mobile Network

Identity (IMSI). Another advantage of the SIM card is the mobility of the users. In fact, the only element that personalizes a terminal is the SIM card. Therefore, the user can have access to its subscribed services in any terminal using its SIM card.

4.2.2 The Base Station Subsystem

The Base Station Subsystem is composed of two parts, the Base Transceiver Station (BTS) and the Base Station Controller (BSC). These communicate across the

standardized Abis interface, allowing (as in the rest of the system) operation between components made by different suppliers.

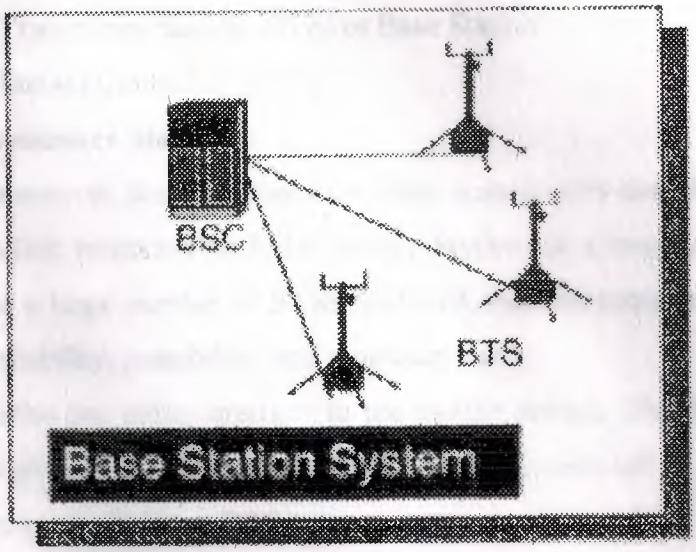


Figure 4.9 Base Station System

When a call is made from a mobile, the terminal searches for a local base station to connect to. A Base Station Sub-system is made up of two parts – the Base Transceiver Station (BTS) and the Base Station Controller (BSC). They both communicate across the standardized Abis interface, which allows a network to be composed of parts from different suppliers. The Base-Transceiver Stations provide for one or more channels per radio cell. Its main job is to handle the radio-link protocols with the Mobile Station. It provides the two lowest layers of the radio interface, and so provides an error-corrected data path. At least one of the channels is used to carry control signals, which insure that the data arrives correctly at the destination. The Base Station Controller manages the radio resources for one or more BTSs and operates within a particular region. Its main functions are to handle radio-channel setup, control frequency hopping, undertake handovers (except to cells outside its region) and provide radio performance measurements. The BSC is the connection between the mobile station and the Mobile Services Switching Center (MSC). Once the mobile has been successfully connected to a BTS, the BSC will set up a bi-directional signaling channel specifically for itself and it will connect it on to the MSC. All radio-related functions are performed in the BSS, which consists of base station controllers (BSCs) and the base transceiver stations (BTSs).

The BSS connects the Mobile Station and the NSS. It is in charge of the transmission and reception.

The BSS can be divided into two parts:

- The Base Transceiver Station (BTS) or Base Station.
- The Base Station Controller (BSC).

a) The Base Transceiver Station

The Base Transceiver Station houses the radio transceivers that define a cell and handles the radio-link protocols with the Mobile Station. In a large urban area, there will potentially be a large number of BTSs deployed, thus the requirements for a BTS are ruggedness, reliability, portability, and minimum cost.

The BTS handles the radio interface to the mobile station. The BTS is the radio equipment (transceivers and antennas) needed to service each cell in the network. A group of BTSs are controlled by a BSC.

The BTS corresponds to the transceivers and antennas used in each cell of the network. A BTS is usually placed in the center of a cell. Its transmitting power defines the size of a cell. Each BTS has between one and sixteen transceivers depending on the density of users in the cell.

b) The Base Station Controller

The Base Station Controller manages the radio resources for one or more BTSs. It handles radio-channel setup, frequency hopping, and handovers, as described below. The BSC is the connection between the mobile station and the Mobile service Switching Center (MSC).

The BSC also translates the 13 kbps voice channel used over the radio link to the standard 64 kbps channel used by the Public Switched Telephone Network or ISDN.

