NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Electrical and Electronic Engineering

GSM Networks

Graduation Project
EE- 400

Student:	Ahmad Gharaibeh(20033542)
Supervisor:	Dr Jamal Fathi

Nicosia - 2007

ACKNOWLEDGEMENT

Firstly I would like to thank my supervisor Dr. Jamal Fathi, he was very helpful with me to complete the project. He gave me too much information, advises, comments and endless effort in preparation for this project.

Secondly I offer special thanks to my parents and my brothers, who encouraged me in every field of life and try to help whenever I needed. They enhanced my confidence in myself to make me able to face every difficulty easily. I am also grateful to my mother whose prayers and my father whose words for me had made this day comes true. And because of them I am able to complete my work

I would also like to pay my special thanks to my all friends who helped me and encouraged me for doing my work. Their reluctance and friendly environment for me has helped me allot. I want to thank them as they contributed their time and provided very helpful suggestions to me.

TABLE OF CONTANTS

INTRODUCTION

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

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 Grouped 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.

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 interworking between the different elements of the GSM system. In 1990, the phase I of the GSM specifications were published but the commercial use of GSM did not start until mid-1991.

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

Table : 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 charts the different mobile cellular systems developed since the commercial launch of cellular systems.

Table : 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>

CHAPTER ONE
1.SYSTEM ARCHITECTUTE of GSM

1.1 Overview

Like all modern mobile networks, GSM utilizes a cellular structure as illustrated in Figure 1.1. The basic idea of a cellular network is to partition the available frequency range, to assign only parts of that frequency spectrum to any base transceiver station, and to reduce the range of a base station in order to reuse the scarce frequencies as often as possible. One of the major goals of network planning is to reduce interference between different base stations.

Anyone who starts thinking about possible alternatives should be reminded that current mobile networks operate in frequency ranges where attenuation is substantial. In particular, for mobile stations with low power emission, only small distances (less than 5 km) to a base station are feasible.

Besides the advantage of reusing frequencies, a cellular network also: comes with the following disadvantages:

- An increasing number of base stations increase the cost of infrastructure and access lines.
- All cellular networks require that, as the mobile station moves, an active call is handed over from one cell to another, a process known as handover.
- The network has to be kept informed of the approximate location of the mobile station, even without a call in progress, to be able to deliver an incoming call to that mobile station.
- The second and third items require extensive communication between the mobile station and the network, as well as between the various network elements.

That communication is referred to as signaling and goes far beyond the extent of signaling that fixed networks use. The extension of communications requires a cellular network to be of modular or hierarchical structure. A single central computer could not process the amount of information involved.

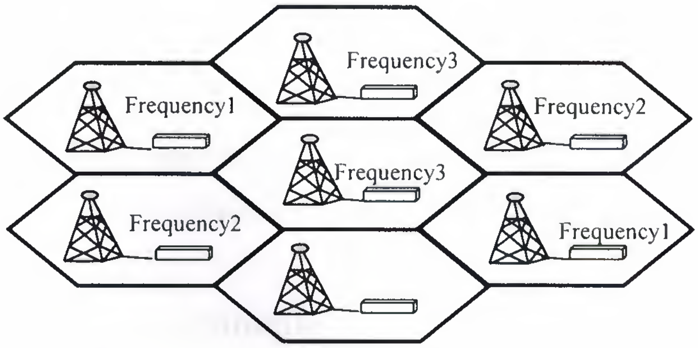

Figure 1.1 The Radio Coverage of an Area by Single Cells

1.2 An Overview on the GSM Subsystems

A GSM network comprises several elements: the mobile station (MS), the subscriber identity module (SIM), the base transceiver station (BTS), the base station controller (BSC), the transcending rate and adaptation unit (TRAU), the mobile services switching center (MSC), the home location register (HLR), the visitor location register (VLR), and the equipment identity register (EIR). Together, they form a public land mobile network (PLMN). Figure 1.2 provides an overview of the GSM subsystems.

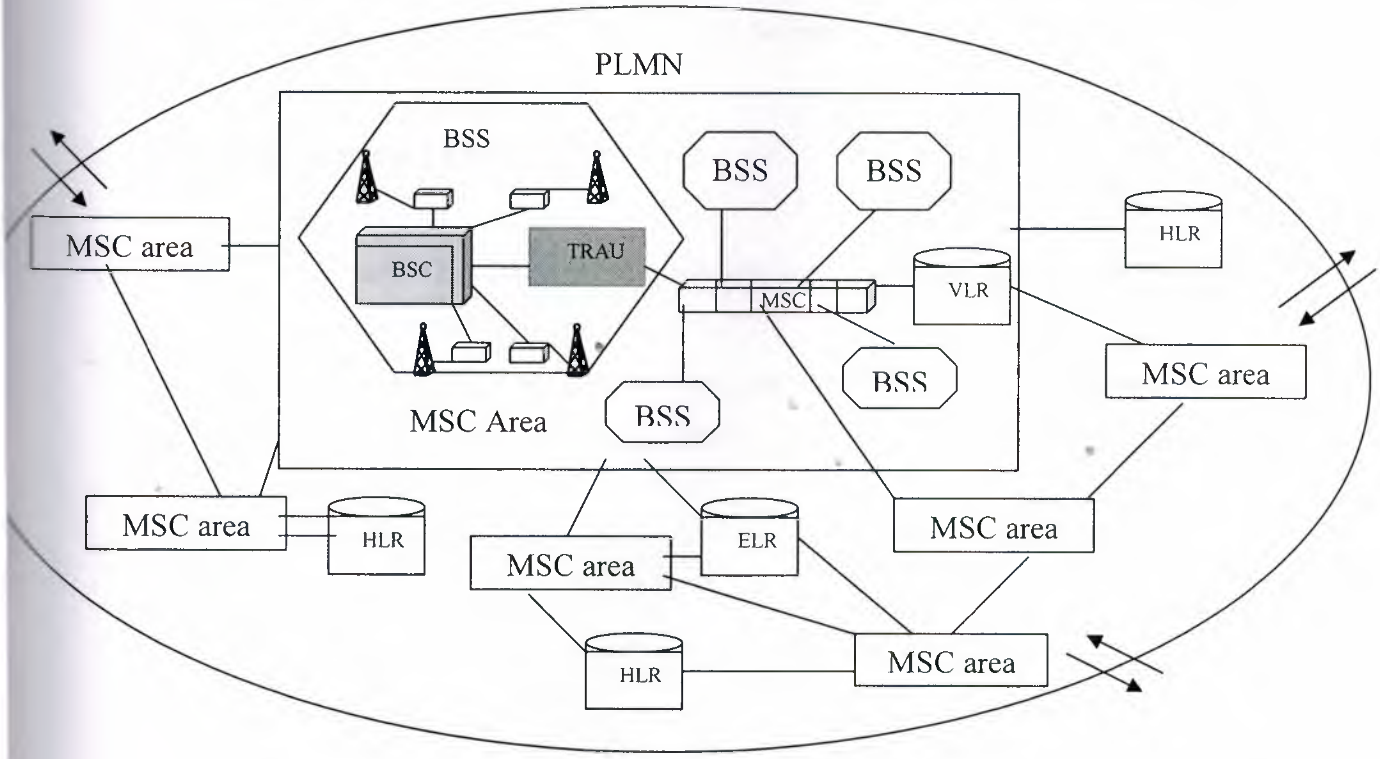

Figure 1.2 The Architecture of a PLMN

1.3 Mobile Station

GSM-PLMN contains as many MSs as possible, available in various styles and power classes. In particular, the handheld and portable stations need to be distinguished.

