NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Electrical and Electronics Engineering

RADIO INTERFACE IN GSM

Graduation Project
EE – 400

Student : Saher Abdel hafez

Supervisor: Prof. Dr. Fakhreddin Mamedov

NICOSIA - 2004

ACKNOWLEDGEMENT

First of all, I would like to extend my utmost and deepest thanks to my advisor, Prof. Dr. Fakhreddin Mamedov, for the intellectual support, encouragement, and enthusiasm, which made this project possible.

I also pay tribute to my dearest parents, my friends and all my electrical engineering dept. staff members specially Mr. Halil Adahan, Mr. Ozgur Ozerdem, Mr. Izzet Agoren, and who had taught me that no dream is impossible.

I am so happy and excited to complete the task which I had been given with the blessing of God and also I am grateful to all the people in my life whom had supported me, advised me, taught me and whom had always encouraged me to follow my dreams and ambitions.

Also, my sincerest thanks must go to my friends, Omar Daban,, Adeeb Husseini, whom shared their suggestions and evaluations throughout the completion of my project. The comments from these friends enabled me to present this project successfully.

Finally, I thank God for giving me the will and courage to achieve my objectives.

ABSTRACT

Different requirements and the dedication to meet them led to, the development of the GSM standard. An unprecedented effort has been taken by telecommunication authorities, network operators, and industry sectors to establish and maintain a state-of-the-art cellular standard for the benefit of the entire industry and all its customers.

The GSM standard can be regarded as an evolving standard. The whole standardization process could not be completed before the actual launch of the services; a phased approach to rolling out the specifications and the networks was adopted. The reduced features were initially designed to be upwardly compatible *odd-ons* of services and functions, the subset was called GSM *Phase* 1. The additional supplements to full implementation of all the planned services and network features were called GSM *Phase* 2. By this, the GSM platform was created, a platform which is full of hooks, mechanisms and not at least potential to continue to build on and to provide mobile communication in all its possible forms and variations.

Even before the *Phase* 2 standard has been completed, GSM has grown far beyond its original geographical "limitations" and the Global System Of Mobile Communication really starts to deserve its name. With Phase 2, and in particular with Phase 2+, GSM will also expand far beyond its originally intended functional boundaries and open up for new applications, new access methods, new technologies and thus altogether for new categories of markets, needs and users.

It looks Promising.

TABLE OF CONTENTS

INTRODUCTION

GSM stands for "Global System For Mobile Communication". Words cannot easily express the tireless efforts expanded to propel the development of the GSM standard, design a network architecture, test and verify technical parameters, prove functionalities, promote the system itself, and design and manufacture the necessary equipment. What we see today is the result of this work.

The new standard has given new momentum to the economy and has created new markets. A common standard for a market whose customer's number in the tens of millions lead s to minimize costs for the manufacturers of appropriate equipment. They can produce large number of terminals for a large market, which drives down the cost to end-user.

New services and features, especially the roaming and security features, as well as the digital advantages, such as reduced power consumption (state-of-the-art semiconductor devices, TDMA technology) and improved speech quality are the keys that convince network operators and potential subscribers to choose GSM.

This project "Radio Interface in GSM" consist of an Introduction, four Chapters and a Conclusion.

Chapter one: Cellular Telecommunications, its principles and services, the use of frequencies and cells.

Chapter two: Introduction To GSM, contains a brief introduction about GSM, its history, services offered by GSM, the System Architecture of GSM, it's Radio Link Aspects and it's Network Aspects.

Chapter Three: Radio Interface, this chapter gives an introduction about Radio Interface, it also explain the Access to the Trunking System, the Channel Structure, the Burst Structure, Frequency Hopping and Radio Frequency Power Level.

Chapter four: Cell Planning, this chapter confines the focus on different aspects of Cell Planning. Starting from History, it explains the Cellular Structure, Network Planning, Mobile Radio Network Planning Tasks, Radio Wave Propagation, Cellular Network and Frequency allocation and finally Call Handover/Handoff.

Finally, the Conclusion explains the knowledge gained during the making of this project and the future of GSM.

1. CELLULAR TELECOMMUNICATIONS

1.1 Principles of Cellular Telecommunications

A Cellular telephone system links mobile station (MS) subscribers into the public telephone system or to another cellular system's MS subscriber.

Information sent between the MS subscriber and the cellular network uses radio communication. This removes the necessity for the fixed wiring used in the traditional telephone installation. Due to this, the MS subscriber is able to move around and become fully mobile, perhaps travelling in a vehicle or on foot [1].

1.1.1 Advantages of Cellular Communications

Cellular networks have many advantages over the existing "land" telephone networks. There are many advantages for the network provider as well as the mobile subscriber.

1.1.2 Advantages to mobile Subscriber

1. Mobility
2. Flexibility
3. Convenience

1.1.3 Advantages to Network Provider

1. Network Expansion Flexibility
2. Revenue/Profile Margins
3. Efficiency
4. Easier Re-Configuration

1.2 Services provided by GSM

GSM was designed having interoperability with ISDN in mind, and the services provided by GSM are a subset of the standard ISDN services. Speech is the most basic, and most important, tele-service and bearer service provided by GSM.

In addition, various data services are supported, with user bit rates up to 9600 bps. Specially equipped GSM terminals can connect with PSTN, ISDN, Packet Switched and Circuit Switched Public Data Networks, through several possible methods, using synchronous or asynchronous transmission. Also supported are Group 3 facsimile service, videotex, and teletex. Other GSM services include a cell broadcast service, where messages such as traffic reports, are broadcast to users in particular cells.
A service unique to GSM, the Short Message Service, allows users to send and receive point-to-point alphanumeric messages up to a few tens of bytes. It is similar to paging services, but much more comprehensive, allowing bi-directional messages, store-and-forward delivery, and acknowledgement of successful delivery.

Supplementary services enhance the set of basic tele-services. In the Phase I specifications, supplementary services include variations of call forwarding and call barring, such as Call Forward on Busy or Barring of Outgoing International Calls. Many more supplementary services, including multiparty calls, advice of charge, call waiting, and calling line identification presentation will be offered in the Phase 2 specification [2].

1.3 Cell Site

The number of cells in any geographic area is determined by the number of Mobile Station (MS) subscribers whom will be operating in that area, and the geographic layout of the area (hills, lakes, buildings etc).

1.3.1 Large Cells

The maximum cell size for GSM is approximately 80.5 Km in diameter, but this is dependent on the terrain the cell is covering and the power class of the MS. In GSM the MS can be transmitting anything up to 8 watts, obviously, the higher the power output of the MS the larger the cell size. If the cell site is on top of a hill with no obstruction for miles, then the radio waves will travel much further than if the cell site was in the middle of a city, with many high-rise building blocking the path of the radio waves.

Generally large cells are employed in:

1. Remote areas.
2. Coastal regions.
3. Area with few subscribers.
4. Large areas which need to be covered with the minimum number of cell sites.

1.3.2 Small Cells

Small cells are used where there is a requirement to support a large number of MSs in a small geographic region, or where a low transmission power may be required to reduce the effects of interference. Small cells currently cover 200 m and upward.

Typical uses of a small cells:

1. Urban areas.
2. Low transmission power required.
3. High number of MSs

1.3.3 The Trade off – Large v Small

There is no right answer when choosing the type of cell to use. Network provides would like to use large cells to reduce installation and maintenance cost, but realize that to provide a quality service to their customers, they have to consider many factors, such as terrain, transmission power required, number of MSs. This inevitably leads to a mixture of both large and small cells [1] .

1.4 Network Components

GSM networks are made up of Mobile Services Switching Centre (MSC), Base Station Systems (BSS) and Mobile Stations (MS). These three entities can be broken down further into smaller entities as within BSS we have Base Station Controllers (BSC), Base Transceiver Stations (BTS) and Transcoders (XCDR). These smaller network elements, as they are referred to, will be discussed later in the research. For now we will use three major entities.

With the MSC, BSS and MS we can make calls, receive calls, perform billing etc, as any normal PSTN network would be able to do. The only problem for the MS is that all the calls made or received are from other MSs. Therefore, it is also necessary to connect the GSM network to the PSTN.

Mobile Stations within the cellular network are located in "cells", these cells are provided by the BSSs. Each BSS can provide one or more cells, dependent on the manufacturers equipment.

The cells are normally drawn as hexagonal, but in practice they are irregularly shaped, this is as a result of the influence of the surrounding terrain, or of design by the network planners [1] .

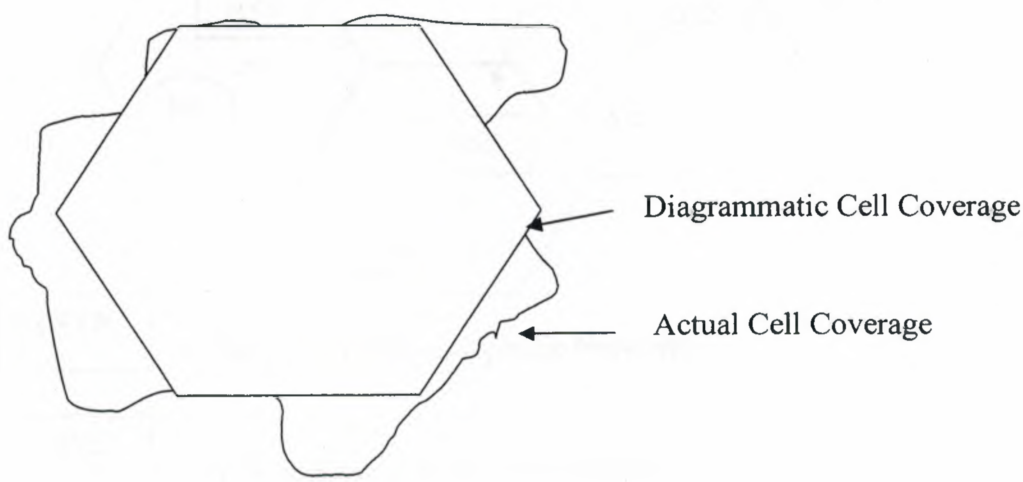

Figure 1.1 Actual and Diagrammatic Cell Coverage

PSTN is connected to the GSM Network through the MSC

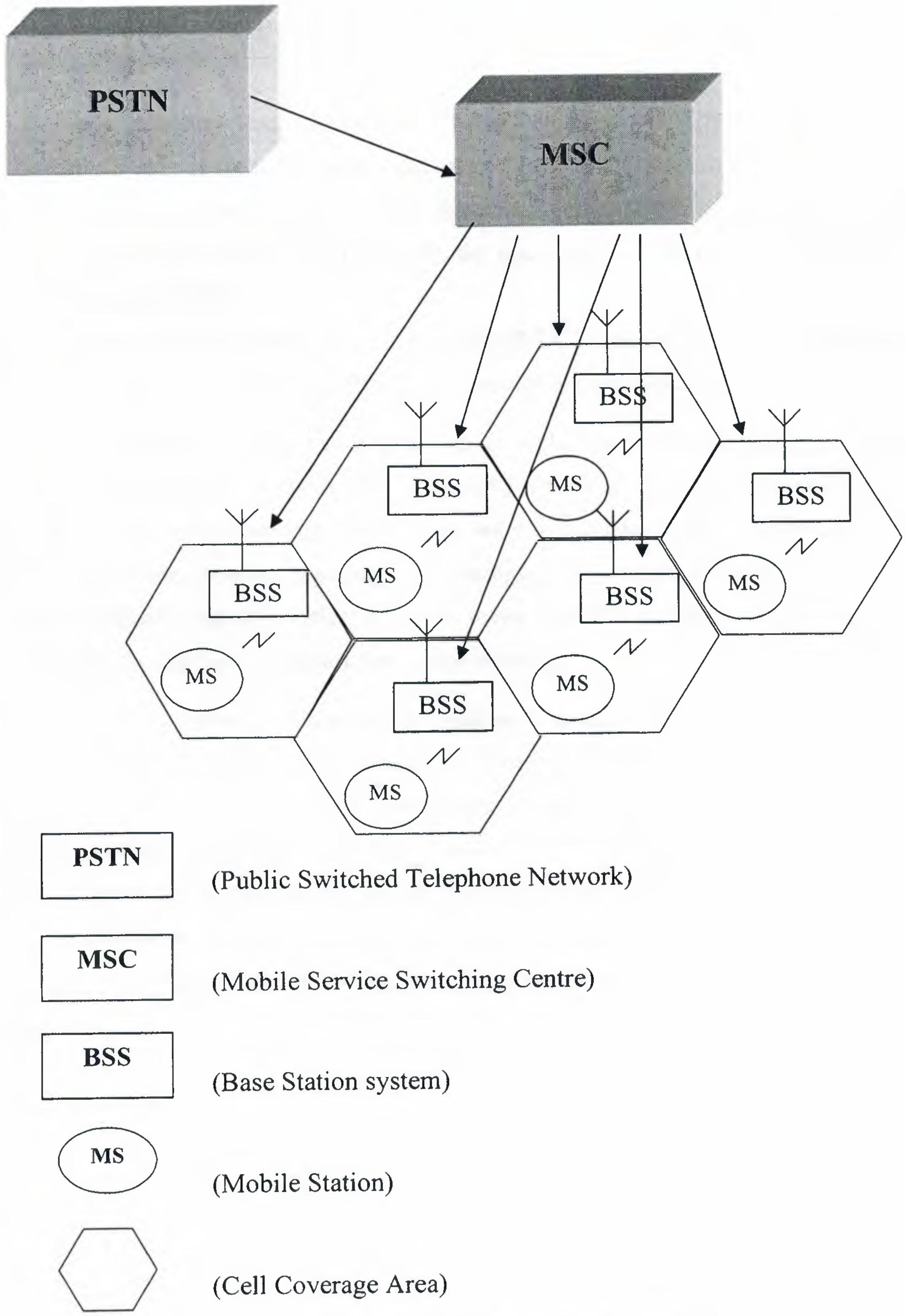

Figure 1.2 Network components

1.5 Frequency Spectrum

The frequency spectrum is very congested, with only narrow slots of bandwidth allocated for cellular communication. Number of frequencies and spectrum allocated for GSM, Extended GSM (EGSM), GSM1800 (DCS1800) and PCS1900 are covered in the next section.