The BSC provides all the control functions and physical links between the MSC and BTS. It is a high-capacity switch that provides functions such as handover, cell configuration data, and control of radio frequency (RF) power levels in base transceiver stations. A number of BSCs are served by an MSC.

The BSC controls a group of BTS and manages their radio resources. A BSC is principally in charge of handovers, frequency hopping, exchange functions and control of the radio frequency power levels of the BTSs.

4.2.3 The Network and Switching Subsystem

The central component of the Network Subsystem is the Mobile services Switching Center (MSC). It acts like a normal switching node of the PSTN or ISDN, and additionally provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber. These services are provided in conjunction with several functional entities, which together form the Network Subsystem. The MSC provides the connection to the fixed networks (such as the PSTN or ISDN). Signaling between functional entities in the Network Subsystem uses Signaling System Number 7 (SS7), used for trunk signaling in ISDN and widely used in current public networks.

The Home Location Register (HLR) and Visitor Location Register (VLR), together with the MSC, provide the call-routing and roaming capabilities of GSM. The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network, along with the current location of the mobile. The location of the mobile is typically in the form of the signaling address of the VLR associated with the mobile station. The actual routing procedure will be described later. There is logically one HLR per GSM network, although it may be implemented as a distributed database.

The Visitor Location Register (VLR) contains selected administrative information from the HLR, necessary for call control and provision of the subscribed services, for each mobile currently located in the geographical area controlled by the VLR. Although each functional entity can be implemented as an independent unit, all manufacturers of switching equipment to date implement the VLR together with the MSC, so that the geographical area controlled by the MSC corresponds to that controlled by the VLR, thus simplifying the signaling required. Note that the MSC contains no information about particular mobile stations; this information is stored in the location registers.

The other two registers are used for authentication and security purposes. The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where its International Mobile Equipment Identity (IMEI) identifies each mobile station. An IMEI is marked as invalid if it has been reported stolen or is not type approved. The Authentication Center (AuC) is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and encryption over the radio channel.

The NSS handles the switching of GSM calls between external networks and the BSCs in the radio subsystem and is also responsible for managing and providing external access to several customer databases. The MSC is the central unit in the NSS and controls the traffic among all of the BSCs. In the NSS, there are three different databases called the Home Location Register (HLR), Visitor Location Register (VLR), and the Authentication Center (AuC). The HLR is a database, which contains subscriber information and location information for each user who resides in the same city as the MSC. Each subscriber in a particular GSM market is assigned a unique International Mobil Subscriber Identity (IMSI), and this number is used to identify each home user. The VLR is a database, which temporarily stores the IMSI and customer information for each roaming subscriber who is visiting the coverage area of a particular MSC. The Authentication Center is a strongly protected database, which handles the authentication and encryption keys for every single subscriber in the HLR and VLR. The OSS supports one or several Operation Maintenance Centers (OMC), which are used to monitor and maintain the performance of each MS, BS, BSC, and MSC within a GSM system. The switching system (SS) is responsible for performing call processing and subscriber-related functions. The switching system includes the following functional units. The main component of the Network Subsystem is the Mobile services Switching Center (MSC). It is made up of a usual trunk ISDN exchange but additionally provides all the functionality needed to handle a mobile user such as registration, authentification, checking the whereabouts of the user, handovers and call routing. The MSC provides the connection to the fixed networks, such as PSTN or ISDN. The Home Location Register (HLR) and the Visitor Location Register (VLR) handle call routing and roaming. There is more information on Roaming in the GSM Network as a separate project on this ICT site.

The HLR contains all the necessary information about the user and the current location of the mobile. This location is usually in the form of the signaling address of the VLR associated with the mobile station. The Equipment Identity Register (EIR) contains a list of all the mobile equipment (identified by their IMEI) on the network. Authentification: If the mobile user attempts to access the system, it is asked for its International Mobile Subscriber Identity (IMSI). This unique number is checked and validated by the system.