1.4 Subscriber Identity Module

GSM distinguishes between the identity of the subscriber and that of the mobile equipment. The SIM determines the directory number and the calls billed to a subscriber. The SIM is a database on the user side. Physically, it consists of a chip, which the user must insert into the GSM telephone before it can be used. To make its handling easier, the SIM has the format of a credit card or is inserted as a plug-in SIM. The SIM communicates directly with the VLR and indirectly with the HLR.

1.5 Base Transceiver Station

A large number of BTSs take care of the radio-related tasks and provide the connectivity between the network and the mobile station via the Air-interface.

1.6 Base Station Controller

The BTSs of an area (e.g., the size of a medium-size town) are connected to the BSC via an interface called the Abis-interface.

The BSC takes care of all the central functions and the control of the subsystem, referred to as the base station subsystem (BSS). The BSS comprises the BSC itself and the connected BTSs.

1.7 Transcoding Rate and Adaptation Unit

One of the most important aspects of a mobile network is the effectiveness with which it uses the available frequency resources. Effectiveness addresses how many calls can be made by using certain bandwidth, which in turn translates into the necessity to compress data, at least over the Air-interface. In a GSM system, data compression performed in both the MS and the TRAU. From the architecture perspective, the TRAU is part of the BSS. An appropriate graphical representation of the TRAU is a black box or, more symbolically, a clamp.

1.8 Mobile Services Switching Center

A large number of BSCs are connected to the MSC via the A-interface. The MSC is very similar to a regular digital telephone Exchange and is accessed by external networks exactly the same way. The major tasks of an MSC are the routing of incoming and outgoing calls and the assignment of user channels on the A—interface.

1.9 Home Location Register

The MSC is only one sub center of a GSM network. Another sub center is the HLR, a repository that stores the data of a large number of subscribers. An HLR can be regarded as a large database that administers the data of literally hundreds of thousands of subscribers. Every PLMN requires at least one HLR.

1.10 Visitor Location Register

The VLR was devised so that the HLR would not be overloaded with inquiries on data about its subscribers. Like the H LR, a VLR contains subscriber data, but only part of the data in the HLR and only while the particular subscriber roams in the area for which the VLR is responsible. When the subscriber moves out of the VLR area, the HLR requests removal of the data related to a subscriber from the VLR. The geographic area of the VLR consists of the total area covered by those BTSs that are related to the MSCs for which the VLR provides its services.

1.11 Equipment Identity Register

The theft of GSM mobile telephones seems attractive, since the identities of subscribers and their mobile equipment are separate. Stolen equipment can be reused simply by using any valid SIM.Barring of a subscriber by the operator does not bar the mobile equipment .

To prevent that kind of misuse, every GSM terminal equipment contains a unique identifier, the international mobile equipment identity (IMEI). It lies within the realm of responsibilities of a network operation to equip the PLNM with an additional database, the EIR, in which stolen equipment is registered and so can he used to bar fraudulent calls and even, theoretically, to track down a thief (by analyzing the related SIM data).

1.12 GSM Base Station Measurements And It's Methods

In recent years there has been a proliferation of base station towers designed to meet increased demands placed on mobile telephone networks by the growing number of mobile phone users .In parallel with the construction of these base station towers there has been an increase in community concern about possible health effects from the radio frequency (RF) radiation emissions from the towers.

The Australian Government Committee on Electromagnetic Energy (EME) Public Health Issues (CEMEPHI), as part of the public information component of its RF EME program, considers it important that the general public be informed about the RF EME levels to which they may be exposed. Accordingly, the CEMEPHI requested the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA) to carry out a survey of the RF EME levels in the vicinity of mobile telephone base stations.

This report provides information 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 (e.g., UNEP/WHO/IRPA, 1993; Barnett, 1994; McKinley etal, 1996; ICNIRP, 1998; Repacholi, 1998; Byrus et al., 1999).

A survey on RF EME in and around five Vancouver schools by Thansandote et al. (1999), Both at indoor and outdoor sites, yielded power density measurements well within Canada's safety code limits (Safety Code 6, 1990).

Signal sources investigated in the Thansandote et al survey included base station frequency bands for analog cellular phones and personal communication services (PCS – the new generation of digital cellular phone), as well as AM radio, FM radio and TV broadcasts. A US study by Petersen and Testagrossa (1992) characterized RF EME fields in the vicinity of several frequency modulated (FM) cellular radio antennae towers, at heights varying from 46 to 82 meters.

They reported maximum power densities considered representative of public exposure levels to be less than 0.0001 W/m 2 per transmitter. Hence, in a worst-case scenario of 96 transmitters operating at an Effective radiated power (ERP) of 100 watts per transmitter; the aggregate maximum power density was estimated by Petersen and Testagrossa to be below 0.01 W/m^2. In Poland, where the maximum permissible power density value is 0.1 W/m^2 at relevant base station.

Frequencies, measurements of electromagnetic fields (EMF) in the surrounds of 20 GSM base stations showed that 'admissible EMF intensities at the level of people's presence, in existing buildings, in surroundings of base stations and inside buildings with antennas, were not exceeded' (Aniolczyk, 1999, p.57).

The purpose of the work reported here is to provide data on RF EME levels at independently nominated sites, over the range of the digital Global System for Mobile communication (GSM) mobile telephone base stations frequency band (935 – 960 MHz), and to make comparisons with the limit for non-occupational exposure specified in the relevant Australian exposure standard. The Radio communications (Electromagnetic Radiation Human Exposure) Standard 1999 adopted by the Australian Communications Authority (ACA) requires mobile phones and mobile phone base stations to comply with the exposure limits in the interim Australian and New Zealand Standard 2772.1(Int): 1998 which has now been withdrawn by

Standards Australia. The ACA standard is subsequently abbreviated as ACAS in this publication. The non-occupational exposure limit specified in the ACAS, expressed in terms of power flux density, is 2 W/m^2 (equivalent to 200 $\mu W/cm^2$) for frequencies between 10 MHz and 300 GHz, averaged over a 6 minute period. It should be noted that the exposure limits in the ACAS were 'developed on the basis of there being a threshold of 4 W/kg whole body specific absorption rate (SAR) before any adverse health consequences are likely to appear' (ibid, p.13). However, because the SAR (units W/kg) is difficult and often impractical to measure, the ACAS provides derived levels of electric (E) and magnetic (H) field strengths, as well as the equivalent plane wave power flux densities (S), which are more readily measured.

Although the primary focus of the ARPANSA study was to measure the RF EME emission levels from GSM base stations, fixed site environmental measurements from other RF EME sources were also recorded, including the analog mobile phone system (AMPS), VHF TV UHF TV, AM radio, FM radio and Paging.

1.12.1 Method of Measurement Locations

Measurements were performed at fourteen different locations throughout Australia. Two localities were chosen from each state, and the Northern Territory. In most instances the sites were chosen by local governments, who were asked to nominate two mobile telephone base stations sites in major population centers that were of concern to local communities. Security of monitoring equipment for the 24-hour data-logging component was taken into account in the final selection of the measurement sites. Following the nature and type of the measurements required.

- Fixed Site Environmental Measurements

Broadcast communication sources such as television, and both AM radio and FM radio, are usually transmitted at high powers from a single base facility. Such sources have very extensive areas of effective reception frequently extending to many hundreds of kilometers from a single station transmitter. Furthermore, for such sources and considering their necessary broadcast design requirements, we do not expect to encounter significant or strong variations in signal strength in relatively open areas surrounding a mobile telephone base station. Given the nature and emphasis of our study we therefore adopted a protocol of making a single set of static environmental measurements for all broadcast sources other than mobile telephone base stations.

Buildings or other likely objects may significantly attenuate or scatter the RF signal. Hence, where possible, measurements were made in locations that maintained direct line-of-sight with known RF sources, at a height of 1.7 meters above ground, in open areas in the near vicinity of the GSM base station of interest. Measurement antenna were oriented to obtain a maximum signal strength for the particular frequency band Being measured. The environmental RF EME signals were measured at a location within 500 meters of the base station.