A single Absolute Radio Frequency Channel Number (ARFCN) or RF carrier is actually a pair of frequency, one used in each direction (transmit and receive). This allows information to be passed in both directions. For GSM900, the paired frequencies are separated by 45MHz. For DCS1800, the separation is 95MHz. And for PCS1900, separation is 75MHz.
For each cell in GSM network (GSM, EGSM OR DCS1800), at least one ARFCN must be allocated, and more may be allocated to provide greater capacity.

The RF carrier in GSM can support up to eight Time Division Multiple Access (TDMA) timeslots. That is, in theory, each RF carrier is capable of supporting up to eight simultaneous telephone calls. But as we will see later in this research, although this is possible, network signaling and messaging may reduce the overall number of eight timeslots per RF carrier to six or seven timeslots per RF carrier. Therefore, reducing the number of mobiles that can be supported.

Unlike a PSTN network, where every telephone is linked to the land network by a pair of fixed wires, each MS only connects to the network over the radio interface when required. Therefore, it is possible for a single RF carrier to support many more mobile stations than its eight TDMA timeslots would lead us to believe. Using statistics, it has been found that a typical RF carrier can support up to 15, 20 or even 25 MSs. Obviously, not all of these MS subscribers could make a call at the same time. Therefore, without knowing it, MSs share the same physical resources, but at different times [3] .

1.5.1 Frequency Range

GSM	EGSM	DCS1800	ARFCN
Receive (uplink) 890-915 MHZ	Receive (uplink) 880-915 MHZ	Receive (uplink) 1710-1785 MHZ	Bandwidth = 200 KHZ
Transmit (downlink) 935-960 MHZ	Transmit (downlink) 925-960 MHZ	Transmit (downlink) 1805-1880 MHZ	8 TDMA timeslots
124 Absolute Radio Frequency Channels (ARFCN)	175 Absolute Radio Frequency Channels (ARFCN)	374 Absolute Radio Frequency Channels (ARFCN)	

1.6 Frequency Re-use

Standard GSM has a total of 124 frequencies available for use in a network. Most network providers are unlikely to be able to use all of these frequencies and are generally allocated a small subset of the 124.

As an example, a network provider has been allocated 48 frequencies to provide coverage over a large area, let us take for example Great Britain. As we have already seen, the maximum cell size is approximately 80.5 Km in diameter, This our 48 frequencies would not be able to cover the whole Britain. To cover this limitation the network provider must re-use the same frequencies over and over again, in what is termed a "frequency re-use pattern". When planning the frequency re-use pattern, the network planner must take into account how often to use the same frequencies and determine how close together the cells are, otherwise co-channel interference and / or adjacent channel interference may occur. The network provider will also take into account the nature of the area to be covered. This may range from a densely populated (high frequency re-use, small cells, high capacity) to sparsely populated rural expanse (large omni cells, low re-use, low capacity).

1.6.1 Co-Channel Interference

This occurs when RF carrier of the same frequency are transmitting in close proximity to each other, the transmission from one RF carrier interferes with the other RF carrier.

1.6.2 Adjacent Channel Interference

This occurs when a RF source of nearby frequency interferes with the RF carrier [3].

1.7 Sectorization

The cells we have looked at up to now are omni- directional cells. That is each site has a single cell and that cell has a single transmit antenna, which radiates the radio waves to 360 degrees.

The problem with employing omni-directional cells is that as the number of MSs increases in the same geographical region, we have to increase the number of cells to meet the demand. To do this, as we have seen, we have to decrease the size of the cell and fit more cells into this geographical area. Using omni –directional cells we can only go so far before we start introducing co-channel and adjacent channel interference both of which degrade the cellular network's performance.

To gain a further increase in capacity within the geographic area we can employ a technique called " Sectorization ". Sectorization splits a single site into a number of cells each cell has transmit and receive antennas and behaves as an independent cell. Each cell uses special directional antennas to ensure that the radio propagation from one cell is concentrated in a particular direction. This has a number of advantages:

Firstly, as we are now concentrating all energy from the cell in a smaller area 60, 120, 180 degrees instead of 360 degrees, we get much stronger signal, which is beneficial in location such as "in-building coverage".

Secondly, we can use the same frequencies in a much closer re-use pattern, thus allowing more cells in our geographic region, which allows us to support more MSs [2].

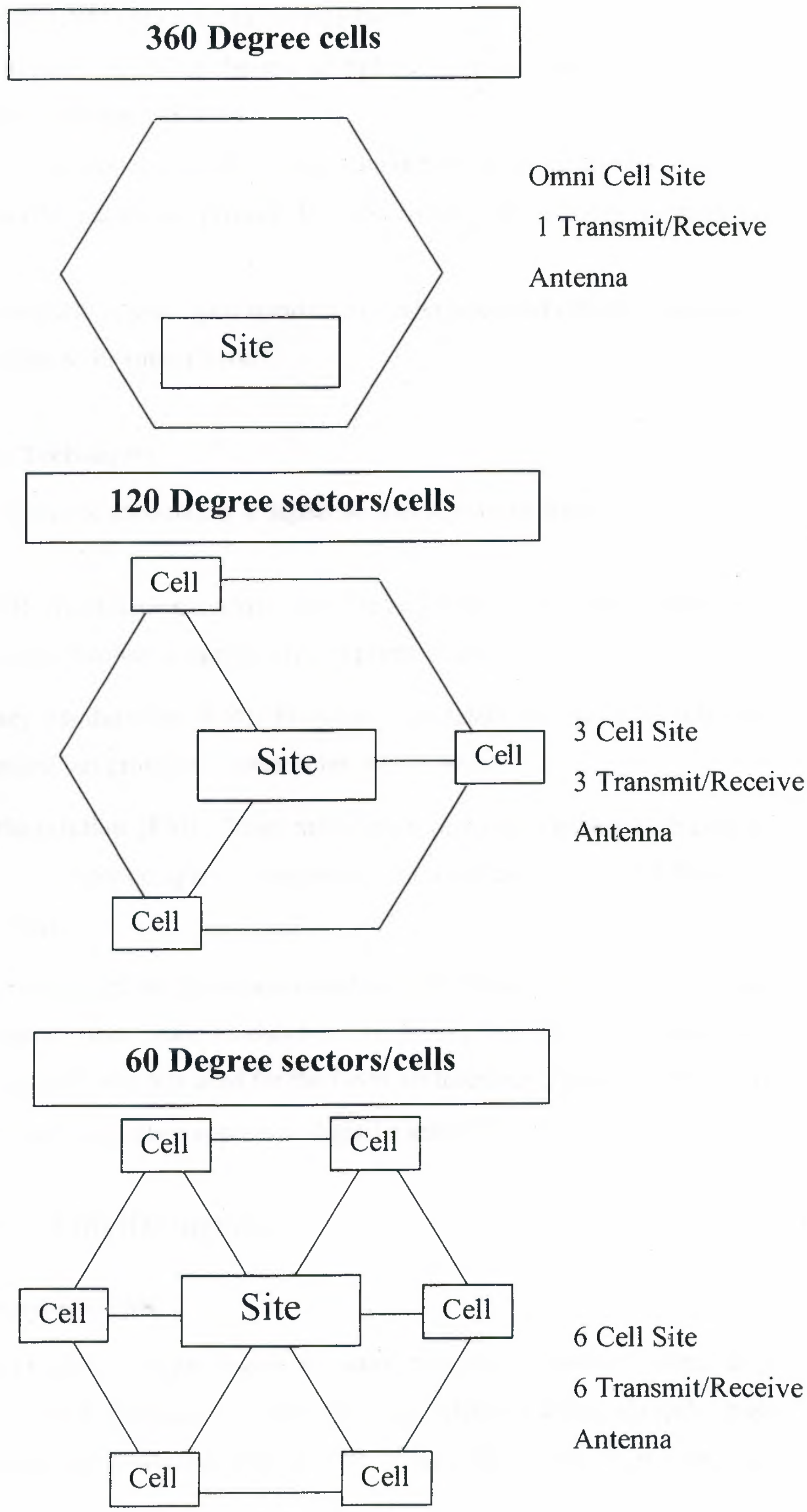

Figure 1.3 Sectorization

1.8 Transmission of Analogue and Digital Signals

The main reasons why GSM uses a digital air interface:

- It is "noise robust", enabling the use of tighter frequency re-use patterns and minimizing interference problems.
- It incorporates error correction, thus protecting the traffic that it carries.
- It offers greatly enhanced privacy to subscribers and security to network providers.
- It is ISDN compatible, uses open standardized interfaces and offers an enhanced range of services to its subscribers.

1.8.1 Modulation Techniques

There are three methods of modulating a signal so that it may be transmitted over the air:

1. **Amplitude Modulation (AM):** Amplitude Modulation is very simple to implement for analogue signals but it is prone to noise.
2. **Frequency Modulation (FM):** Frequency Modulation is more complicated to implement but provides a better tolerance to noise.
3. **Phase Modulation (PM):** Phase modulation provides the best tolerance to noise but it is very complex to implement for analogue signals and therefore is rarely used.

Digital signals can use any of the modulation methods, but phase modulation provides the best noise tolerance; since phase modulation can be implemented easily for digital signals, this is the method, which is used for the GSM air interface. Phase Modulation is known as Phase Shift Keying when applied to digital signals [1].

1.9 Transmission of Digital Signals

1.9.1 Phase Shift Keying – PSK

Phase Modulation provides a high degree of noise tolerance. However, there is a problem with this form of modulation. When the signal changes phase abruptly, high frequency components are produced; thus a wide bandwidth would be required for transmission.

GSM has to be as efficient as possible with the available bandwidth. Therefore, it is not this technique, but a more efficient development of phase modulation that is actually used by GSM air interface, it is called Gaussian Minimum Shift Keying (GMSK).

1.9.2 Gaussian Minimum Shift Keying – GMSK

With GMSK, the phase change which represents the change from a digital '1' or a '0' does not occur instantaneously as it does with Binary Phase Shift Keying (BPSK). Instead it occurs over a period of time and therefore the addition of high frequency components to the spectrum is reduced.

With GMSK, first the digital signal is filtered through a Gaussian filter. This filter causes distortion to the signa, the corners are rounded off. This distorted signal is then used to phase shift the carrier signal. The phase change therefore is no longer instantaneous but spread out [1].