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.

a) The Mobile services Switching Center (MSC)

The MSC performs the telephony switching functions of the system. It controls calls to and from other telephone and data systems. It also performs such functions as toll ticketing, network interfacing, common channel signaling, and others

It is the central component of the NSS. The MSC performs the switching functions of the network. It also provides connection to other networks.

b) The Gateway Mobile services Switching Center (GMSC)

A gateway is a node interconnecting two networks. The GMSC is the interface between the mobile 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.

c) Home Location Register (HLR)

The HLR is a database used for storage and management of subscriptions. The HLR is considered the most important database, as it stores permanent data about subscribers, including a subscriber's service profile, location information, and activity status. When an individual buys a subscription from one of the PCS operators, he or she is registered

in the HLR of that operator. The HLR is considered as a very important database that stores information of the subscribers belonging to the covering 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 corresponds to the SS7 address of the Visitor Location Register (VLR) associated to the terminal.

d) Visitor Location Register (VLR)

The VLR is a database that contains temporary information about subscribers that is needed by the MSC in order to service visiting subscribers. The VLR is always integrated with the MSC. When a mobile station roams into a new MSC area, the VLR connected to that MSC will request data about the mobile station from the HLR. Later, if the mobile station makes a call, the VLR will have the information needed for call setup without having to interrogate the HLR each time.

The VLR contains information from a subscriber's HLR necessary in order 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 information

in order 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; so the area under control of the MSC is also the area under control of the VLR.

e) The Authentication Center (AuC)

A unit called the AuC provides authentication and encryption parameters that verify the user's identity and ensure the confidentiality of each call. The AuC protects network operators from different types of fraud found in today's cellular world.

The Authentification Center (AuC) is the network sub-system register, which contains all the password numbers in the customer's SIM card, which is used for authentification and security over the network. One of the main reasons why cell-phones can be so small and still have enough power to remain on standby for so long is that they use a receiving method known as Discontinuous Receive (DRX). This allows the mobile to only listen to paging signals when they are emitted by a known paging cycle of the network. The phones are not continuously checking for signals and use one tenth of the power requirements they would need therefore.

The AuC register is used for security purposes. It provides the parameters needed for authentication and encryption functions. These parameters help to verify the user's identity.

f) The Equipment Identity Register (EIR)

The EIR is a database that contains information about the identity of mobile equipment that prevents calls from stolen, unauthorized, or defective mobile stations. The AUC and EIR are implemented as stand-alone nodes or as a combined AUC/EIR node.

The EIR is also used for security purposes. It is a register containing information about the mobile equipments. More particularly, it contains a list of all valid terminals. Its International Mobile Equipment Identity (IMEI) identifies a terminal. 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).

g) The GSM Interworking Unit (GIWU)

The GIWU consists of both hardware and software that provides an interface to various networks for data communications. Through the GIWU, users can alternate between speech and data during the same call. The GIWU hardware equipment is physically located at the MSC/VLR.

The GIWU corresponds to an interface to various networks for data communications. During these communications, the transmission of speech and data can be alternated.

h) Message center (MXE)

The MXE is a node that provides integrated voice, fax, and data messaging. Specifically, the MXE handles short message service, cell broadcast, voice mail, fax mail, e-mail, and notification.

i) Mobile service node (MSN)

The MSN is the node that handles the mobile intelligent network (IN) services.