Measurement of such fixed site environmental RF EME levels involved investigating a number of different RF EME sources. These included GSM, AMPS, VHF TV, UHF TV, AM radio, FM radio and paging. All signals with power densities greater than 1% of the observed maximum for each frequency band were recorded individually. Other signals, such as emergency services (police, ambulance, etc.) and taxis, were rarely detected and are not included in this summary report. To measure the environmental RF EME levels the average RF EME levels over a six minute scanning period during the day was determined. The time taken to record all the relevant sources of environmental RF EME at each site was approximately one hour. A spectrum analyzer was used and some transient signal sources,Such as paging services, may have gone undetected if by chance the relevant frequency band was not swept by the spectrum analyzer when the signal was transmitted.

- GSM Base Station Activity Measurements

The primary aim of this study was to determine the RF EME level resulting from all signal frequencies produced by the particular GSM base stations under survey. Mobile telephone communication signals are both transient and partly random in their occurrence and distribution. In this context, we were interested in determining the RF EME levels at many locations and more particularly, we wanted to estimate both maximum and minimum levels and also the long term average value for each location and to map such levels in the area surrounding the base station. Because telephone communications are based on human activity,

A diurnal signal pattern is generally observed. Site-specific GSM mobile telephone exposure levels were therefore monitored over a 24-hour period. Relevant spectrum analyzer data were recorded automatically under PC control and subsequently analyzed to determine both the temporal and daily average activity. Measurements were performed within a single sector, at a fixed location close to the base station, by continuously scanning the frequency bands and logging the signal level for the GSM mobile phone systems. The recorded data were used to determine the temporal activity for the GSM systems over the 24-hour period.

The activity level of the data samples was determined by counting the number of simultaneous active time slots for a single carrier base station. For the majority of GSM base stations there is a possible minimum of eight and a possible maximum of thirty-two time slots for any given sector.

Hence, eight time slots will amount to 25% of the total activity possible from the transmitting antenna of a single carrier GSM base station.

The digital GSM base stations produce carrier frequencies between 935 to 960 MHz (analog AMPS system operates at 870 to 890 MHz). The GSM system transmits data in bursts of 0.6μsec with a repetition rate of 217 Hz. The temporal RF EME levels of the transmitting antennae at GSM base stations were analyzed to identify control frequencies or additional carrier frequencies. For GSM the frequency range investigated was divided up into three sub-bands, with the sampling order of each sub-band and frequency randomized to avoid bias. The system was optimized to gather as much data as possible by sampling more often when fewer frequencies were detected. Post logging data analysis was performed to determine the average activity over a six-minute scanning period, yielding an activity value for every six minutes of the day. The analysis software included only the signals identified as belonging to the base station in question. Where more than one carrier (Telstra, Optus or Vodafone) shared the same tower, the combined activity from all carriers was determined. A diurnal correction factor was derived from analysis of the 24-hour activity measurements for use in mobile measurements.

- Mobile GSM Base Station Area Measurements

A fixed antenna was roof mounted on a car and automated mobile measurements were made whilst driving around the streets near the GSM base station under survey. Both signal data and position information [using Global Positioning System (GPS)] were recorded. For technical reasons, we were not able to make simultaneous measurements of all frequencies at each particular mobile measurement sample location. However, for each base station sector there is always a single "control frequency" present and this frequency is produced at a constant transmitter power. The control frequency is broadcast from the same antennae as additional transient carrier frequencies. In addition, the control frequency will have similar propagation characteristics to those of any additional frequencies. Hence, to determine the RF EME area levels, only the control frequency (surrogate for all frequencies) was measured. Application of the diurnal correction factor obtained by previous activity data analysis yielded an estimate of the average RF EME over 24 hours at each measured point in the mapping area.

Maps of each survey area displaying the distribution of the 24-hour average RF EME levels at each measured point are presented in the individual reports for each survey site.

1.13 GSM Security

GSM provides authentication of users and encryption of the traffic across the air interface. This is accomplished by giving the user and network a shared secret, kalled Ki. this 128-bit number is stored on the SIM-card, and is not directly accessible to the user.

Each time the mobile connects to the network, the network authenticates the user by sending a random number (challenge) to the mobile. The SIM then uses an authentication algorithm to compute a authentication token SRES using the random number and Ki. The mobile sends the SRES back to the network which compares the value with an independently computed SRES. At the same time, an encryption key Kc is computed. This key is used for encryption of subsequent traffic across the air interface. Thus, even if an attacker listening to the air traffic could crack the encryption key Kc, the attack would be of little value, since this key changes each time the authentication procedure is performed.

1.14 GSM Service

It is important to note that all the GSM services were not introduced since the appearance of GSM but they have been introduced in a regular way. The GSM Memorandum of Understanding (MoU) defined four classes for the introduction of the different GSM services:

1-E1: introduced at the start of the service.

2-E2: introduced at the end of 1991.

3-Eh: introduced on availability of half-rate channels.

4-A: these services are optional.

Three categories of services can be distinguished:

- Teleservices.
- Bearer services.
- Supplementary Services.

1.14.1 Teleservices

1-Telephony (E1® Eh).

2- Facsimile group 3 (E1).

3- Emergency calls (E1® Eh).

4-Teletex.

Short Message Services (E1, E2, A). Using these services, a message of a maximum of 160 alphanumeric characters can be sent to or from a mobile station. If the mobile is powered off, the message is stored. With the SMS Cell Broadcast (SMS-CB), a message of a maximum of 93 characters can be broadcast to all mobiles in a certain geographical area. Fax mail. Thanks to this service, the subscriber can receive fax messages at any fax machine. Voice mail. This service corresponds to an answering machine.

1.14.2 Bearer Services

A bearer service is used for transporting user data. Some of the bearer services are listed below:

1- Asynchronous and synchronous data, 300-9600 bps (E1).

2- Alternate speech and data, 300-9600 bps (E1).

3- Asynchronous PAD (packet-switched, packet assembler/disassembler) access, 300-9600 bps (E1).

4-Synchronous dedicated packet data access, 2400-9600 bps (E2).

1.14.3 Supplementary Services

Call Forwarding (E1). The subscriber can forward incoming calls to another number if the called mobile is busy (CFB), unreachable (CFNRc) or if there is no reply (CFNRy). Call forwarding can also be applied unconditionally (CFU).

There are different types of `call barring' services:

1-Barring of All Outgoing Calls, BAOC (E1).

2-Barring of Outgoing International Calls, BOIC (E1).

3-Barring of Outgoing International Calls except those directed toward the Home PLMN Country, BOIC-exHC (E1).

4-Barring of All Incoming Calls, BAIC (E1)

5-Barring of incoming calls when roaming (A).

-Call hold (E2). Puts an active call on hold.

- Call Waiting, CW (E2). Informs the user, during a conversation, about another incoming call. The user can answer, reject or ignore this incoming call.

- Advice of Charge, AoC (E2). Provides the user with an online charge information.

- Multiparty service (E2). Possibility of establishing a multiparty conversation.

- Closed User Group, CUG (A). It corresponds to a group of users with limited possibilities of calling (only the people of the group and certain numbers).

- Calling Line Identification Presentation, CLIP (A). It supplies the called user with the ISDN of the calling user.

- Calling Line Identification Restriction, CLIR (A). It enables the calling user to restrict the presentation.
- Connected Line identification Presentation, CoLP (A). It supplies the calling user with the directory number he gets if his call is forwarded.

- Connected Line identification Restriction, CoLR (A). It enables the called user to restrict the presentation.

- Operator determined barring (A). Restriction of different services and call types by the operator.