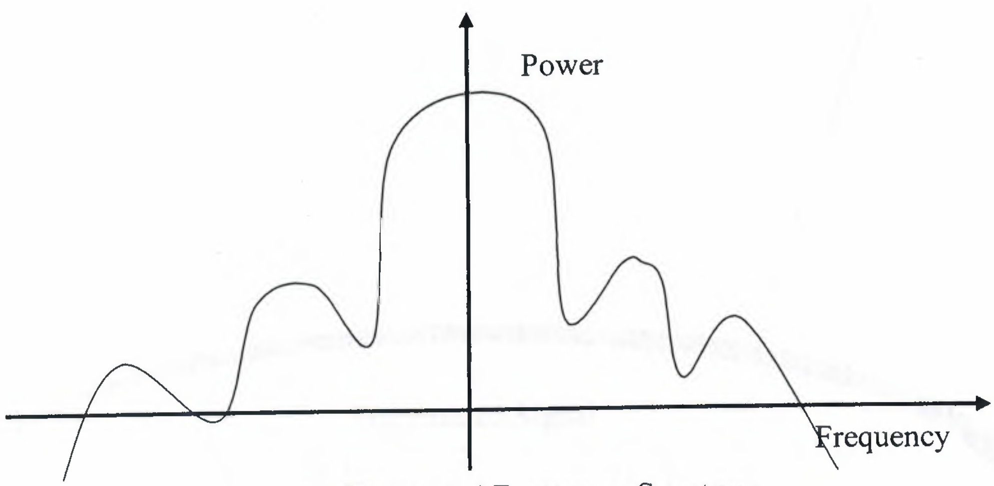

Figure 1.4 Frequency Spectrum

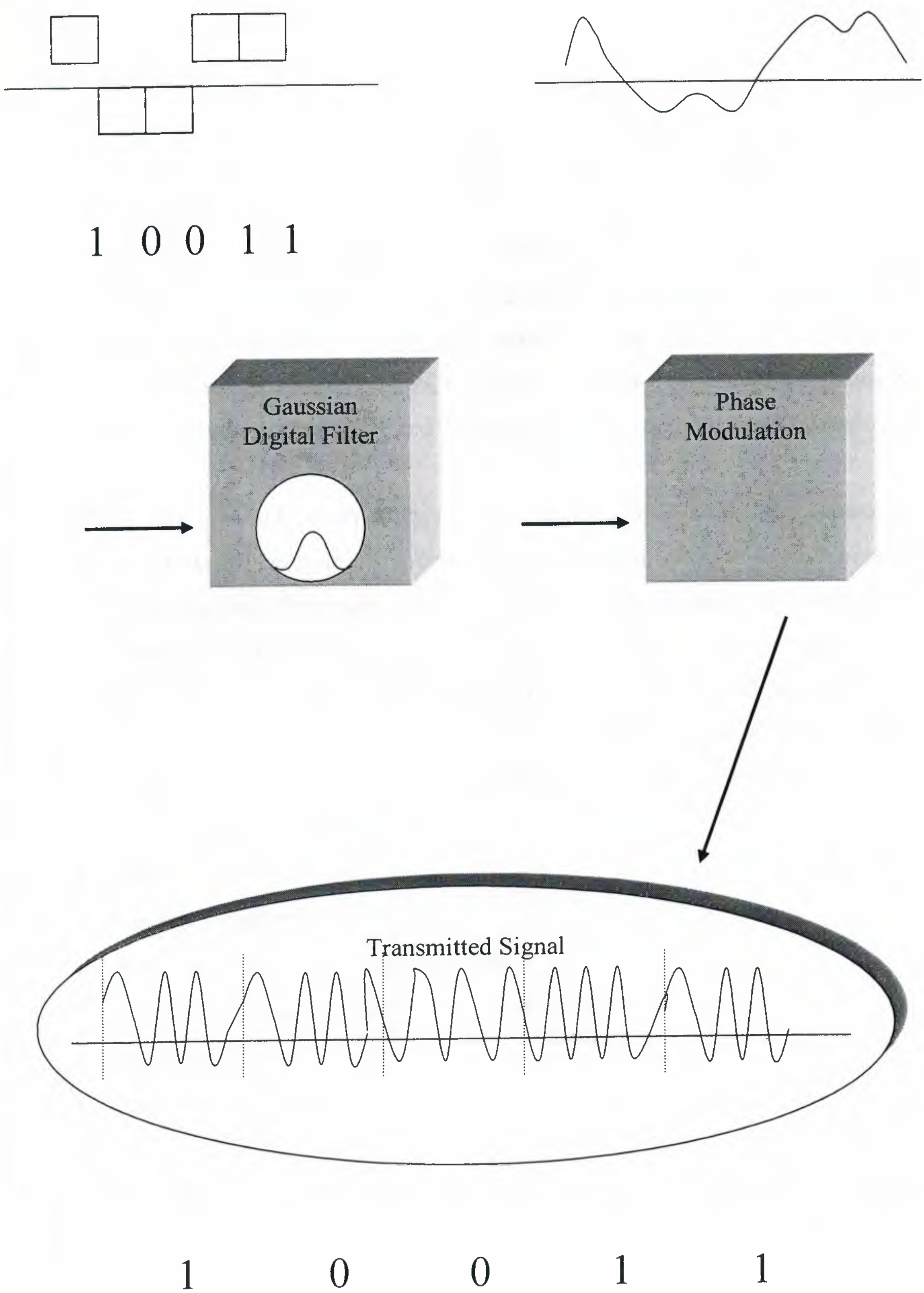

Figure 1.5 Gaussian Minimum Shift Keying (GMSK)

CHAPTER TWO
ARCHITECTUTE of GSM

2.1 Overview

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. Each country developed its own system, which was incompatible with everyone else's in equipment and operation. This was an undesirable situation, because not only was the mobile equipment limited to operation within national boundaries, which in a unified Europe were increasingly unimportant, but there was a very limited market for each type of equipment, so economies of scale, and the subsequent savings, could not be realized.

In 1981 a joint Franco German study was initiated to develop a common approach, which, it was hoped, would become a standard for Europe. Soon after, in 1982 a proposal from Nordic Telecom and Netherlands PTT to the CEPT (Conference of European Post and Telecommunications) to develop a new digital cellular standard that would cope with the ever burgeoning demands on European mobile networks. Then a study group formed called the Group Special Mobile (GSM) to study and develop a pan-European public land mobile system. The proposed system had to meet certain criteria:

- Good subjective speech quality
- Low terminal and service cost
- Support for international roaming
- Ability to support handheld terminals
- Support for range of new services and facilities
- Spectral efficiency
- ISDN compatibility

In 1989, GSM responsibility was transferred to the European Telecommunication Standards Institute (ETSI), and phase I of the GSM specifications was published in 1990.

Commercial service was started in mid-1991, and by 1993 there were 36 GSM networks in 22 countries. Although standardized in Europe, GSM is not only a European standard. Over 200 GSM networks (including DCS1800 and PCS1900) are operational in 110 countries around the world. In the beginning of 1994, there were 1.3 million subscribers worldwide, which had grown to more than 55 million by October 1997. With North America making a delayed entry into the GSM field with a derivative of GSM called PCS1900, GSM systems exist on every continent, and the acronym GSM now aptly stands for Global System for Mobile communications.

The developers of GSM chose an unproven (at the time) digital system, as opposed to the then-standard analog cellular systems like AMPS in the United States and TACS in the United Kingdom. They had faith that advancements in compression algorithms and digital signal processors would allow the fulfillment of the original criteria and the continual improvement of the system in terms of quality and cost. The over 8000 pages of GSM recommendations try to allow flexibility and competitive innovation among suppliers, but provide enough standardization to guarantee proper networking between the components of the system. This is done by providing functional and interface descriptions for each of the functional entities defined in the system.

The original French name was later changed to Global System for Mobile Communications, but the original GSM acronym stuck.

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.

The Global System for Mobile communications (GSM) is a digital cellular communications system initially developed in an European context which has rapidly gained acceptance and market share worldwide. It was designed to be compatible with ISDN systems and the services provided by GSM are a subset of the standard ISDN services (speech is the most basic).

The functional architecture of a GSM system can be divided into the Mobile Station (MS), the Base Station (BS), and the Network Subsystem (NS). The MS is carried by the subscriber, the BS subsystem controls the radio link with the MS and the NS performs the switching of calls between the mobile and other fixed or mobile network users as well as mobility management. The MS and the BS subsystem communicate across the Um interface also known as radio link.

2.2 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 Group Special 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 criteria:

- 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. The reasons for this choice are explained in section 3.

In 1989 the responsibility 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 networking between the different elements of the GSM system. In 1990, the phase I of the GSM specifications was published but the commercial use of GSM did not start until mid 1991.

The most important events in the development of the GSM system are presented in the table 2.1

Table 2.1 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 responsibility 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 operational 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 table 2 charts the different mobile cellular systems developed since the commercial launch of cellular systems.

Table 2.2 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>

2.3 Architecture of the GSM Network

The GSM network is composed of several functional entities, whose functions and interfaces are defined. The GSM network can be divided into four broad parts. The Mobile Station is carried by the subscriber; 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, performs the switching of calls between the mobile and other fixed or mobile network users, as well as management of mobile services, such as authentication. With the Operations and Maintenance center, which oversees the proper operation and setup of the network. And the operational and support subsystem. The Mobile Station and the Base Station Subsystem communicate across the Um interface, also known as the air interface or radio link. The Base Station Subsystem communicates with the Mobile service Switching Center.

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 2.1.

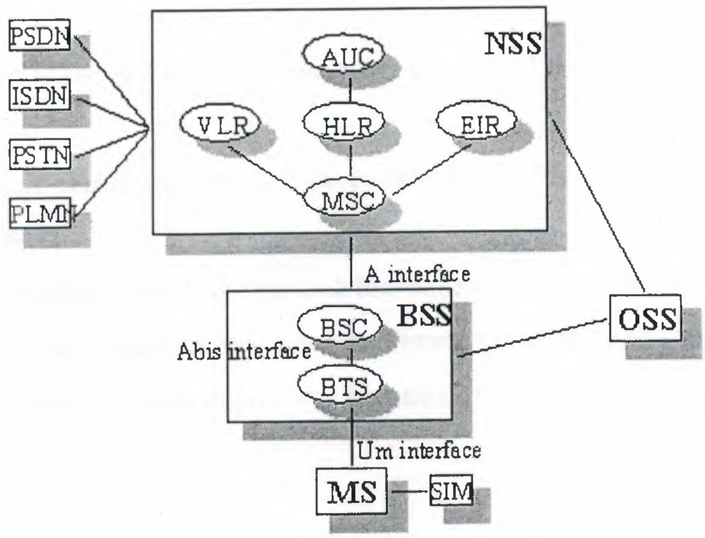

Figure 2.1 Architecture of the GSM network

2.3.1 Mobile Station

The mobile station (MS) consists of the physical equipment, such as the radio transceiver, display and digital signal processors, and a smart card called the Subscriber Identity Module (SIM). The SIM provides personal mobility, so that the user can have access to all subscribed services irrespective of both the location of the terminal and the use of a specific terminal. By inserting the SIM card into another GSM cellular phone, the user is able to receive calls at that phone, make calls from that phone, or receive other subscribed services.

The mobile equipment is uniquely identified by the International Mobile Equipment Identity (IMEI). The SIM card contains the International Mobile Subscriber Identity (IMSI), identifying the subscriber, a secret key for authentication, and other user information. The IMEI and the IMSI are independent, thereby providing personal mobility. The SIM card may be protected against unauthorized use by a password or personal identity number.

- **The Terminal**

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

1-The" fixed" terminals are the ones installed in cars. Their maximum allowed output power is 20 W.

2-The GSM portable terminals can also be installed in vehicles. Their maximum allowed output power is 8W.

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

- **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; The SIM card is protected by a four-digit Personal Identification Number (PIN). In order to identify the subscriber to the system, the SIM card contains some parameters of the user such as its International Mobile Subscriber 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.

2.3.2 The Base Station Subsystem

The Base Station Subsystem (BSS) is composed of two parts, the Base Transceiver Station (BTS) and the Base Station Controller (BSC). These communicate across the specified A-bis interface, allowing (as in the rest of the system) operation between components made by different suppliers.

The BTS 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. The requirements for a BTS are ruggedness, reliability, portability, and minimum cost. BTS is responsible for providing layers 1 and 2 of the radio interface, that is, an error-corrected data path. Each BTS has at least one of its radio channels assigned to carry control signals in addition to traffic.

The BSC manages the radio resources for one or more BTSs. It is responsible for the management of the radio resource within a region. Its main functions are to allocate and control traffic channels, control frequency hopping, undertake handovers (except to cells outside its region) and provide radio performance measurements. Once the mobile has accessed, and synchronized with, a BTS the BSC will allocate it a dedicated bi-directional signaling channel and will set up a route to the Mobile services 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.

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:

1-The Base Transceiver Station (BTS) or Base Station.

2-The Base Station Controller (BSC).

- **The Base Transceiver Station**

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.

- **The Base Station Controller**

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.

2.3.3 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 in addition 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 public fixed network (PSTN or ISDN), and signaling between functional entities uses the ITUT Signaling System Number 7 (SS7), used 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 (possibly international) 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. It also contains a unique authentication key and associated challenge/response generators.

The current location of the mobile is in the form of a Mobile Station Roaming Number (MSRN), which is a regular ISDN number used to route a call to the MSC where the mobile is currently located. There is logically one HLR per GSM network, although it may be implemented as a distributed database.

The 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, most manufacturers of switching equipment implement one VLR together with one MSC, so that the geographical area controlled by the MSC corresponds to that controlled by the VLR, 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

Mobile Equipment Identity (IMEI). An IMEI is marked as invalid if it has been reported stolen or is not type approved. The Authentication Canter is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and ciphering of the radio channel.

The 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.

- **The Mobile services Switching Center (MSC)**

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

- **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.

- **Home Location Register (HLR)**

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

- **Visitor Location Register (VLR)**

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.

- **The Authentication Center (AuC)**

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.

- **The Equipment Identity Register (EIR)**

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. A terminal is identified by its International Mobile Equipment Identity (IMEI). The EIR allows then to forbid calls from stolen or unauthorized terminals (e.g., a terminal which does not respect the specifications concerning the output RF power).

- **The GSM Interworking Unit (GIWU)**

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

2.3.4 The Operation and Support Subsystem (OSS)

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 transferred to the BTS. This transfer decreases considerably the costs of the maintenance of the system.

2.4 The Geographical Areas of The GSM Network

The figure 2.2 presents the different areas that form a GSM network.

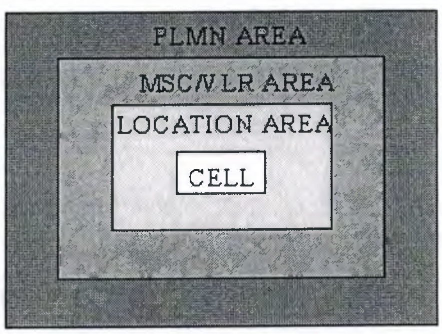

Figure 2.2 GSM network areas

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

2.5 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).

2.5.1 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.

2.5.2 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:

1- Channel assignment, change and release.
2- Handover.
3- Frequency hopping.
4- Power-level control.
5- Discontinuous transmission and reception.
6- Timing advance.