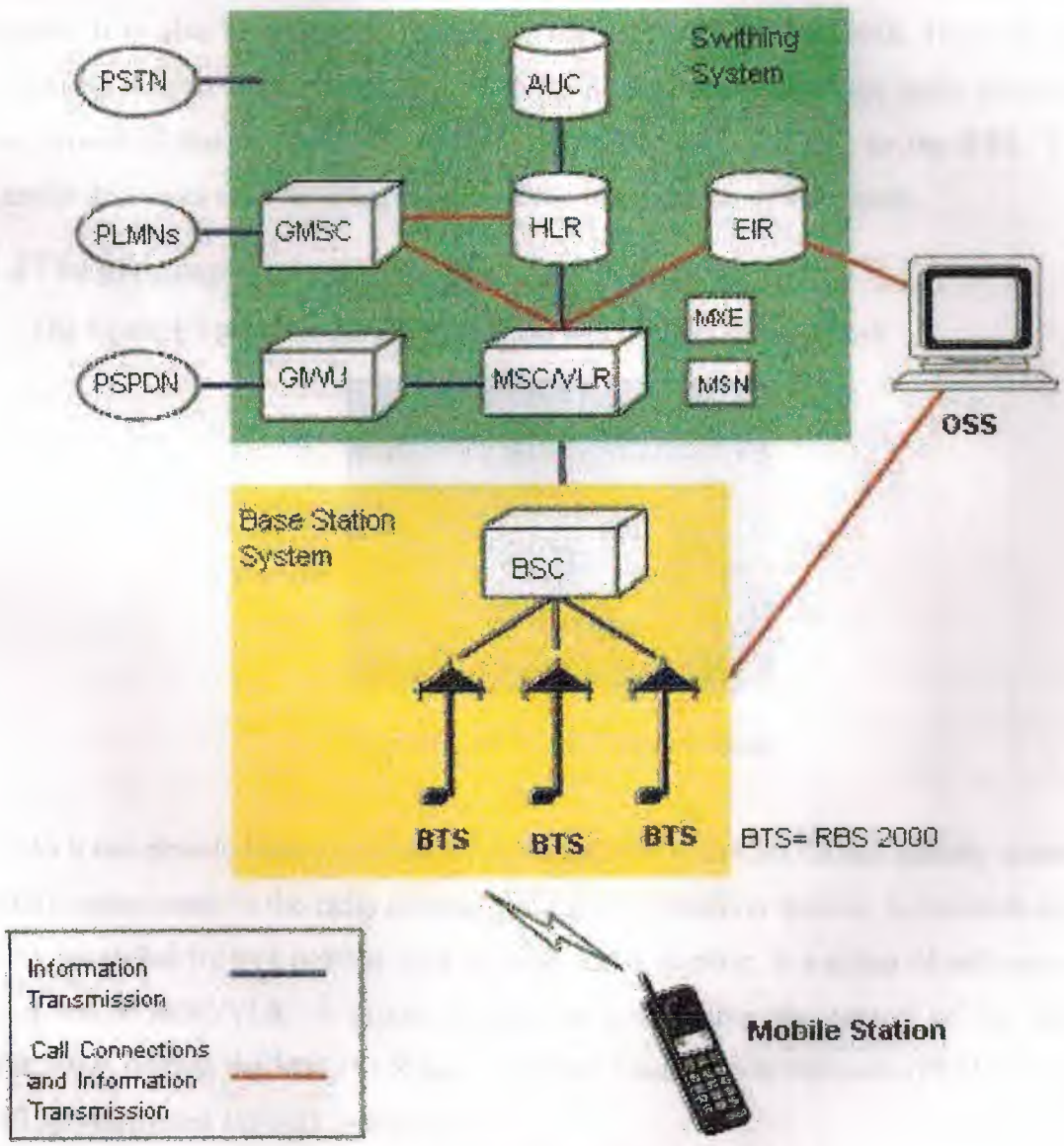


Figure 4.9 GSM Network Elements

4.2.4 The Operation and Support Subsystem (OSS)

The operations and maintenance center (OMC) is connected to all equipment in the switching system and to the BSC. The implementation of OMC is called the operation and support system (OSS). The OSS is the functional entity from which the network operator monitors and controls the system. The purpose of OSS is to offer the customer cost-effective support for centralized, regional, and local operational and maintenance activities that are required for a GSM network. An important function of OSS is to provide a network overview and support the maintenance activities of different operation and maintenance organizations. The OSS is connected to the different components of the NSS and to the BSC, in order to control and monitor the GSM system. It is also in charge of controlling the traffic load of the BSS. However, the increasing number of base stations, due to the development of cellular radio networks, has provoked that some of the maintenance tasks are transfered to the BTS. This transfer decreases considerably the costs of the maintenance of the system.

4.3 The geographical areas of the GSM network

The figure 4.5 presents the different areas that form a GSM network.

Figure 4.10 GSM Network Areas

As it has already been explained a cell, identified by its Cell Global Identity number (CGI), corresponds to the radio coverage of a base transceiver station. A Location Area (LA), identified by its Location Area Identity (LAI) number, is a group of cells served by a single MSC/VLR. A group of location areas 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.