1.15 Summary

This chapter presents, Overview of System Architectute of GSM, An Overview on the GSM Subsystems, Mobile Station, Subscriber Identity Module, Base Transceiver Station, Base Station Controller, Transcoding Rate and Adaptation Unit, Mobile Services Switching Center, Home Location Register, Visitor Location Register, Equipment Identity Register, GSM Base Station Measurements And It's Methods, GSM Security, GSM services.

CHAPTER TWO

2.THE GSM RADIO INTERFACE

2.1 Overview

The radio interface is the interface between the mobile stations and the fixed infrastructure. It is one of the most important interfaces of the GSM system.

One of the main objectives of GSM is roaming. Therefore, in order to obtain a complete compatibility between mobile stations and networks of different manufacturers and operators, the radio interface must be completely defined.

The spectrum efficiency depends on the radio interface and the transmission, more particularly in aspects such as the capacity of the system and the techniques used in order to decrease the interference and to improve the frequency reuse scheme. The specification of the radio interface has then an important influence on the spectrum efficiency.

2.2 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.

2.3 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.

2.3.1 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.

2.4 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

2.4.1 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 t 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).

2.4.2 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 2.1. 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 10th 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 correction of MS downlink. It is required for 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., allocation of dedicated control channels). The CCCH channels help to 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.

2.5 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

2.5.1 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.

2.5.2 Synchronization Burst

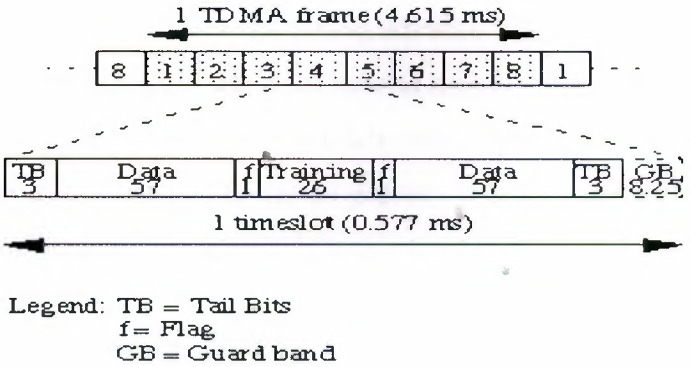

Figure 2.2. GSM TDMA structure and normal burst number of bits per field below the field legend

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).

2.5.3 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.

2.5.4 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.

2.5.5 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 2.3.

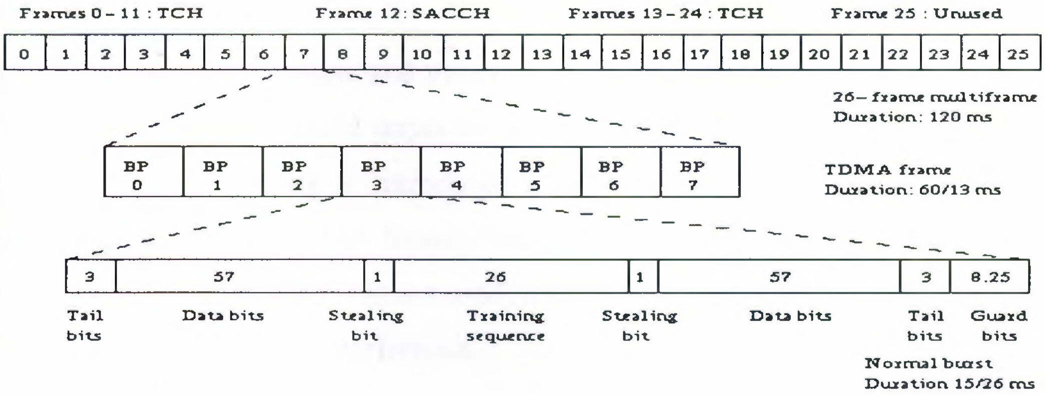

Figure 2.3: Structure of the 26-Multiframe, the TDMA frame and the normal burst

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.

2.6 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.

2.7 Summary

This chapter presents, Overview of The GSM Radio Interface, Frequency Allocation, Multiple Access Scheme, GSM Channel Structure, Structure of TDMA Slot With a Frame, Frequency Hopping.

CHAPTER THREE
3.THE MOBILE TELEPHONE SYSTEM

3.1 Overview

The traditional telephone system (even if it some day gets multigigabit endto-end fiber) will still not be able to satisfy a growing group of users: people on the go. People now expect to make phone calls from airplanes, cars, swimming pools, and while jogging in the park. Within a few years they will also expect to send e-mail and surf the Web from all these locations and more. Consequently, there is a tremendous amount of interest in wireless telephony. In the following sections we will study this topic in some detail.

Wireless telephones come in two basic varieties: cordless phones and mobile phones (sometimes called cell phones). Cordless phones are devices consisting of a base station and a handset sold as a set for use within the home. These are never used for networking, so we will not examine them further. Instead we will concentrate on the mobile system, which is used for wide area voice and data communication.

Mobile phones have gone through three distinct generations, with different technologies:

1. Analog voice.
2. Digital voice.
3. Digital voice and data (Internet, e-mail, etc.).

Although most of our discussion will be about the technology of these systems, it is interesting to note how political and tiny marketing decisions can have a huge impact. The first mobile system was devised in the U.S. by AT&T and mandated for the whole country by the FCC. As a result, the entire U.S. had a single (analog) system and a mobile phone purchased in California also worked in NewYork. In contrast, when mobile came to Europe, every country devised its own system, which resulted in a fiasco.

Europe learned from its mistake and when digital came around, the government-run PTTs got together and standardized on a single system (GSM), so any European mobile phone will work anywhere in Europe. By then, the U.S. had decided that government should not be in the standardization business, so it left digital to the marketplace. This decision resulted in different equipment manufacturers producing different kinds of mobile phones. As a consequence, the U.S. now has two major incompatible digital mobile phone systems in operation (plus one minor one).

Despite an initial lead by the U.S., mobile phone ownership and usage in Europe is now far greater than in the U.S. Having a single system for all of Europe is part of the reason, but there is more. A second area where the U.S. and Europe differed is in the humble matter of phone numbers. In the U.S. mobile phones are mixed in with regular (fixed) telephones. Thus, there is no way for a caller to see if, say, (212) 234-5678 is a fixed telephone (cheap or free call) or a mobile phone (expensive call). To keep people from getting nervous about using the telephone, the telephone companies decided to make the mobile phone owner pay for incoming calls.

As a consequence, many people hesitated to buy a mobile phone for fear of running up a big bill by just receiving calls. In Europe, mobile phones have a special area code (analogous to 800 and 900 numbers) so they are instantly recognizable. Consequently, the usual rule of ''caller pays'' also applies to mobile phones in Europe (except for international calls where costs are split).

A third issue that has had a large impact on adoption is the widespread use of prepaid mobile phones in Europe (up to 75% in some areas). These can be purchased in many stores with no more formality than buying a radio. You pay and you go. They are preloaded with, for example, 20 or 50 euro and can be recharged (using a secret PIN code) when the balance drops to zero. As a consequence, practically every teenager and many small children in Europe have (usually prepaid) mobile phones so their parents can locate them, without the danger of the child running up a huge bill. If the mobile phone is used only occasionally, its use is essentially free since there is no monthly charge or charge for incoming calls.

3.2 First-Generation Mobile Phones: Analog Voice

Enough about the politics and marketing aspects of mobile phones. Now let us look at the technology, starting with the earliest system. Mobile radiotelephones were used sporadically for maritime and military communication during the early decades of the 20th century. In 1946, the first system for car-based telephones was set up in St. Louis. This system used a single large transmitter on top of a tall building and had a single channel, used for both sending and receiving. To talk, the user had to push a button that enabled the transmitter and disabled the receiver. Such systems, known as push-to-talk systems, were installed in several cities beginning in the late 1950s. CB-radio, taxis, and police cars on television programs often use this technology.