Handover, which represents one of the most important responsibilities of the RR, will
Be described:

- **Handover:**

Movements can produce the need to change the channel or cell, especially 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:

1- Handover of channels in the same cell.
2- Handover of cells controlled by the same BSC.
3- Handover of cells belonging to the same MSC but controlled by different BSCs.
4- 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 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 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.

2.5.3 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.

- **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.

- **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.

The SIM card and the Authentication Center are used for 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.

2.5.4 Communication Management (CM)

The CM function is responsible for:

1 -Call control.

2 - Supplementary Services management.

3 -Short Message Services management.

- **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 dials the Mobile Subscriber ISDN (MSISDN) number, which includes:

1-A country code

2-A national destination code identifying the subscriber's operator

3-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.

- **Supplementary Services Management**

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

- **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:

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

2 -The SMS-IWMSC for Mobile Originating Short Messages (SMS-MO/PP).

2.5.5 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 as it is shown in the following examples:

1-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 analyzing it and control the network.

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

3-The BSC, in charge of controlling several BTSs, is another example of an OAM function performed outside the OSS.

2.6 How Does It Work

2.6.1 Make Call

When the mobile user initiates a call, his equipment will search for a local base station, i.e. The BSS. Once the mobile has accessed, and synchronized with, a BTS the BSC will allocate it a dedicated bi-directional signaling channel and will set up a route to the Mobile services Switching Center (MSC).

2.6.2 Call Initialization

When a mobile requests access to the system it has to supply its IMEI (International Mobile Equipment Identity). This is a unique number, which will allow the system to initiate a process to confirm that the subscriber is allowed to access it. This process is called authentication. Before it can do this, however, it has to find where the subscriber is based. Every subscriber is allocated to a home network, associated with an MSC within that network. This is achieved by making an entry in the Home Location Register (HLR), which contains information about the services the subscriber is allowed.

Whenever a mobile is switched on and at intervals thereafter, it will register with the system; this allows its location in the network to be established and its location area to be updated in the HLR. A location area is a geographically defined group of cells. On first registering, the local MSC will use the IMSI to interrogate the subscriber's HLR and will add the subscriber data to its associated Visitor Location Register (VLR). The VLR now contains the address of the subscriber's HLR and the authentication request is routed back through the HLR to the subscriber's Authentication Centre (AC). This generates a challenge/response pair which is used by the local network to challenge the mobile. In addition, some operators also plan to check the mobile equipment against an Equipment Identity Register (EIR), in order to control stolen, fraudulent or faulty equipment.

2.6.3 Authentication

The authentication process is very powerful and is based on advanced cryptographic principles. It especially protects the network operators from fraudulent use of their services. It does not however protect the user from eavesdropping. The Time Division Multiple Access (TDMA) nature of GSM coupled with its frequency hopping facility will make it very difficult for an eavesdropper to lock onto the correct signal however and thus there is a much higher degree of inherent security in the system than is found in today's analogue systems. Nevertheless for users who need assurance of a secure transmission, GSM offers encryption over the air interface. This is based on a public key encryption principle and provides very high security.

2.6.4 Call Set-up

Once the network accepts the user and his equipment, the mobile must define the type of service it requires (voice, data, supplementary services etc.) and the destination number. At this point a traffic channel with the relevant capacity will be allocated and the MSC will route the call to the destination. Note that the network may delay assigning the traffic channel until the connection is made with the called number. This is known as off-air call set-up, and it can reduce the radio channel occupancy of any one call thus increasing the system traffic capacity.

2.6.5 Handover

GSM employs mobile-assisted handover. In this technique the mobile continuously monitors other base stations in its vicinity, measuring signal strength and error rate. These measurements are combined into a single function and the identities of the best six base stations are transmitted back to the system. The network can then decide when to initiate handover. The use of bit error rate, in addition to signal strength, adds considerably to the ability of the network to make informed handover decisions and is another example of the advantage of digital transmission over analogue. The BSC can initiate and execute handover if both BTS's are under its own control. In this instance the BSC can be considered as the manager of a specific group of radio frequencies for a geographic region and can control that resource to maximize its utilization. Alternatively and whenever handover must take place to a cell outside the control of the BSC, the MSC controls and executes handover.

CHAPTER THREE

The GSM RADIO INTERFACE

3.1 Introduction

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:

1-The band 890-915 Mhz has been allocated for the uplink direction (transmitting from the mobile station to the base station).

2-The band 935-960 Mhz has been allocated for the downlink direction (transmitting from the base station to the mobile station).

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.

3.2.1 FDMA and TDMA

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.

On the other hand, TDMA allows several users to share the same channel. Each of the users, sharing the common channel, are assigned their own burst within a group of bursts called a frame. Usually TDMA is used with a FDMA structure.

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 and 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 GSM Channel Structure

The GSM standard not only specifies then "when" of different channels in those different types of information is transmitted in different burst periods, frames, multi-frames super-frames etc.

It also distinguish the "why" of the information under the phrase of "logical channels", For example, it is not sufficient to identify between TCH and CCH. The GSM standard identifies the different types of CCH and TCH that are used.

Depending on the kind of information transmitted (user data and control signaling), we refer to different logical channels, which are mapped under physical channels (slots).

Digital speech is sent on a logical channel named TCH, which during the transmission can be an allocated to a certain physical channel. In a GSM system no RF channel and no slot is dedicated to a priori to the exclusive use of anything (any RF channel can be used for number of different uses).

Logical channels are divided into two categories:

I) Traffic Channels (TCHs)
ii) Control Channels.

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:

1-The traffic channels used to transport speech and data information.

2-The control channels used for network management messages and some channel maintenance tasks, We have already introduced the physical channels used in GSM, namely 8 burst periods per frame on an FDMA carrier.

We have also seen the need for the transmission of two distinct types of information between MS and BS, namely control (signaling) and user traffic information, This leads to the concept of two types of channels: Traffic Channel (TCH) used to convey user traffic information, Control Channels (CCH) used to convey signaling information between MS and network

Typically, burst period 0 in a frame is used (in both directions) as a CCH, Remaining seven burst periods in the TDMA are "nominally" TCHs, However, and this simple picture is not the complete picture.

We have already seen that the normal burst in a burst period which carries TCH can be "stolen" to carry specific types of "urgent" signalling information, Up to four consecutive frames can be stolen for this Fast Associated Control Channel (FACCH), For example, the 26 channel multi-frame structure applies to burst periods used as TCH, in this multi-frame structure, in frames 0 to 11; the burst period acts as a TCH, In frame 12, it acts as a means of transmitting specific type of control information (Slow Associated Control Channel - SACCH). In frames 13 to 24, it again acts as a TCH, in frame 25; it is actually unused to allow the MS to do other tasks.

Similarly, the 51 frame multi-frame used on burst period carrying certain CCH (e.g. burst period 0) is used in a similarly manner to separate when different "types" of signalling information (or channels) are transmitted

3.4.1 Traffic channels (TC)

A traffic channel (TCH) is used to carry speech and data traffic. Traffic channels are defined using a 26-frame multiframe, or group of 26 TDMA frames. The length of a 26-

frame multiframe 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. 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.

TCHs carry either encoded speech or user data in both up and down directions in a point-to-point communication.

There are two types of TCHs that are differentiated by their traffic rates.

1-Full Rate TCH

2-Half Rate TCH

Full Rate TCH (Also represented as Bm) It carries information at a gross rate of 22.82 Kbps, Half Rate TCH carries information with half of full rate channels.

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:

1- 24 frames are reserved to traffic.

2- 1 frame is used for the Slow Associated Control Channel (SACCH).

3- 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, TCH are also classified accord to the type of traffic that they are carrying

The main ones are:

1-TCH/F: Full rate speech codec traffic channel (1 per burst period)

2-TCH/H: Half rate speech codec traffic channel (2 per burst period)

3-TCH/n: n (e.g. 9.6, 4.8) kbps data traffic channel (1 per burst period).

3.4.2 Control Channels

Basic structure of Control channel

1	2	3	4	.	.	.	.	.	10	11	.	.	.	.	.					21						26

F	S	x	X	X	X	X	X	X	X	F	S	X	X	X	X	X	X	X	X	F	S	X	X

Figure 3.1 Basic structure of Control channel

Actually in the above diagram S will be at slot 1 of next frame, F is frequency correction channel, which occurs every 10^{th} burst. The next frame to S contains service operator's information. There are four important different classes of control channels defined:

1-Broadcast Channels (BCH)

2-Common Control Channels (CCCH)

3-Dedicated Control Channels (DCCH)

4-Associated Control Channels (ACCH)

Each class is further subdivided to identify specific "logical channels",

The mapping of these "logical" channels onto "physical" channels is quite complex but

some examples have already been mentioned

- Broadcast Channels

Which gives to the mobile station the training sequence needed in order to demodulate the information transmitted by the base station, Broadcast channels are transmitted by the base station to convey "information" to ALL MS in the cell Three different "logical" BCH exist information necessary for the MS to register in the system.

1- The Broadcast Control Channel (BCCH)

Which gives to the mobile station the parameters needed in order to identify and access the network. BCCH is a point-to-multipoint unidirectional control channel from the fixed subsystem to MS that is intended to broadcast a variety of information to MSs, BCCH has 51 bursts. BCCH is dedicated to slot1 and repeats after every 51 bursts.

Broadcast Control Channel (BCCH) continually broadcasts, on the downlink, information including base station identity, frequency allocations, and frequency hopping sequences. This provides general information per BTS basis (cell specific information) including information necessary for the MS to register at the system. After initially accessing the mobile, the BS calculates the requires MS power level and sets a set of power commands on these channels. Other information sent over these channels includes country code network code, local code, PLMN code, RF channels used with in the cell where the mobile is located, surrounding cells, hopping sequence number, mobile RF channel number for allocation, cell selection parameters, and RACH description. One of the important messages on a BCCH channel is CCCH_CONF, which indicates the organization of the CCCHs. This channel is used to down link point-to-multipoint communication and is unidirectional; there is no corresponding uplink. The signal strength is continuously measured by all mobiles which may seek a hand over from its present cell and thus it is always transmitted on designated RF channel using time slot 0(zero). This channel is never kept idle-either the relevant messages are sent or a dummy burst is sent.

2- Frequency correction channel (FCCH)

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 (FCCH) is used to allow an MS to accurately tune to a BS. The FCCH carries information for the frequency c orrection of M S downlink. It i s required f or the correct operation of radio system. This is also a point-to multipoint communication. This allows an MS to accurately tune to a BS.) conveys all information required by the MS to access and identify the network - transmitted in burst period 0 on only one (non-hopping) carrier in a cell The BCCH is a point-to-multipoint unidirectional control channel from the fixed subsystem to MS that is intended to broadcast a variety of information to MSs, including information necessary for the MS to register in the system. BCCH has 51 bursts. BCCH is dedicated to slot1 and repeats after every 51 bursts.

3- Synchronization channel (SCH)

Which gives to the mobile station the training sequence needed in order to demodulate the information transmitted by the base station (SCH) is used to provide TDMA frame oriented synchronization data to a MS. When a mobile recovers both FCCH and SCH signals, the synchronization is said to be complete. SCH repeats for every 51 frames. SCH carries information for the frame synchronization (TDMA frame number of the MS

And the identification of BTS). This is also required for the correct operation of the mobile.

The Synchronization Channel contains 2 encoded parameters:

1-BTS identifications code (BSIC)

2- Reduced TDMA frame number (RFN).

- Common Control Channels (CCCH)

A CCCH is a point-to-multipoint (bi-directional control channel) channel that is primarily intended to carry signaling information necessary for access management functions (e.g., a llocation of dedicated c ontrol c hannels). The CCCH channels help t o establish the calls from the mobile station or the network. Three different types of CCCH can be defined:

The CCCH includes:

1- paging channel (PCH)

Which is used to search (page) the MS in the downlink direction, The Paging Channel (PCH). It is used to alert the mobile station of an incoming cal

2- random access channel (RACH)

The Random Access Channel (RACH), which is used by the mobile station to request access to the network which is used by MS to request of an SDCCH either as a page response from MS or call origination/ registration from the MS. This is uplink channel and operates in point-point mode (MS to BTS).This uses slotted ALOHA protocol. This causes a possibility of contention. If the mobiles request through this channel is not answered with in a specified time the MS assumes that a collision has occurred and repeats the request. Mobile must allow a random delay before re-initiating the request to avoid repeated collision. It is used by MS when it attempts to request access to the network

3- access grant channel (AGCH)

Which is a downlink channel used to assign a MS to a specific SDCCH or a TCH. AGCH operates in point-to-point mode. A combined paging and access grant channel is designated as PAGCH. The Access Grant Channel (AGCH). It is used, by the base station, to inform the mobile station about which channel it should use. This channel is the answer of a base station to a RACH from the mobile station _Access Grant Channel (AGCH) is used by BS to tell MS which DCH to use after it has sent a message over the RACH

- Dedicated Control Channels (DCCH)

The Standalone Dedicated Control Channels (SDCCH) are allocated to specific mobiles to exchange information with the network for a specific duration

A typical use of the SDCCH would be to exchange signalling relating to a call set up.

A DCCH is a point-to-point, directional control channel. 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:

Two types of DCCHs used are:

1- Standalone DCCH (SDCCH)

Is used for system signaling during idle periods and call setup before allocating a TCH , for example MS registration, authentication and location updates through this channel.