4.4 The Gsm Functions

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

4.4.1 Transmission

The transmission function includes two sub-functions:

- The first one is related to the means needed for the transmission of user information.
- The second one is related to the means needed for the transmission of signaling information.

Not all the components of the GSM network are strongly related with the transmission functions. The MS, the BTS and the BSC, among others, are deeply concerned with transmission. But other components, such as the registers HLR, VLR or EIR, are only concerned with the transmission for their signaling needs with other components of the GSM network.

4.4.2 Radio Resources Management (RR)

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 mobile station and the base station. However, as the RR function is also in charge of maintaining a connection even if the user moves from one cell to another, the MSC, in charge of handovers, is also concerned with the RR functions.

The RR is also responsible for the management of the frequency spectrum and the reaction of the network to changing radio environment conditions. Some of the main RR procedures that assure its responsibilities are:

- Channel assignment, change and release.
- Handover.
- Frequency hopping.

- Power-level control.
- Discontinuous transmission and reception.
- Timing advance.

Some of these procedures are described in section 5. In this paragraph only the handover, which represents one of the most important responsibilities of the RR, is described.

Handover

The user movements can produce the need to change the channel or cell, specially when the quality of the communication is decreasing. This procedure of changing the resources is called handover. Four different types of handovers can be distinguished:

- Handover of channels in the same cell.
- Handover of cells controlled by the same BSC.
- Handover of cells belonging to the same MSC but controlled by different BSCs.
- Handover of cells controlled by different MSCs.
- Handovers are mainly controlled by the MSC. However in order to avoid unnecessary signaling information, the first two types of handovers are managed by the concerned BSC (in this case, the MSC is only notified of the handover).

The mobile station is the active participant in this procedure. In order to perform the handover, the mobile station controls continuously its own signal strength and the signal strength of the neighboring cells. The base station gives the list of cells that must be monitored by the mobile station. The power measurements allow to decide which is the best cell in order to maintain the quality of the communication link. Two basic algorithms are used for the handover:

- The `minimum acceptable performance' algorithm. When the quality of the transmission decreases (i.e. the signal is deteriorated), the power level of the mobile is increased. This is done until the increase of the power level has no effect on the quality of the signal. When this happens, a handover is performed.
- The `power budget' algorithm. This algorithm performs a handover, instead of continuously increasing the power level, in order to obtain a good communication quality.

4.4.3 Mobility Management

The MM function is in charge of all the aspects related with the mobility of the user, specially the location management and the authentication and security.

a) Location Management

When a mobile station is powered on, it performs a location update procedure by indicating its IMSI to the network. The first location update procedure is called the IMSI attach procedure.

The mobile station also performs location updating, in order to indicate its current location, when it moves to a new Location Area or a different PLMN. This location-updating message is sent to the new MSC/VLR, which gives the location information to the subscriber's HLR. If the mobile station is authorized in the new MSC/VLR, the subscriber's HLR cancels the registration of the mobile station with the old MSC/VLR.

A location updating is also performed periodically. If after the updating time period, the mobile station has not registered, it is then deregistered.

When a mobile station is powered off, it performs an IMSI detach procedure in order to tell the network that it is no longer connected.

b) Authentication and Security

The authentication procedure involves the SIM card and the Authentication Center. A secret key, stored in the SIM card and the AuC, and a ciphering algorithm called A3 are used in order to verify the authenticity of the user. The mobile station and the AuC compute a SRES using the secret key, the algorithm A3 and a random number 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.

Another security procedure is to check the equipment identity. If the IMEI number of the mobile is authorized in the EIR, the mobile station is allowed to connect the network. In order to assure user confidentiality, the user is registered with a Temporary Mobile Subscriber Identity (TMSI) after its first location update procedure.

4.4.4 Communication Management (CM)

The CM function is responsible for:

- Call control.
- Supplementary Services management.
- Short Message Services management.

a) Call Control (CC)

The CC is responsible for call establishing, maintaining and releasing as well as for selecting the type of service. One of the most important functions of the CC is the call routing. In order to reach a mobile subscriber, a user diales the Mobile Subscriber ISDN (MSISDN) number which includes:

- A country code.
- A national destination code identifying the subscriber's operator.
- A code corresponding to the subscriber's HLR.