In the 1960s, IMTS (Improved Mobile Telephone System) was installed.

It, too, used a high-powered (200-watt) transmitter, on top of a hill, but now had two frequencies, one for sending and one for receiving, so the push-to-talk button was no longer needed. Since all communication from the mobile telephones went inbound on a different channel than the outbound signals, the mobile users could not hear each other (unlike the push-to-talk system used in taxis).

IMTS supported 23 channels spread out from 150 MHz to 450 MHz. Due to the small number of channels, users often had to wait a long time before getting a dial tone. Also, due to the large power of the hilltop transmitter, adjacent systems had to be several hundred kilometers apart to avoid interference. All in all, the limited capacity made the system impractical.

3.2.1 Advanced Mobile Phone System

All that changed with AMPS (Advanced Mobile Phone System), invented by Bell Labs and first installed in the United States in 1982. It was also used in England, where it was called TACS, and in Japan, where it was called MCS-L1.

Although no longer state of the art, we will look at it in some detail because many of its fundamental properties have been directly inherited by its digital successor, D-AMPS, in order to achieve backward compatibility.

In all mobile phone systems, a geographic region is divided up into cells, which is why the devices are sometimes called cell phones. In AMPS, the cells are typically 10 to 20 km across; in digital systems, the cells are smaller. Each cell uses some set of frequencies not used by any of its neighbors. The key idea that gives cellular systems far more capacity than previous systems is the use of relatively small cells and the reuse of transmission frequencies in nearby (but not adjacent) cells. Whereas an IMTS system 100 km across can have one call on each frequency, an AMPS system might have 100 10-km cells in the same area and be able to have 10 to 15 calls on each frequency, in widely separated cells. Thus, the cellular design increases the system capacity by at least an order of magnitude, more as the cells get smaller. Furthermore, smaller cells mean that less power is needed, which leads to smaller and cheaper transmitters and handsets.

Hand-held telephones put out 0.6 watts; transmitters in cars are 3 watts, the maximum allowed by the FCC.

The idea of frequency reuse is illustrated in Fig. 3.1(a). The cells are normally roughly circular, but they are easier to model as hexagons. In Fig. 3.1(a), the cells are all the same size. They are grouped in units of seven cells. Each letter indicates a group of frequencies. Notice that for each frequency set, there is a buffer about two cells wide where that frequency is not reused, providing for good separation and low interference.

Finding locations high in the air to place base station antennas is a major issue.

This problem has led some telecommunication carriers to forge alliances with the Roman Catholic Church, since the latter owns a substantial number of exalted potential antenna sites worldwide, all conveniently under a single management.
In an area where the number of users has grown to the point that the system is overloaded, the power is reduced, and the overloaded cells are split into smaller microcells to permit more frequency reuse, as shown in Fig. 3.1(b).

Telephone companies sometimes create temporary microcells, using portable towers with satellite links at sporting events, rock concerts, and other places where large numbers of mobile users congregate for a few hours. How big the cells should be is a complex matter, which is treated in (Hac, 1995).
At the center of each cell is a base station to which all the telephones in the cell transmit. The base station consists of a computer and transmitter/receiver connected to an antenna. In a small system, all the base stations are connected to

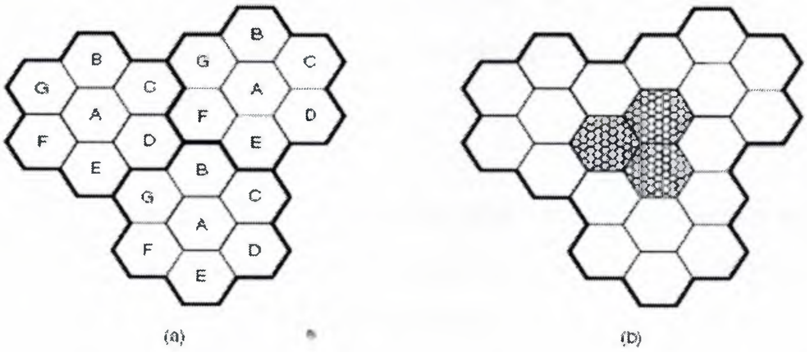

Figure 3.1. (a) Frequencies are not reused in adjacent cells. (b) To add more users, smaller cells can be used.

a single device called an MTSO (Mobile Telephone Switching Office) or MSC (Mobile Switching Center). In a larger one, several MTSOs may be needed, all of which are connected to a second-level MTSO, and so on. The MTSOs are essentially end offices as in the telephone system, and are, in fact, connected to at least one telephone system end office. The MTSOs communicate with the base stations, each other, and the PSTN using a packet-switching network.

At any instant, each mobile telephone is logically in one specific cell and under the control of that cell's base station. When a mobile telephone physically leaves a cell, its base station notices the telephone's signal fading away and asks all the surrounding base stations how much power they are getting from it. The base station then transfers ownership to the cell getting the strongest signal, that is, the cell where the telephone is now located. The telephone is then informed of its new boss, and if a call is in progress, it will be asked to switch to a new channel (because the old one is not reused in any of the adjacent cells). This process, called handoff, takes about 300 msec. Channel assignment is done by the MTSO, the nerve center of the system. The base stations are really just radio relays.

Handoffs can be done in two ways. In a soft handoff, the telephone is acquired by the new base station before the previous one signs off. In this way there is no loss of continuity. The downside here is that the telephone needs to be able to tune to two frequencies at the same time (the old one and the new one). Neither first nor second generation devices can do this.

In a hard handoff, the old base station drops the telephone before the new one acquires it. If the new one is unable to acquire it (e.g., because there is no available frequency), the call is disconnected abruptly. Users tend to notice this, but it is inevitable occasionally with the current design.

3.2.2 Channels

The AMPS system uses 832 full-duplex channels, each consisting of a pair of simplex channels. There are 832 simplex transmission channels from 824 to 849 MHz and 832 simplex receive channels from 869 to 894 MHz. Each of these simplex channels is 30 kHz wide. Thus, AMPS uses FDM to separate the channels.

In the 800-MHz band, radio waves are about 40 cm long and travel in straight lines. They are absorbed by trees and plants and bounce off the ground and buildings.

It is possible that a signal sent by a mobile telephone will reach the base station by the direct path, but also slightly later after bouncing off the ground or a building. This may lead to an echo or signal distortion (multipath fading). Sometimes, it is even possible to hear a distant conversation that has bounced several times.

The 832 channels are divided into four categories:

1. Control (base to mobile) to manage the system.
2. Paging (base to mobile) to alert mobile users to calls for them.
3. Access (bidirectional) for call setup and channel assignment.
4. Data (bidirectional) for voice, fax, or data.

Twenty-one of the channels are reserved for control, and these are wired into a PROM in each telephone. Since the same frequencies cannot be reused in nearby cells, the actual number of voice channels available per cell is much smaller than 832, typically about 45.

3.2.3 Call Management

Each mobile telephone in AMPS has a 32-bit serial number and a 10-digit telephone number in its PROM. The telephone number is represented as a 3-digit area code in 10 bits, and a 7-digit subscriber number in 24 bits. When a phone is switched on, it scans a preprogrammed list of 21 control channels to find the most powerful signal.

The phone then broadcasts its 32-bit serial number and 34-bit telephone number. Like all the control information in AMPS, this packet is sent in digital form, multiple times, and with an error-correcting code, even though the voice channels themselves are analog.

When the base station hears the announcement, it tells the MTSO, which records the existence of its new customer and also informs the customer's home MTSO of his current location. During normal operation, the mobile telephone reregisters about once every 15 minutes.