When a TCH is assigned to MS this channel is released. Its data rate is one-eighth of the full rate speech channel which is achieved by transmitting data over the channel once every eighth frame. The channel is used for uplink and downlink and is meant for point-to-point usage, it is used in order to exchange signaling information in the downlink and uplink directions.

2- the slow associated control channels (SACCH)

Is data channel carrying information such as measurement reports from the mobile of received signal strength for a serving cell as well as the adjacent cells, This is necessary channel for the assisted over hand over function, is also used for power regulation of MS and time alignment and is meant for uplink and down link. It is used for point-to-point communication. SACCH can be linked to TCH or an SDCCH.

- Associated Control Channels

Two types of ACH, which have already been mentioned:

1-Slow ACH (SACCH) which is transmitted in the TCH burst period once every TCH multi-frame and is used for signalling of a non-urgent nature relating to the call (e.g. supplementary service and call related requests)

2-Fast ACH (FACCH) which is formed by "stealing" up to four consecutive TCH bursts (frames) to convey "urgent" signalling information (e.g. handover, power control, timing advance) 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.

It is a DCCH whose allocation is linked to the allocation of a CCH. A FACCH or burst stealing is a DCCH obtained by pre-emptive dynamic multiplexing on a TCH.

A FACCH is also associated to TCH. FACCH works in a stealing mode. This means that if suddenly during a speech transmission it is necessary to exchange signaling information with the system at a rate much higher than the SACCH can handle, then 20 ms speech (data) bursts are stolen for signaling purposes. This is the case at the case at the hand over. The user will not hear the interruption of the speech since it lasts only for 20 ms and cannot sensed by human ears.

3.5 Structure of TDMA Slot With a Frame

There are five different kinds of bursts in the GSM system. They are:

1-Normal Burst

2- Synchronization Burst

3-Frequency Correction Burst

4- Access Burst

5- Dummy Burst

3.5.1 Normal Burst

This burst is used to carry information on the TCH and on control channels. The lowest bit number is transmitted first. The encrypted bits are 57 bits of data or (speech + 1 bit stealing flag) indicating whether the burst was stolen for FACCH signaling or not. The reason why the training sequence is placed in the middle is that the channel is constantly changing. By having it there, the chances are better that the channel is not too different when it affects the training sequence compared to when the information bits were affected. If the training sequence is put at the beginning of the burst, the channel model that is created might not be valid for the bits at the end of a burst there are 8 training sequences shown at the diagram. The 26 bits equalization patterns are determined at the time of the call setup.

Tail Bits (TB) always equal (0,0,0), which has bit location from 0 to 2 and 145 to 147.

The Guard Period are the empty spaced bits and are used to synchronize the burst with exact accuracy and makes sure that different time.

3.5.2 Synchronization Burst

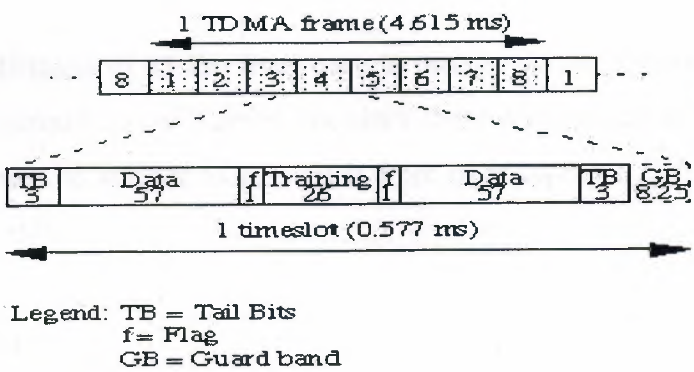

Figure 3.2 GSM TDMA structure and normal burst number of bits per field below the field legend

This burst is used for the time synchronization of the mobile. It contains 64 bit synchronization sequence. The encrypted 78 bits carry information of the TDMA frame number along with the BSIC. It is broadcast together with the correction burst. The TDMA frame is broadcast over SCH, in order to protect the user information against eavesdropping, which is accomplished is ciphering the information before transmitting. The algorithm that calculates the ciphering key uses a TDMA frame number as one of the parameters and therefore, every frame must have a frame number. By knowing the

TDMA frame number, the mobile will know what kind of logical channel is being transmitted on the control channel TS0. BSIC is also used by the mobile to check the identity of the BTS when making signal strength measurements (to prevent measurements on co-channel cells).

3.5.3 Frequency Correction Burst

This burst is used for frequency synchronization of the mobile. It is equivalent to an un-modulated channel with a specific frequency offset. The repetition of these bursts are called FCCH.

3.5.4 Access Burst

This burst is used for random access and longer GP to protect for burst transmission from a mobile that does not know the timing advance when it must access the system.

This allows for a distance of 35 km from base to mobile. Incase the mobile is far away from the BTS, the initial burst will arrive late since there is no timing advance on the first burst. The delay must be shorter to prevent it from overlapping a burst in the adjacent time-slot following this.

3.5.5 Dummy Burst

It is sent from BTS on some occasions as discussed previously which carries no information and has the format same as 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. Its structure is presented in figure 3.3.

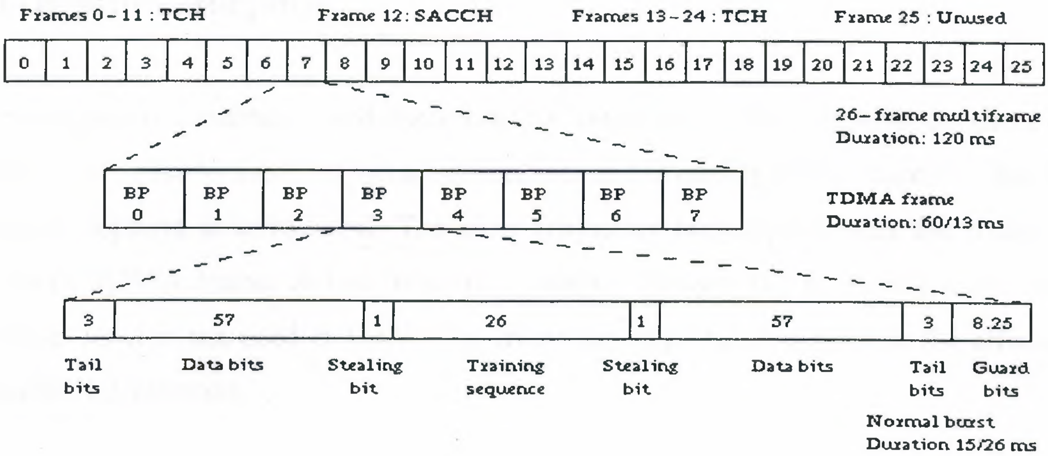

Figure 3.3 Structure of the 26-Multiframe, the TDMA frame and the normal burst

This figure has been taken, with the corresponding authorization, from "An Overview of GSM" by John Scourias (see Other GSM sites)

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 corresponds 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.

3.6 Frequency Hopping

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.

CHAPTER FOUR
CELL PLANNING

4.1 Introduction:

It was some time since the days of Heinrich Rudolf Hertz until the first real achievements of cellular radio. In the years 1887 and 1888, Hertz discovered that invisible waves which originated from an electric spark were able to transport *influence* or, as we call it today, *information* through the air. Only a few years later, this phenomenon was further investigated and developed until it was possible to actually transmit and receive signals over a distance of several kilometers. Guglieimo Marconi performed a dramatic demonstration of this several years later.

These early experiments formed the basis not only of cellular radio, but also of many types of transmissions. One merely has to think of early radio broadcasting, which was introduced in the early 1920s in the United States and Europe, to see how far these first experiments have taken society. Later applications for radio found quick and numerous paths to mass markets, even though the quality of the early AM transmissions were not very good by today's standards. The introduction of FM by Edwin H. Armstrong in 1929 was a breakthrough for quality of reception, and it became the standard for the remainder of the century. The current analog cellular networks are still based on Armstrong's FM.

Mobile radio applications took a longer and more halting path to their markets. In the days when the first transmitters started broadcasting, people were trying to make use of this technique for mobile applications, but they had a problem in that the transmitters were still very large. In the first applications for mobile radio, only the receiving system was mobile, similar to the paging systems, which are so popular today. There were experiments by police departments, which used only one high-power transmitter to cover a whole city. The called police officer had to get out of his car at the next public telephone to report back to his office for further instructions. This awkward procedure and the limited ability of the receiver to withstand the problems of propagation and road hazards were limiting factors for mobile radio.

When FM was introduced, the quality of received information increased a great deal, but the applications were still limited by transmitter size and the huge amounts of power consumed at the mobile end of the communications links by those early transmitters.

Commercial mobile phone service had to wait for the perfection of the public dispatch systems, such as police and other public safety applications. The breakthroughs were small, low-power transmitters (run from motor generators in the vehicle), and the move to higher operating frequencies (above 30 MHz) to further decrease the size and weight of mobile transmitters. An initial step toward viable mobile phone service appeared with the radio common carrier (RCC) and mobile telephone service (MTS) systems. These were simply conventional land mobile radios fitted with a special control panel, called a *control head,* which were suitable for commercial use by people who were unfamiliar with operating two-way radios. The RCC and MTS systems could direct calls from a single transmitter to a particular mobile, but remained, after all, simple dispatch systems in which the users set up all their calls through a mobile operator. Later, some additional inband tone signaling was added to the MTS system to make the newer improved mobile telephone service (IMTS), which automated to a considerable extent the interface between the mobile customer and the fixed telephone network. The mobile operator almost disappeared from the mobile phone landscape when IMTS was introduced. Cellular radio became popular only when carefully designed, engineered, and thoroughly tested systems like AMPS and TACS started to work.

4.2 Cellular Structure:

In the beginning of radio, engineers were happy to achieve a simple dedicated link between a transmitter and a receiver. These first links were not even two-way ones, but remained one-way dispatch links; that is, the people who called the mobiles did not get a response right away and did not even get a confirmation that their calls had reached the mobile addressees. The next step was to establish a two-way transmission link that allowed an immediate response. This came with mobile transmitters, but the structure of the network was simplistic and awkward to use. Service was limited to a certain area that could be reached with one transmitter or a small collection of transmitters on different channels at a single base site (Figure 4.1). We call the coverage area a *cell.* The cell or network size was determined by the transmitter's power. It was not possible to have a link between two different cells, or coverage areas, since an orderly means of directing traffic (voice audio) between transmitter sites and moving mobiles was missing. It was important to select the frequency of the transmitter and receiver in the cell carefully so that there was no interference from other systems, perhaps in the next town, which would interfere with the system's local operation.

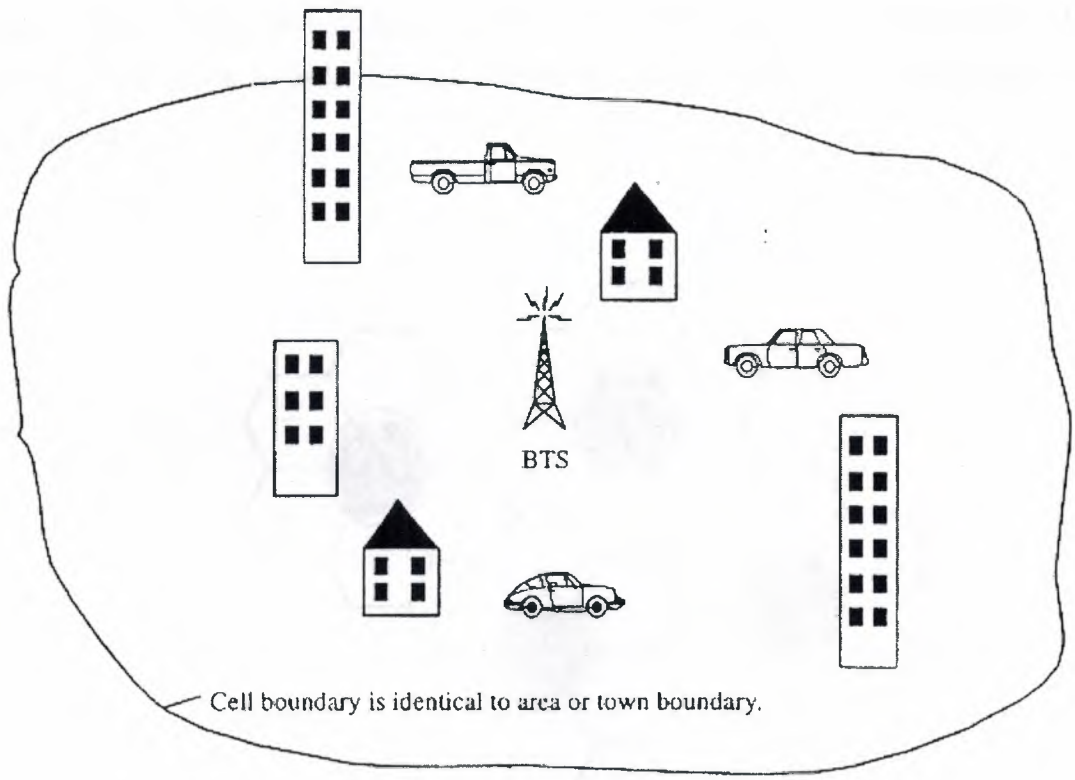

Figure 4.1 Single-Cell Structure

The disadvantage of this is obvious to everyone from today's perspective. A small set of frequencies was used for a huge area. The transmitters were so powerful that their operating frequencies could not be reused for hundreds of kilometers. This was a major limitation to the capacity of the system; once a channel was in use, the channel was tied up over the whole coverage area, even though the need for a mobile communications channel was confined to a small part of the network's service area. One could argue that capacity was not an issue in those days, for the mobile radios were expensive enough to limit the need for capacity below that of the technical limits of the system. Eventually the price of the mobile equipment dropped so low that the artificial capacity threshold was broken, and long waiting lists were common in the 1960s and 1970s for even rudimentary mobile phone service. A search for a solution continued in many countries. The possibility of allocating more frequency space was not a viable one. Other institutions and agencies needed spectrum too.