The call is then passed to the GMSC (if the call is originated from a fixed network), which knows the HLR corresponding to a certain MISDN number. The GMSC asks the HLR for information helping to the call routing. 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. Thanks to the MSRN number, the call is routed to subscriber's current MSC/VLR. In the subscriber's current LA, the mobile is paged.

b) Supplementary Services Management

The mobile station and the HLR are the only components of the GSM network involved with this function

c) Short Message Services Management

In order to support these services, a GSM network is in contact with a Short Message Service Center through the two following interfaces:

- The SMS-GMSC for Mobile Terminating Short Messages (SMS-MT/PP). It has the same role as the GMSC.
- The SMS-IWMSC for Mobile Originating Short Messages (SMS-MO/PP).

4.4.5 Operation, Administration and Maintenance (OAM)

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

The components of the BSS and NSS provide the operator with all the information it needs. This information is then passed to the OSS, which is in charge of analize it and control the network.

The self-test tasks, usually incorporated in the components of the BSS and NSS, also contribute to the OAM functions.

CONCLUSION

The first cellular radio system in Europe was installed in Scandinavia in 1981 and it served initially only a few thousand subscribers. But now days from 1981 to 2001 we are seeing that a few thousand subscribers reached to 500 million subscribers.

A general objective of the GSM system is to provide a wide range of services and facilities, both voice and data, that are compatible with the existing fixed Public Switched Telephone Network (PSTN), Public Switched Data Networks (PSDN), Public Land Mobile Network (PLMN) and Integrated Services Digital Networks (ISDN). Another objective is to give compatibility considered mobile subscriber the access to any mobile subscriber in any country, which operates the system, and provides facilities for automatic roaming, locating and updating the mobile subscriber's status.

The Radio Interface is the interface between the mobile stations and the fixed infrastructure. It is one of the most important interfaces of the GSM system. One of the main objectives of GSM is Roaming. Therefore, in order to obtain a complete compatibility between mobile stations and networks of different manufacturers and operates, the radio interface must be completely defined.

GSM as the modern telecommunication system is a complex object. Its implementation and operation are not simple task, neither easy its describtion.

In this Graduation Project I have tried to give an explanations of the GSM, GSM (PLMN), channel and frame structures, radio Interface and most weighted about GSM ArchitectureAs with any explanations, there are many details missing. I believe, however, that gave the brief explanations in each chapters.

REFERENCES

[1] Mamedov F. S., Telecommunications. Lecture notes, Near East University Press, Lefkoşa, 2000

[2] Vijay K. Garg, Joseph E. Wilkes, Wireless and Personel Communications Systems, Feher/Prentice Hall Digital and Wireless Communications Series, AT&T Bell Labs, Holmdel,New Jersey, 1996.

[3] Padgett, Jay E., Guther, Christoph H., Hattori, Takeshi " Overview of Wirless Personal Communication", IEEE Communications Magazine, V33, n1, January, 1995.

[4] Lee, W. C. Y., Mobile Cellular Telecommunication Systems, New York:McGraw-Hill.1989

[5] Hans Lobensommer and Helmut Mahner: GSM – a European mobile radio standard for the world market. Telecom Report International, 15(3-4), 1992.

[6] Mouly, Mm and Poutert, M "The GSM System for Mobile Communication". Palaiseau, France, 1992.

[7] Vijay K. Garg, Willowbrook, Illinois Joseph E. Wilkes, "Principles and Applications of GSM" Red Bank, New Jesrsy, 1999.

[8] David M. Bolston. The pan-European system: GSM. In David M. Bolston and R.C.V. Macario, editors, cellular Radio System. Artech House, Boston, 1993.

[9] Javier Gozalvez Sempere Reserch Engineer in Mobile Communications " An Overview of the GSM system" Univesity of Strothclyde Glasgow, Scotland.

[10] John Scourios (University of Waterloo). "Overview of Global System for Mobile Communications.".

"http"//ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html"