To make a call, a mobile user switches on the phone, enters the number to be called on the keypad, and hits the SEND button. The phone then transmits the number to be called and its own identity on the access channel. If a collision occurs there, it tries again later. When the base station gets the request, it informs the MTSO. If the caller is a customer of the MTSO's company (or one of its partners), the MTSO looks for an idle channel for the call. If one is found, the channel number is sent back on the control channel. The mobile phone then automatically switches to the selected voice channel and waits until the called party picks up the phone.

Incoming calls work differently. To start with, all idle phones continuously listen to the paging channel to detect messages directed at them. When a call is placed to a mobile phone (either from a fixed phone or another mobile phone), a packet is sent to the callee's home MTSO to find out where it is. A packet is then sent to the base station in its current cell, which then sends a broadcast on the paging channel of the form ''Unit 14, are you there?'' The called phone then responds with ''Yes'' on the access channel.

The base then says something like: ''Unit 14, call for you on channel 3.'' At this point, the called phone switches to channel 3 and starts making ringing sounds (or playing some melody the owner was given as a birthday present).

3.3 Second-Generation Mobile Phones: Digital Voice

The first generation of mobile phones was analog; the second generation was digital. Just as there was no worldwide standardization during the first generation, there was also no standardization during the second, either. Four systems are in use now: D-AMPS, GSM, CDMA, and PDC. Below we will discuss the first three. PDC is used only in Japan and is basically D-AMPS modified for backward compatibility with the first-generation Japanese analog system. The name PCS (Personal Communications Services) is sometimes used in the marketing literature to indicate a second-generation (i.e., digital) system. Originally it meant a mobile phone using the 1900 MHz band, but that distinction is rarely made now.

3.3.1 D-AMPS—The Digital Advanced Mobile Phone System

The second generation of the AMPS systems is D-AMPS and is fully digital.
It is described in International Standard IS-54 and its successor IS-136. D-AMPS was carefully designed to co-exist with AMPS so that both first- and second generation mobile phones could operate simultaneously in the same cell. In particular, D-AMPS uses the same 30 kHz channels as AMPS and at the same frequencies so that one channel can be analog and the adjacent ones can be digital.

Depending on the mix of phones in a cell, the cell's MTSO determines which channels are analog and which are digital, and it can change channel types dynamically as the mix of phones in a cell changes.

When D-AMPS was introduced as a service, a new frequency band was made available to handle the expected increased load. The upstream channels were in the 1850–1910 MHz range, and the corresponding downstream channels were in the 1930–1990 MHz range, again in pairs, as in AMPS. In this band, the waves are 16 cm long, so a standard ¼-wave antenna is only 4 cm long, leading to smaller phones. However, many D-AMPS phones can use both the 850-MHz and 1900-MHz bands to get a wider range of available channels.

On a D-AMPS mobile phone, the voice signal picked up by the microphone is digitized and compressed using a model that is more sophisticated than the delta modulation and predictive encoding schemes.

Compression takes into account detailed properties of the human vocal system to get the bandwidth from the standard 56-kbps PCM encoding to 8 kbps or less. The compression is done by a circuit called a vocoder (Bellamy, 2000). The compression is done in the telephone, rather than in the base station or end office, to reduce the number of bits sent over the air link. With fixed telephony, there is no benefit to having compression done in the telephone, since reducing the traffic over the local loop does not increase system capacity at all.

3.3.2 GSM—The Global System for Mobile Communications

D-AMPS is widely used in the U.S. and (in modified form) in Japan. Virtually everywhere else in the world, a system called GSM (Global System for Mobile communications) is used, and it is even starting to be used in the U.S. on a limited scale.

To a first approximation, GSM is similar to D-AMPS. Both are cellular systems. In both systems, frequency division multiplexing is used, with each mobile transmitting on one frequency and receiving on a higher frequency (80 MHz higher for D-AMPS, 55 MHz higher for GSM). Also in both systems, a single frequency pair is split by time-division multiplexing into time slots shared by multiple mobiles. However, the GSM channels are much wider than the AMPS channels (200 kHz versus 30 kHz) and hold relatively few additional users (8 versus 3), giving GSM a much higher data rate per user than D-AMPS.

The printed GSM standard is over 5000 [sic] pages long. A large fraction of this material relates to engineering aspects of the system, especially the design of receivers to handle multipath signal propagation, and synchronizing transmitters and receivers.

3.3.3 CDMA—Code Division Multiple Access

D-AMPS and GSM are fairly conventional systems. They use both FDM and TDM to divide the spectrum into channels and the channels into time slots. However, there is a third kid on the block, CDMA (Code Division Multiple Access), which works completely differently.

When CDMA was first proposed, the industry gave it approximately the same reaction that Columbus first got from Queen Isabella when he proposed reaching India by sailing in the wrong direction. However, through the persistence of a single company, Qualcomm, CDMA has matured to the point where it is not only acceptable, it is now viewed as the best technical solution around and the basis for the third-generation mobile systems. It is also widely used in the U.S. in second-generation mobile systems, competing head-on with D-AMPS. For example, Sprint PCS uses CDMA, whereas AT&T Wireless uses D-AMPS. CDMA is described in International Standard IS-95 and is sometimes referred to by that name. The brand name cdmaOne is also used. CDMA is completely different from AMPS, D-AMPS, and GSM. Instead of dividing the allowed frequency range into a few hundred narrow channels, CDMA allows each station to transmit over the entire frequency spectrum all the time.

Multiple simultaneous transmissions are separated using coding theory. CDMA also relaxes the assumption that colliding frames are totally garbled. Instead, it assumes that multiple signals add linearly.

CDMA is a clever scheme that is being rapidly introduced for wireless mobile communication. It normally operates in a band of 1.25 MHz (versus 30 kHz for D-AMPS and 200 kHz for GSM), but it supports many more users in that band than either of the other systems. In practice, the bandwidth available to each user is at least as good as GSM and often much better.

In an ideal, noiseless CDMA system, the capacity (i.e., number of stations) can be made arbitrarily large, just as the capacity of a noiseless Nyquist channel can be made arbitrarily large by using more and more bits per sample. In practice, physical limitations reduce the capacity considerably. First, we have assumed that all the chips are synchronized in time. In reality, such synchronization is impossible.

What can be done is that the sender and receiver synchronize by having the sender transmit a predefined chip sequence that is long enough for the receiver to lock onto. All the other (unsynchronized) transmissions are then seen as random noise.

If there are not too many of them, however, the basic decoding algorithm still works fairly well. A large body of theory exists relating the superposition of chip sequences to noise level (Pickholtz et al., 1982). As one might expect, the longer the chip sequence, the higher the probability of detecting it correctly in the presence of noise. For extra reliability, the bit sequence can use an error-correcting code. Chip sequences never use error-correcting codes.

An implicit assumption in our discussion is that the power levels of all stations are the same as perceived by the receiver. CDMA is typically used for wireless systems with a fixed base station and many mobile stations at varying distances from it.

The power levels received at the base station depend on how far away the transmitters are. A good heuristic here is for each mobile station to transmit to the base station at the inverse of the power level it receives from the base station. In other words, a mobile station receiving a weak signal from the will use more power than one getting a strong signal. The base station can also give explicit commands to the mobile stations to increase or decrease their transmission power.

We have also assumed that the receiver knows who the sender is. In principle, given enough computing capacity, the receiver can listen to all the senders at once by running the decoding algorithm for each of them in parallel. In real life, suffice it to say that this is easier said than done. CDMA also has many other complicating factors that have been glossed over in this brief introduction.

Nevertheless, CDMA is a clever scheme that is being rapidly introduced for wireless mobile communication. It normally operates in a band of 1.25 MHz (versus 30 kHz for D-AMPS and 200 kHz for GSM), but it supports many more users in that band than either of the other systems. In practice, the bandwidth available to each user is at least as good as GSM and often much better.