An idea was proposed to split the frequency band allocated to one cell among many cells, and has several cells coexist next to each other (Figure 4.2). The cellular structure was born. In order for this scheme to work properly, some restrictions had to be applied:

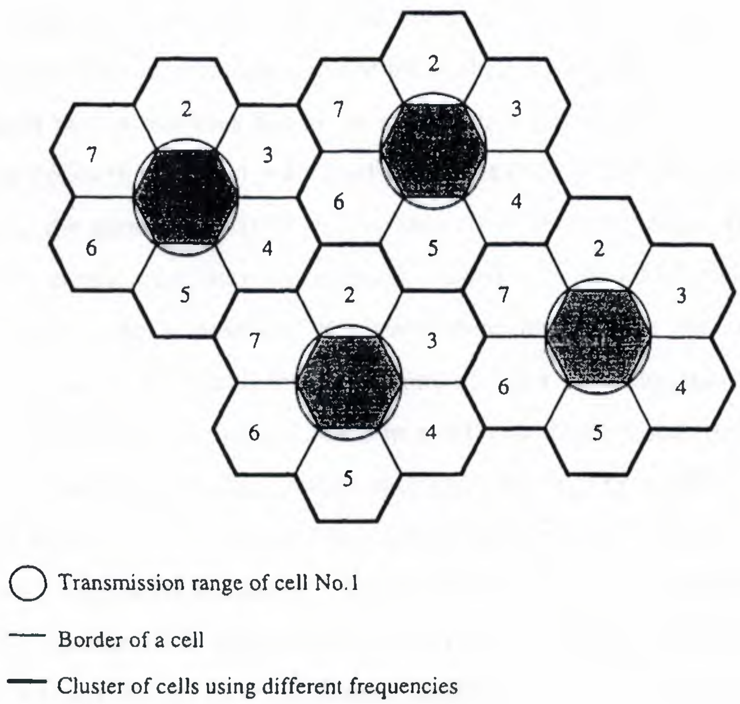

Figure 4.2 Cellular Structure

The frequencies had to be reused only within a certain pattern in order to reduce the interference between two different stations using the same channel. Neighboring cells could not share the same channels.

The power levels used within the single cells had to be carefully limited, again to reduce the interference between the different stations. Receiver filters had to be improved.

The pattern used for early systems was the seven-cell reuse pattern, which was a result of the distance required between cells using the same frequencies, yet again to preclude excessive interference. Interference had to be limited to some level that could be handled by the input filters of all the receivers in all the cells. Typically, a distance of about 2.5 to 3 times the diameter of an average cell had to be reserved between base site transmitters to guarantee that interference would not render the system useless. Calculations and experiments dictated this reuse pattern. If the systems were carefully designed and installed, more users could be accommodated as the same frequencies were used more and more times in the system.

In the early systems, it was not possible to roam among the cells. This meant that a user was not able to travel freely between cells while engaged in a single phone call. It was also not possible to place a call from the fixed network to a particular mobile station (MS) without knowing the exact position of the mobile. Each area had its own code, and a mobile station within this area had to be called with this code in a manner similar to the use of area codes in the fixed public network. The only difference is that in the fixed public network, the phones are fixed and the area codes do not change. The introduction of much more intelligence into the network, together with additional audio routing equipment, made roaming possible. Registers were installed in the network, which traced all the mobiles and stored their positions in order to route calls to them. These registers could be queried so that the audio in a call could be passed from cell to cell as needed. A single incidence of this process is called a handoff or handover, and a host of details within both the network and the mobile station itself need to be carefully coordinated for this process to happen reliably. Mobile stations, for example, have to be equipped with synthesized transmitters, which can change operating frequencies quickly. The network has to have sufficient equipment and signaling to make sure the handover or handoff is directed to the correct cell site

4.2.1 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

4.2.1.1 Macrocells:

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

4.2.1.2 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.

4.2.1.3 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 coverage of 360 degrees is not needed. In this case, a selective cell with coverage of 120 degrees is used.

4.2.1.4 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. 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.

4.3 Network Planning:

If one thinks of a country as varied in population density as the United States, it is easy to understand that it does not make sense to apply the same size to each cell. It makes a difference if an operator has to supply a big and densely populated city, such as New York, with a network, or a remote and sparsely populated area, such as the island of Hawaii. Different possibilities of network planning and cell planning have been developed:

Cell-splitting or microcell applications. As the number of subscribers grew larger, the density within these networks also became higher. The operators and radio engineers had to look for new capacity funds. A rather basic idea was to split the existing space into smaller portions, thus multiplying the number of channels available (Figure 4.3). Along with this simple scheme, the power levels used in these cells decreased, making it possible to reduce the size of batteries required for mobile stations. With the decreased power required for mobiles came decreased size and weight. This made the networks more attractive to new users.

Selective cells. It does not always make sense to have circular cells. Radio engineers designed cells with a wide variety of shapes, together with the required antennas, which are able to confine transmitted power within a particular area and exclude power from adjacent areas.

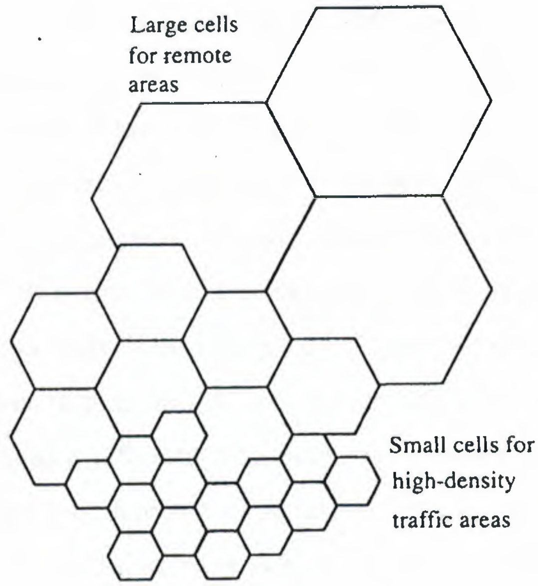

Figure 4.3 Cell Splitting And Microcells

The most common of these selective coverage schemes is the sectored cell, where coverage is confined to individual 120-deg sectors rather than the typical full 360-deg coverage (Figure 4.4). Such antennas may be located at the entrances of tunnels, on the edge of a valley, or at the ends of streets among skyscrapers.

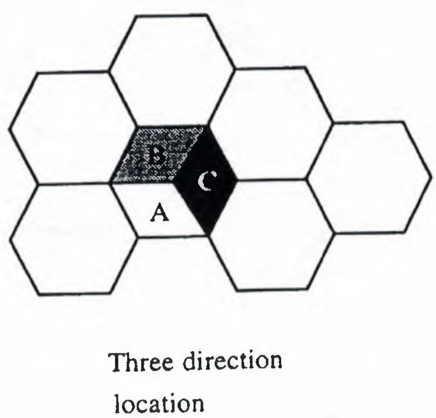

Figure 4.4 Selective Cells

Umbrella cells. When the cell-splitting technique was first applied, the operators realized that a freeway crossing within very small cells caused a large number of handovers among the different small cells. Since each handover requires additional work by the network, it is not particularly desirable to increase the number of such events. This is particularly true on European freeways, where the average speed is very high. The time a mobile on such a European freeway would stay in one cell decreases with increasing speed. Umbrella cells were introduced (Figure 4.5) to address this problem. In an umbrella cell, power is transmitted at a higher power level than it is within the underlying microcells and at a different frequency. This means that when a mobile that is traveling at a high speed is detected as a fast mover, it can be handed off to the umbrella cell rather than tie up the network with a fast series of handoffs. Such a mobile can be detected from its propagation characteristics or distinguished by its excessive handoff demands. In this cell, the mobile can stay for a longer period of time, thus reducing the workload for the network.

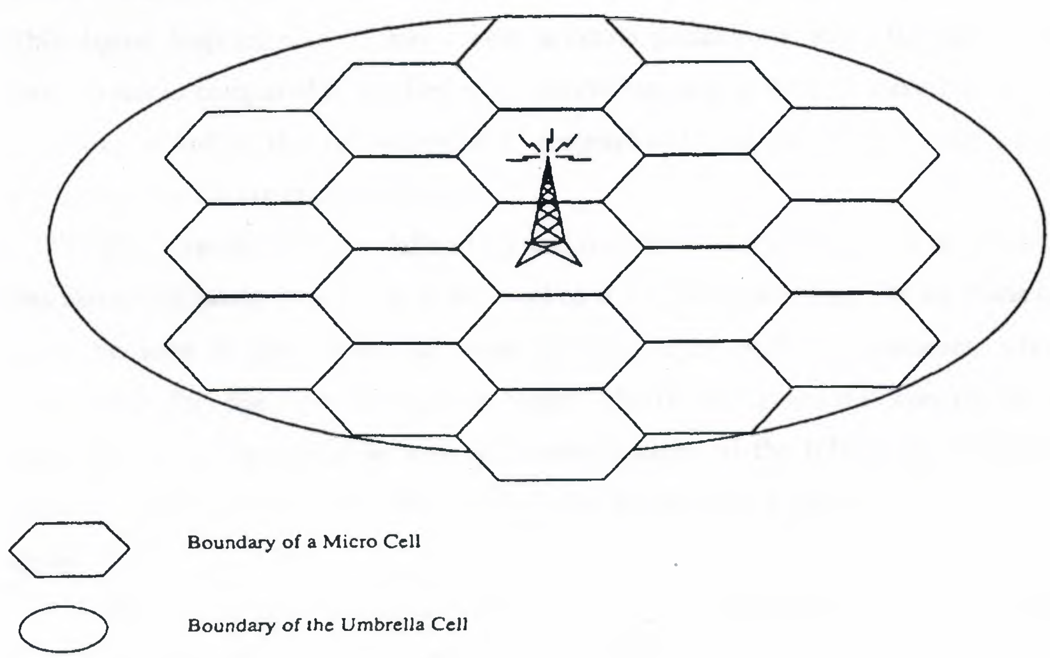

Figure 4.5 Umbrella Cells

4.4 Mobile Radio Network Planning Tasks:

The mobile radio network is the connecting element between the mobile telephone users and the fixed network.

In this network the base transceiver station equipment (BTSE) is the direct interface to the subscriber. It has to make radio communication channels available to the users and to care for a satisfactory signal quality within a certain area around the base station. This area may be split into different sectors (cells), which belong to one BTSE.

Planning a mobile radio network is a complex task. Because radio propagation along the earth surface is submitted to many influences due to the local environment. Furthermore the performance requirements to a radio network cover a wide field of applications, which depend on the operator's potentialities and goals. To respond to all these subjects, it is necessary to observe a certain sequence of tasks.

The first step is to get knowledge about the customers/operators objectives and resources (basic planning data). On this basis it is possible to estimate the size of the project and to establish a coarse nominal cell plan.

Then it is necessary to install a digital terrain database into a planning tool, which contains topographical and morphological information about the planning region. This digital map permits to make more accurate predictions about the radio signal propagation as compared to the first rough estimation, and to create a more realistic cell structure, including the recommendable geographical positions of the base stations equipment (coarse coverage prediction).

The network elements defined up to this moment have been found on a more or less theoretical basis. Now it has to be checked if the envisaged radio site locations may realty be kept A site survey campaign in accordance with the customer, who is responsible for the site acquisition, must clarify all Problems concerning the infrastructure and technical as well as financial issues of the BTSE implementation. Inside a tolerable search area the optimum site meeting all these issues has to be selected.

This site selection should also take into account particular properties of the area, e.g. big obstacles that are not recognizable in the digital maps.

Field measurements, to be carried out in typical and in complex areas must give detailed information about the radio characteristics of the planning region. The measurement results will then help to align the radio prediction tool for the actual type of land usage (tool tuning).

Now, fixed site positions and an area-adapted tool being available, it is possible to start the detailed radio planning. The final network design has to care for both sufficient coverage and proper radio frequency assignment In respecting the traffic load and the interference requirements.

The last planning step is the generation of a set of control parameters, necessary to maintain a communication while a subscriber is moving around. These parameters have to comply with the existing cell structure and the needs to handle the traffic load expected in each cell.

After commissioning of the network, the performance must be checked by the network operator by evaluation of statistical data collected in the operation and maintenance center. Situations of congestion or frequent call rejections may be treated by modification of the pertinent control parameters and lead to an optimized network. The individual planning steps are considered more closely in the following sections.

4.4.1 Collection of Basic Planning Data:

The requirements of the network operator concerning traffic load and service area extension are basic data for the design of a mobile network. A coarse network structure complying with these requirements can be created on this basis.
Two fundamental cell types are possible; their properties may be determined

a) By the maximum radio range of the involved transceiver stations and mobile terminals; the range is limited by the available transmit power and the noise figure of the receivers. This type is called a noise-limited cell; it is typical for rural regions.

b) Or it may be determined by the limited traffic capacity of a cell in the case of high subscriber concentration. This leads to the implementation of small cells, mainly in urban areas where interference will become the major problem.

The result of this first planning step is a rough estimate of the network structure, called a nominal cell plan, which gives knowledge about the number of radio stations, their required technical equipment and their approximate geographical positions. Thus allowing assessing the monetary volume of the project.

4.4.2 Terrain Data Acquisition:

Mobile communication occurs in a natural environment. The radio signal propagation is highly affected by the existing terrain properties like hills, forests, towns etc. Therefore the real mapping data must be taken into account by the planning tool.

Absorbing, screening, reflecting and diffracting effects of the surrounding objects and along the radio path influence the signal level encountered by a subscriber in the street.

To make realistic signal level predictions, the propagation models implemented in the prediction tool must be fed with the relevant terrain data.

A very important factor for correct modeling is the morph graphic classification of an area:

- Building heights and density of built up areas (metropolitan, urban, suburban, village, industrial. residential) or forest, parks, open areas, water etc.

The screening by hills, which may affect the coverage of a service area, must be made evident by consideration of the terrain profile (height contour lines).

The procurement of digital maps with this information may be rather expensive. The prediction accuracy is directly related to the size of area elements (resolution) and to the reliability of these information (obsolescence of maps!)

4.4.3 Coarse Coverage Prediction:

On the basis of the digital terrain database and by using standard propagation models, which have been preselected to fit for special terrain types, it is possible to make field strength predictions without having a very detailed knowledge of the particular local conditions.

By variation and modification of the site positions and antenna orientations, coverage predictions of rather good quality may be attained.

Yet the definitive site locations are subject to an Eater scheduled site selection process in accordance and by cooperation with the customer.

The particular local characteristics must be introduced later by comprehensive survey measurement. These measurements will be used to upgrade the propagation models.

4.4.4 Network Configuration:

The results of the "coarse prediction" steps will allow defining the radio network configuration and the layout of individual base stations.

A first frequency allocation plan may also be derived from these predictions. The result might already be a well functioning network. But it is still based on assumptions. The actual impact of the natural environment must be considered in the following steps. Nevertheless, the "coarse planning" results will help to better assess the special details brought in by the real situation.

In designing the radio network one has to keep in mind the requirements emerging from an increasing subscriber number. A multiple phase implementation plan has to govern the network configuration concepts.

In the initial phase a relatively low number of users has to be carried. On the other hand complete coverage of the service area has to be provided from the beginning. Existing sites of the first implementation phase must be useable in later phases. Increasing subscriber numbers (synonymous with increasing interference tendency!) should be responded by completion of the existing TRX-equipment and by addition of new sites. This means reconfiguration of the existing cell patterns and frequency reassignment. The planner should anticipate the future subscriber repartitions and concentrations from the beginning, in creating cell structures capable to respond to future needs,, increasing interference problems arising with higher site density may be overcome by down tilting of directional antennas initially mounted for maximum signal range, as now the radio cell areas will be smaller.

4.4.5 Site Selection:

The site positions found in the coarse planning process on a theoretical basis, must now be verified in a joint campaign, called site survey, between the customer and the radio network planner. All site candidates within a tolerable search area around the theoretical site positions must be checked.

This check includes the availability of electric power and of data transmission lines.

The most important topic is the possibility to install the antennas in a suitable height above the roofs or above ground.

Environmental influences (screening obstacles, reflectors) have also to be regarded. The best fitting site should be selected.

Another important task of this campaign is to declare a certain number of the radio sites be suitable to serve as „ survey sites". This means that radio field measurements shall be done with these stations as transmitters. The resulting measurements will be used for the alignment of radio propagation models.
The environment of the survey sites should be typical for a considerable number of other radio sites.

4.4.6 Field Measurements:

Digital terrain databases (DTDB) as derived from topographical maps or satellite pictures do not contain all details and particularities of the existing environment. Especially in fast developing urban areas maps cannot keep pace with reality and thus reflect an obsolete status. Keeping maps on this quality level would be very expensive.
The characteristics of built up zones and vegetation areas with respect to radio propagation differ in a wide range if we regard different countries. Even climatic conditions may influence the signal level. Knowledge about this specific behavior must be acquired by measurements.

The survey measurements have to be carried out in typical areas. Evaluation of these measurements will result in models that can be applied in comparable areas as well.

Special measurements must be carried out in very complex topographical regions where standardized propagation models will fail. The resulting models are valid exclusively for this measurement Zone.

4.4.7 Tool Tuning:

The measurement results have to be compared with the predictions of proven standard models. The standard parameters will be slightly modified to achieve minimum discrepancies with the measurements, i.e. to keep the mean error and rms-error as low as possible. As the signal level is subject to statistical variations, which cannot be predicted, the rms-error will never be zero.

The reliability of the created models increases with the number of measurement runs that can be exploited.

The new specific model may also be applied in other base stations located in similar environment.

4.4.8 Network Design:

The area-specific models are the basis for the final planning steps. The detailed network design has to care for

- A suitable signal level throughout the planning area
- Sufficient traffic capacity according to the operators requirements
- Assignment of the pertinent number of RF-carriers to all cells

Sufficient decoupling of frequency reuse cells to respect the interference requirements for co-channels and adjacent channels.

Moreover, attention has to be payed to an optimized handover scenario in heavy traffic zones.

The detailed planning process commits the final structure of the radio network and the configuration of the base stations.
The capacity of digital data links connecting the radio stations to the fixed network elements may now be defined.

4.4.9 Data Base Engineering:

A cellular network is a living system with moving subscribers. The service must be maintained while mobiles change radio cells and superior organization units, called location areas. Ail control parameters, necessary to support this task, have to be administered and supervised in central databases.

There is a permanent signaling information exchange between mobiles base stations and control centers.

This signaling communication occurs on predefined time slots, called control channels, which are assigned to one of the RF-carriers of each radio cell.

Important control information's for each radio cell are:

- Cell identification within the network
- Control carrier frequency
- Potential neighbor cells
- Minimum received signal level
- Maximum transmit power of a mobile
- Power reduction factor to perform power control
- Power margin for handover to neighbor cells

4.4.10 Performance Evaluation and Optimization:

Regular performance checks must be carried out after commissioning of the network. These checks comprise the evaluation of statistical data collected in the "operations and maintenance center" (OMC) as well as measurements by means of test mobile stations to explore e.g. handover events under realistic conditions; unwanted handover may lead to traffic congestions in certain cells, or may drain off traffic from other cells.

Detection of murtipath propagation problems-caused by big reflecting objects is also subject to measurements.

Another goal of these checks is to investigate the real traffic load and its distribution, as subscriber behavior in a living system will not necessarily reflect the original assumptions of the operator; assumed hot traffic spots may have been changed or shifted after a couple of years.

Careful evaluation of the measurement data will help to optimize the network performance by modification of the system parameters. As the number of subscribers will normally increase in course of time, supervision and control of these parameters should become a permanent maintenance procedure.

4.5 Radio Wave Propagation:

There are three main components of radio propagation:

- Mean path loss (loss due to distance between MS – BS),
- Shadowing (long term fading),

- Multi path propagation (short term fading).

4.5.1 Path Loss:

Standard path models are of the form:

$$L_m[dB] = A + B\log d[km]$$

Where L_m is the mean propagation path loss between the base station (BS) and the mobile station (MS) at a distance d.

A: unit loss at 1 km.

B: propagation index or loss per decade.

The propagation coefficients A and B depend upon :

- Transmit frequency,
- The MS and BS antenna height,
- The topography and morphology of the propagation area.

4.5.2 Shadowing – Long Term Fading:

In larger cells where the BS antenna is installed above the roof top level, details of the environment near the MS is responsible for a variation of the received level around the mean level calculated.

Usually this variation of level – caused by obstacles near the MS (e.g. building or trees)- is described by the statistical model, i.e. the total path loss L_{tot} is given by the mean "distance" path loss plus a random shadowing:

$$L_{tot}\,[\text{dB}] = L_m + \text{S}$$

S < 0: free line of sight,

S > 0: strong shadowing by e.g. a high building near the MS.

S has a Gaussian distribution (fig 4.6) with mean value 0and a standard deviation s which typically lies in the range s = 4...10dB.

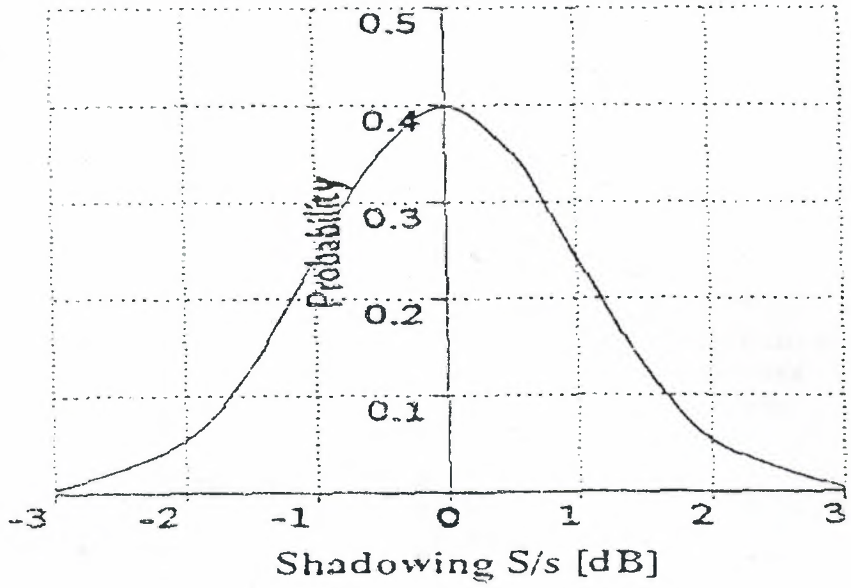

Figure 4.6 Gaussian distribution of Shadowing S

The length scale for variation of the long-term fading is in the 5...100m, i.e. the typical size of the shadowing obstacles.

4.5.3 Multi Path Propagation – Short Term fading:

The superposition of several reflected waves arriving at the receivers on different paths are therefore with different amplitudes and phases cause peaks (constructive superposition) and deep fading dips (destructive supervision) of the received level.

The length scale of variation (e.g. peak to peak) is given by the half of the transmission wavelength, i.e. about 15 cm for GSM 900 or 7.5 cm for DCS 1800.

The statistics of the Rayleigh is described in the following way:

Consider the received level due the path loss and long term fading, which is called local mean: $L_{loc}[dB]$.

4.6 Cellular Networks and Frequency Allocation:

One important characteristic of cellular networks is the re-use of frequencies m different cel(s. *By* re-using frequencies, a high capacity can be achieved. However, the re-use distance has to be high enough, so that the interference caused by subscribers using the same frequency (or an adjacent frequency) in another cell (fig 4.7 and 4.8) is sufficientty low.

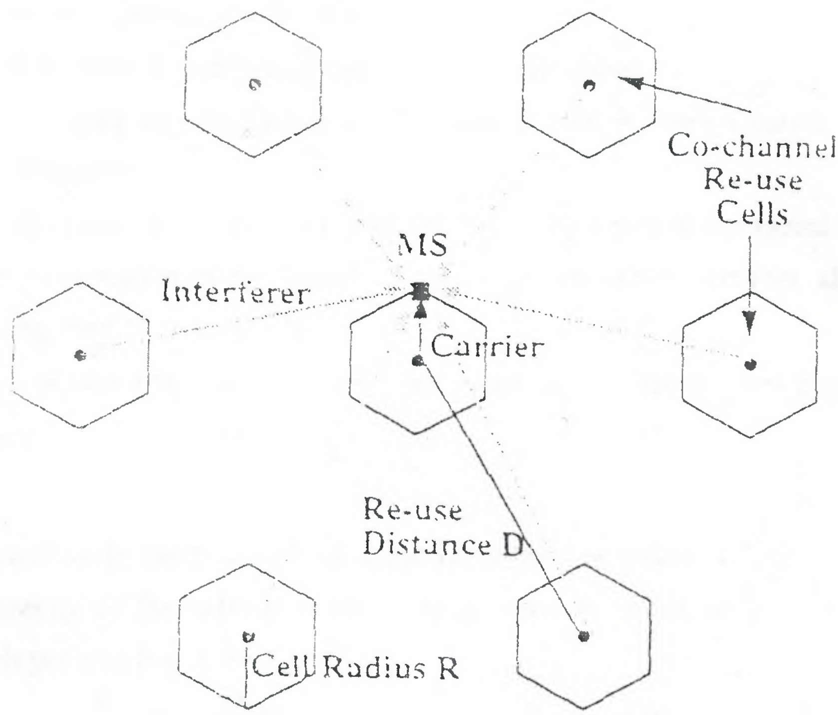

Figure 4.7 Cellular Network and Frequency Allocation

To guarantee an appropriate speech quality, the carrier-to-interference-power-ratio CIR has to exceed a certafn threshold CIR_{min} that is 9 dB for the GSM System.