Engineers who want to gain a very deep understanding of CDMA should read (Lee and Miller, 1998). An alternative spreading scheme, in which the spreading is over time rather than frequency, is described in (Crespo et al., 1995). Yet another scheme is described in (Sari et al., 2000). All of these references require quite a bit of background in communication engineering.

3.4 Third-Generation Mobile Phones: Digital Voice and Data

What is the future of mobile telephony? Let us take a quick look. A number of factors are driving the industry. First, data traffic already exceeds voice traffic on the fixed network and is growing exponentially, whereas voice traffic is essentially flat. Many industry experts expect data traffic to dominate voice on mobile devices as well soon. Second, the telephone, entertainment, and computer industries have all gone digital and are rapidly converging. Many people are drooling over a lightweight, portable device that acts as a telephone, CD player, DVD player, e-mail terminal, Web interface, gaming machine, word processor, and more, all with worldwide wireless connectivity to the Internet at high bandwidth.

This device and how to connect it is what third generation mobile telephony is all about. For more information, see (Huber et al., 2000; and Sarikaya, 2000).
Back in 1992, ITU tried to get a bit more specific about this dream and issued a blueprint for getting there called IMT-2000, where IMT stood for International Mobile Telecommunications. The number 2000 stood for three things: (1) the year it was supposed to go into service, (2) the frequency it was supposed to operate at (in MHz), and (3) the bandwidth the service should have (in kHz). It did not make it on any of the three counts. Nothing was implemented by 2000. ITU recommended that all governments reserve spectrum at 2 GHz so devices could roam seamlessly from country to country. China reserved the required bandwidth but nobody else did. Finally, it was recognized

that 2 Mbps is not currently feasible for users who are *too* mobile (due to the difficulty of performing handoffs quickly enough). More realistic is 2 Mbps for stationary indoor users (which will compete head-on with ADSL), 384 kbps for people walking, and 144 kbps for connections in cars. Nevertheless, the whole area of 3G, as it is called, is one great cauldron of activity. The third generation may be a bit less than originally hoped for and a bit late, but it will surely happen.

The basic services that the IMT-2000 network is supposed to provide to its users are:
1. High-quality voice transmission.
2. Messaging (replacing e-mail, fax, SMS, chat, etc.).
3. Multimedia (playing music, viewing videos, films, television, etc.).
4. Internet access (Web surfing, including pages with audio and video).

Additional services might be video conferencing, telepresence, group game playing, and m-commerce (waving your telephone at the cashier to pay in a store). Furthermore, all these services are supposed to be available worldwide (with automatic connection via a satellite when no terrestrial network can be located), instantly (always on), and with quality-of-service guarantees.

ITU envisioned a single worldwide technology for IMT-2000, so that manufacturers could build a single device that could be sold and used anywhere in the world (like CD players and computers and unlike mobile phones and televisions).

Having a single technology would also make life much simpler for network operators and would encourage more people to use the services. Format wars, such as the Betamax versus VHS battle when videorecorders first came out, are not good for business.

Several proposals were made, and after some winnowing, it came down to two main ones. The first one, W-CDMA (Wideband CDMA), was proposed by Ericsson. This system uses direct sequence spread spectrum of the type we described above. It runs in a 5 MHz bandwidth and has been designed to interwork with GSM networks although it is not backward compatible with GSM. It does, however, have the property that a caller can leave a W-CDMA cell and enter a GSM cell without losing the call. This system was pushed hard by the European Union, which called it UMTS (Universal Mobile Telecommunications System).

The other contender was CDMA2000, proposed by Qualcomm. It, too, is a direct sequence spread spectrum design, basically an extension of IS-95 and backward compatible with it. It also uses a 5-MHz bandwidth, but it has not been designed to interwork with GSM and cannot hand off calls to a GSM cell (or a DAMPS cell, for that matter). Other technical differences with W-CDMA include a different chip rate, different frame time, different spectrum used, and a different way to do time synchronization.

If the Ericsson and Qualcomm engineers were put in a room and told to come to a common design, they probably could. After all, the basic principle behind both systems is CDMA in a 5 MHz channel and nobody is willing to die for his preferred chip rate. The trouble is that the real problem is not engineering, but politics (as usual). Europe wanted a system that interworked with GSM; the U.S. wanted a system that was compatible with one already widely deployed in the U.S. (IS-95). Each side also supported its local company (Ericsson is based in Sweden; Qualcomm is in California). Finally, Ericsson and Qualcomm were involved in numerous lawsuits over their respective CDMA patents.

In March 1999, the two companies settled the lawsuits when Ericsson agreed to buy Qualcomm's infrastructure. They also agreed to a single 3G standard, but one with multiple incompatible options, which to a large extent just papers over the technical differences. These disputes notwithstanding, 3G devices and services are likely to start appearing in the coming years.
Much has been written about 3G systems, most of it praising it as the greatest thing since sliced bread. Some references are (Collins and Smith, 2001; De Vriendt et al., 2002; Harte et al., 2002; Lu, 2002; and Sarikaya, 2000). However, some dissenters think that the industry is pointed in the wrong direction (Garber, 2002; and Goodman, 2000).

While waiting for the fighting over 3G to stop, some operators are gingerly taking a cautious small step in the direction of 3G by going to what is sometimes called 2.5G, although 2.1G might be more accurate. One such system is EDGE (Enhanced Data rates for GSM Evolution), which is just GSM with more bits per baud. The trouble is, more bits per baud also means more errors per baud, so EDGE has nine different schemes for modulation and error correction, differing on how much of the bandwidth is devoted to fixing the errors introduced by the higher speed.

Another 2.5G scheme is GPRS (General Packet Radio Service), which is an overlay packet network on top of D-AMPS or GSM. It allows mobile stations to send and receive IP packets in a cell running a voice system. When GPRS is in operation, some time slots on some frequencies are reserved for packet traffic.

The number and location of the time slots can be dynamically managed by the base station, depending on the ratio of voice to data traffic in the cell.

The available time slots are divided into several logical channels, used for different purposes. The base station determines which logical channels are mapped onto which time slots. One logical channel is for downloading packets from the base station to some mobile station, with each packet indicating who it is destined for. To send an IP packet, a mobile station requests one or more time slots by sending a request to the base station. If the request arrives without damage, the base station announces the frequency and time slots allocated to the mobile for sending the packet. Once the packet has arrived at the base station, it is transferred to the Internet by a wired connection. Since GPRS is just an overlay over the existing voice system, it is at best a stop-gap measure until 3G arrives.
Even though 3G networks are not fully deployed yet, some researchers regard 3G as a done deal and thus not interesting any more. These people are already working on 4G systems (Berezdivin et al., 2002; Guo and Chaskar, 2002; Huang and Zhuang, 2002; Kellerer et al., 2002; and Misra et al., 2002). Some of the proposed features of 4G systems include high bandwidth, ubiquity (connectivity everywhere), seamless

integration with wired networks and especially IP, adaptive resource and spectrum management, software radios, and high quality of service for multimedia.

Then on the other hand, so many 802.11 wireless LAN access points are being set up all over the place, that some people think 3G is not only not a done deal, it is doomed. In this vision, people will just wander from one 802.11 access point to another to stay connected. To say the industry is in a state of enormous flux is a huge understatement. Check back in about 5 years to see what happens.

3.5 Summary

This chapter presents, Overview The Mobile Telephone System, First-Generation Mobile Phones: Analog Voice, Second-Generation Mobile Phones: Digital Voice, Third-Generation Mobile Phones: Digital Voice and Data.