For homogeneous hexagonal networks frequencies can J3e allocated to ceîls in a symmetric way. Defining the ciuster size K as gcoup of celis in which each frequency is used exactty önce, the fo!iow-ing reiatîons between Ciuster Size, Ceil Radius and Re-use Distance are obtained.

Inserung ine Tormula tor the ciuster size into the formula tor the minimum CIR one obtains:

$$0.5 \times B \log 3K > CIR_{min} + LTFM(\times\%) + 10 \log N_1$$

which gives a lower bound for the cluster size which can be used.

For a gıven cluster size K and total number of frequencies N_{tot}, the number of frequencies per cell N_{cell} is gıven by:

$$N_{cell} = N_{tot} / K$$

i.e. the capacity of a cell can be increased by reducing the cluster size.

A reduction of **cluster** size can be achieved by

- Reducing the number of interferers → Sectorisation.
- Reducing the interference from co-channel cells → Power Control, Discontinued Transmission. ...

Obviousiy a real netvvork does not have such a regular hexagonal structure and frequency allocation is performed by planning tools using comptex algorithms for optimizing the CIR in each cell.

The objective is to achieve a high mean value of frequencies per cell $<N_{cell}>$. The ratio:

$$<K> = N_{tot} / N_{cell}$$

can viewed as the mean cluster size in such an inhomogeneous envjronment.

The capacity of the radio netvvork depends upon the available number N of radio channels per area F (e.g. F= 1 km^2).

$$\frac{N}{F} = N_{cell} \times \frac{N_{BTS}}{F} = CPF \times \frac{N_{tot}}{K} \times \frac{1}{F/N_{BTS}} = CPF \times \frac{N_{tot}}{K} \times \frac{i}{CA}$$

N_{BTS} : number of BTS

CA: ceil area

CPF: channel per frequencies

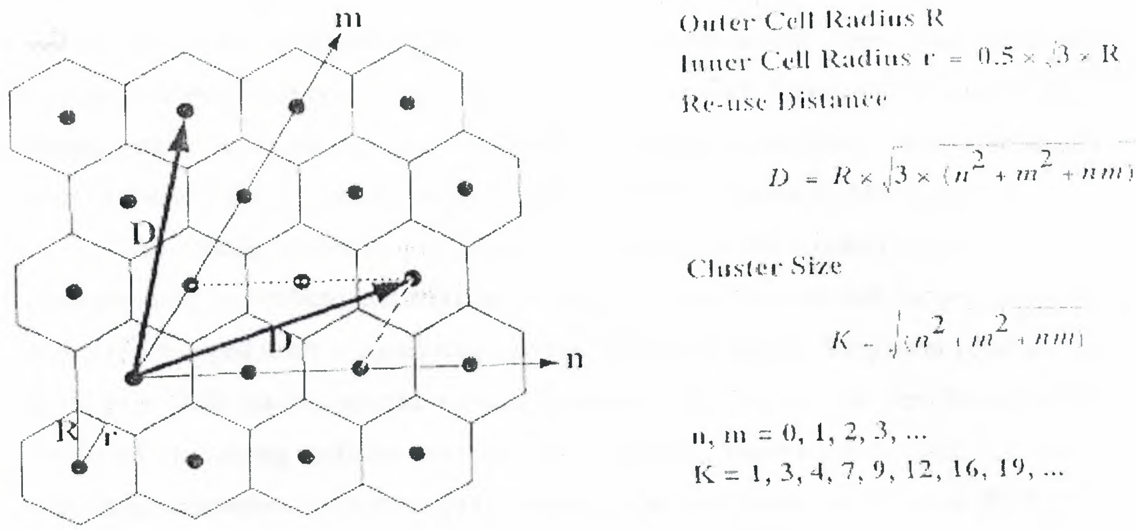

Figure 4.8 Frequency re-Use and Cluster Size.

4.7 Handover / Handoff:

The *handover* or *handoff* procedure is a means to continue a call even when a mobile station crosses the border of one cell into another. As mentioned earlier, the handover or handoff technique, from one cell to another, finally made the mobile station really mobile. Before the introduction of this feature, a call was simply dropped when the cell border was crossed or when the distance between the mobile station and one particular base station became too large.

In a cellular network, one cell has a set of neighboring cells. The system, therefore, has to determine which cell the mobile station should be passed to. The method used to determine the next cell to use differs in analog and digital systems. The difference in the procedure can be determined from the different names. The handoff comes from the analog world, whereas handover was introduced by GSM. The term *handover* will be used when talking about the GSM system, and the term *handoff* will be used when talking about analog systems.

In analog systems, the base station monitors the quality of the link between a mobile station and itself. When the base station realizes that the quality of the link has degraded and the distance to the mobile station has become too large, it requests the the adjacent cells to report the power level they see for the mobile back to the network. It is reasonable that the strongest reported power level for the mobile comes from the closest cell to the mobile station. The network then decides which frequency channel the base station should use in the new cell and which corresponding frequency the mobile should tune to. Eventually, the mobile station is commanded to perform a channel change.

The mobile station is the passive participant in the handoff process. All the measurements and subsequent work are done in the base stations and the network. Cell sites are equipped with a *measuring receiver* used to measure the power level of the different mobile stations on the various frequency channels in use. For those readers interested in analog cellular systems, the distance measurements within cells is sometimes determined from the relative phase of the *supervisory audio tones* (SAT) that the mobiles transponder back to the base stations. The distance is half the time of the phase shift multiplied by the propagation speed of the signal.

The situation in the GSM system is different. The mobile station must continuously monitor the neighboring cell's perceived power levels. To do this, the base station gives the mobile a list of base stations (channels) on which to perform power measurements. The list is transmitted on the base channel (again, system information), which is the first channel a mobile tunes to when it is turned on. The mobile station performs continuous measurements on the quality and the power level of the serving cell, and of the power levels of the adjacent cells. The measurement results are put into a *measurement report,* which are periodically sent back to the base station. The base station itself may also be performing measurements on the quality and power of the link to the mobile station. If these measurements indicate the necessity for a handover, such can be performed without delay, as the appropriate base station for a handover is already known. The measurements are coming in constantly, and they reflect the mobile's point of view. It is up to the operator to act upon different quality or power levels, and the handover constraints or thresholds can be adjusted in accordance with changing environment and operating conditions.

The GSM system distinguishes different types of handovers. Depending on what type of cell border the mobile station is crossing, a different entity may have to control the handover to ensure that a channel is available in the new cell. If a handover has to be performed within the area of a BSC, it can be handled by the BSC without consulting

MSC, which, in any case, must at least be notified. This type of handover Is called a simple handover between BTSs (Figure 4.9).

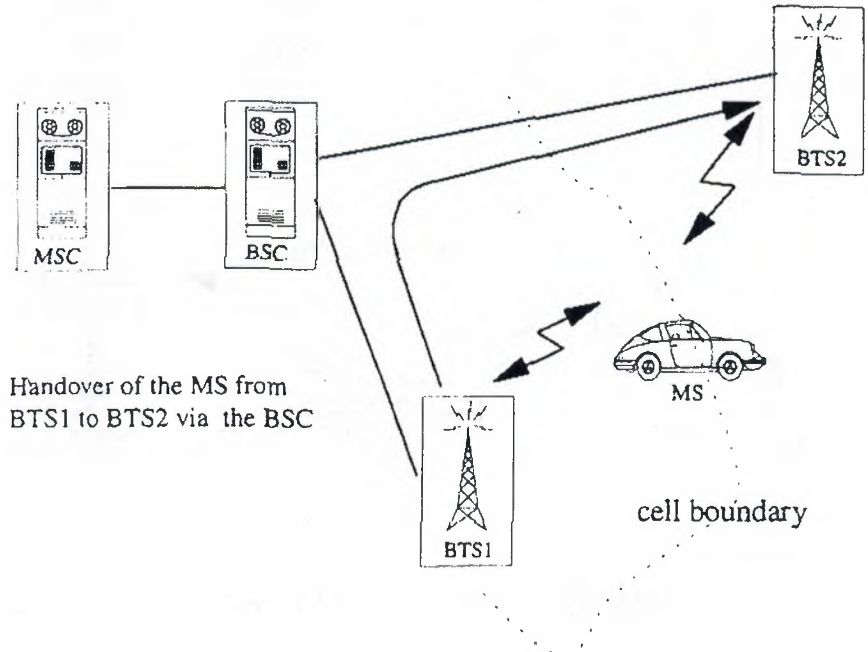

Figure 4.9 Handover Between BTSs

If, instead, a mobile station is crossing the border of a BSC (rather than a BTS), then the MSC has to control the procedure in order to ensure the smooth transition of the conversation. This can be continued for a handover between two MSCs (Figure 4.10). The only difference, in this latter case, is that even though the mobile is eventually handled by the second MSC, the first MSC still has to maintain control of the call management.

In theory, it is possible to perform a handover at a political border between two countries. There are no technical restrictions to this feature. Due to the different roaming agreements, however, it is not possible to start a phone call, let us say, in Germany, and cross the border to Switzerland and still continue the call. The call will be dropped, and subscribers have to register themselves in the new foreign network.

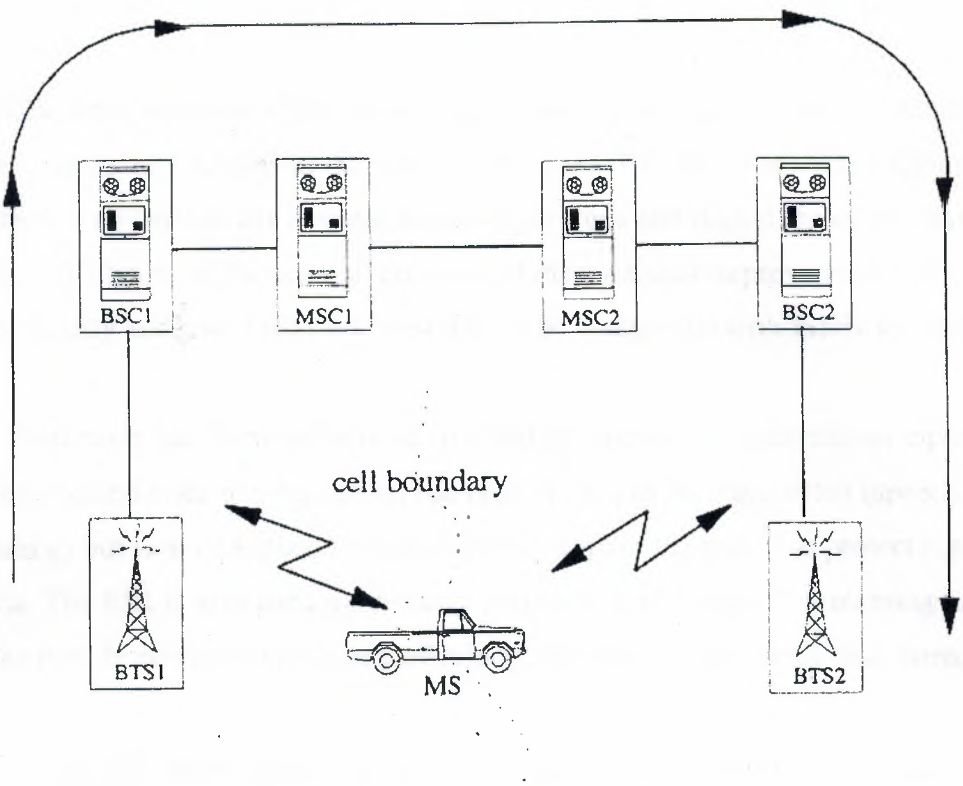

Figure 4.10 Handover Between MSCs

CONCLUSION

The developers of GSM chose digital system, as opposed to the standard analog cellular systems like AMPS in the United States and TACS in the United Kingdom. They had faith that advancements in compression algorithms and digital signal processors would allow the fulfillment of the original criteria and the continual improvement of the system in terms of quality and cost. GSM was designed to be compatible with ISDN services.

Protection has been introduced in GSM by means of transmission ciphering. The ciphering method does not depend on the type of data to be transmitted (speech, user data or signaling) but is only applied to normal bursts; Ciphering is used to protect signaling and user data. 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.

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 specification of the radio interface has then an important influence on the spectrum efficiency. 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.

All information must be provided on the levels of RF radiation from RF transmitter towers (base stations) to which members of the public may be exposed. Reviews on the potential health risks of RF radiation are available elsewhere.

REFERENCES:

[1] Gunnar Heine, Mobil Communication Series ,1998.

[2] Haug T .The GSM Program a Pan-European Effort. Proceeding of the Mobil Radio Conference.Nice,November,1991.

[3] Parsons J.D., Jardine D., Gardiner J.G. Mobil Communication System Blackie, Halsted (New York), 1989.

[4] Rhee Man Young. Cellular Mobil Communication and Network Security. Prentice Hall International Editions, 1999.

[5] MOTOROLA LTD., Training Department Cellular Infrastructure Group, Introduction to Digital Cellular, Edition one 1997.

[6] D. M. Balston. The pan-European system: GSM. In D. M. Balston and R.C.V. Macario, editors, Cellular Radio Systems. Artech House, Boston, 1993.

[7] David M. Balston. The pan-European cellular technology. In R.C.V. Macario, editor, Personal and Mobile Radio Systems. Peter Peregrinus, London, 1991.