CHAPTER FOUR
4.GSM CELLULAR NETWORK

4.1 Overview

A cellular network is a radio network made up of a number of radio cells (or just cells) each served by a fixed transmitter, known as a cell site or base station. These cells are used to cover different areas in order to provide radio coverage over a wider area than the area of one cell. Cellular networks are inherently asymmetric with a set of fixed main transceivers each serving a cell and a set of distributed (generally, but not always, mobile) transceivers which provide services to the network's users.

Cellular networks offer a number of advantages over alternative solutions:

- increased capacity
- reduced power usage
- better coverage

A good (and simple) example of a cellular system is an old taxi driver's radio system where the taxi company will have several transmitters based around a city. We'll use that as an example and assume that each transmitter is handled separately by a different operator.

4.2 Mobile Network

This figure 4.1 shows a simplified functional diagram of a mobile network.

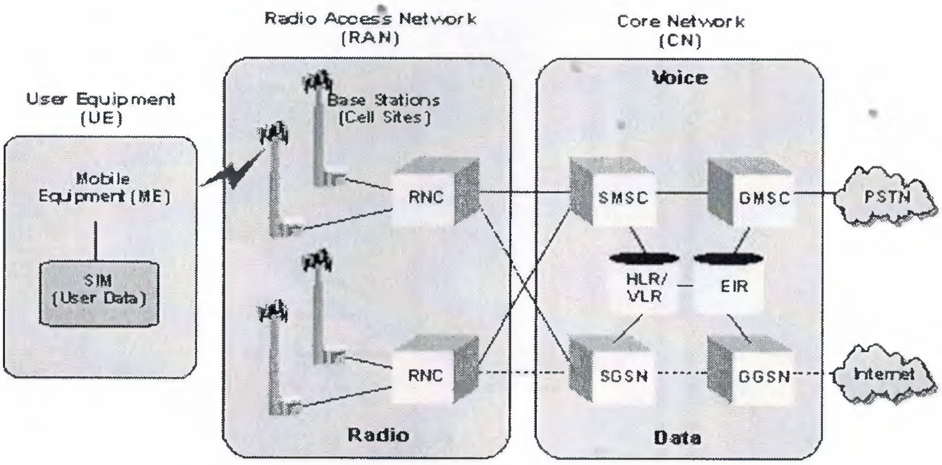

Figure 4.1: Mobile network

This diagram shows that the mobile system is composed of 3 key parts; the user equipment (UE), radio access network (RAN) and a core interconnecting network (CN). The UE is divided into 2 parts, the mobile equipment (ME) and the subscriber identity module (SIM) card. The RAN is composed of base stations and base station controllers (BSCs). This example shows that the BSCs connect voice calls to mobile switching centers (MSCs) and connects data sessions to packet data service nodes (PDSNs).

The core network is basically divided into circuit switched (primarily voice) and packet switched (primarily data) parts. The core network circuit switch parts contain the serving MSC (SMSC) and a gateway MSC (GMSC). The serving SMSC connects to the RAN system and the gateway GMSC connects to the public telephone network. The core network packet switched parts contain the serving general packet radio service (GPRS) support node (SGSN) and a gateway GPRS service node (GGSN). The SGSN connects to the RAN system and the GGSN connects to data networks such as the Internet.

4.2.1 Subscriber Identity Module (SIM) Card

This figure 4.2 shows a block diagram of a SIM. This diagram shows that SIM cards have 8 electrical contacts. This allows for power to be applied to the electronic circuits inside the card and for data to be sent to and from the card.

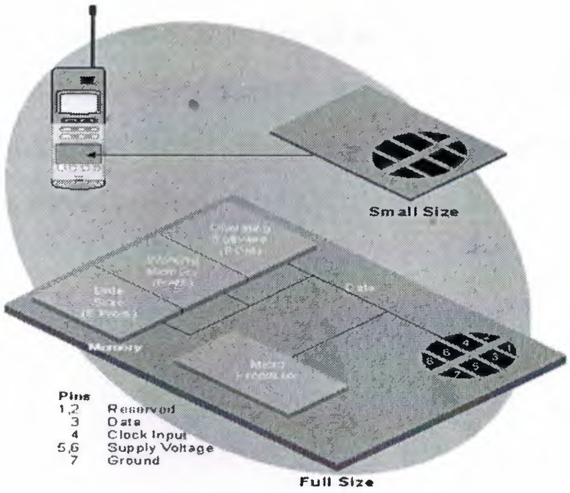

Figure 4.2: SIM card

The card contains a microprocessor that is used to store and retrieve data. Identification information is stored in the cards protected memory that is not accessible by the customer. Additional memory is included to allow features or other information such as short messages to be stored on the card.

4.3 GSM Network coverage

coverage is only part of network availability without sufficient radio signal, mobile phones cannot operate and there are also other factors that impact the use of mobiles. network availability is the general consideration for making a call and this is achieved by having sufficient signal strength at the location of use (coverage) and a free radio channel to use for the call (capacity).

4.3.1 Coverage

Signal strength gets weaker the further the distance from a base site. it can also be affected by obstacles causing 'radio shadow' or operating a mobile within a building or car. design engineers work to complex standards to calculate and predict signal strength and factor in this much weaker signal which is sent out from the mobile device in the return direction. the resulting coverage map is an indication of signal strength where it is not possible to be more exact.

Mobiles phones require a minimum signal free of interference from all other base sites and mobiles making calls. a range of radio channels are used but cellular systems 're-use' these channels many times to make sure there is distance or obstacles between the same channels to avoid the interference this would produce.

4.3.2 Capacity

With a limited set of radio channels, the operator has to adjust the size of each cell area to capture no more potential users than the number of channels he has available to serve them,in towns, where usage is normally highest, cell sizes are small (typically between 100-500m range). at the same time this helps the mobile phones perform better where they may be operated deep inside a building.

The mobile network is naturally designed to cater for normal use. when an otherwise quiet area hosts say, a county show or pop festival, special provisions are made by the network operators <such as extra towers being transported to the site for the event>. however, not every event can be supported in this way and sometimes congestion results and this may be due to the lack of available radio channels.

4.3.3 Mobile Phone Usage

There are various scenarios relating to mobile phone usage which are considered in the network design.

In urban areas, where mobiles are used in office locations, provision is made for 'in-building' use. generally speaking the network can be at its best in towns, for users who are travelling, allowance is made for the use of the mobile phones inside a car or train. this burdens the network design a little. however, the signal experienced is effectively averaged by moving and patches of weaker signals may not degrade the call, tunnels and cuttings, largely affecting train journeys, may have poor coverage and cause a call to drop. the mobile phone waits a little before dropping the call just in case the bad patch is only temporary.

Key locations such as exhibition halls and airports etc. are normally well served. indeed, a service exists to review, design and provide additional coverage for companies needing to operate in an area which is otherwise poor. a cost is associated with this service.

Finally, it is worth remembering that in areas with weak signal, moving a few metres may significantly improve the call. this is especially true if you are able to avoid dense woodland or move to a position which is clear or on higher ground. this may be helpful to know for outdoor groups

4.3.4 Voice vs Data

In GSM, voice and GPRS data require similar signal strengths. however, the nature of voice demands continuous quality through the call. data from gprs devices or text messaging is more forgiving and may perform where voice calls deteriorate.

4.4 General Characteristics Of Networking

The primary requirement for a network in the cellular concept is a way for each distributed station to distinguish the signal from its own transmitter from the signal from other transmitters. There are two common solutions to this, frequency division multiple access (FDMA) and code division multiple access (CDMA). FDMA works by using a different frequency for each neighbouring cell. By tuning to the frequency of a chosen cell the distributed stations can avoid the signal from other neighbours. The principle of CDMA is more complex, but achieves the same result; the distributed transceivers can select one cell and listen to it.

Other available methods of multiplexing such as polarisation division multiple access (PDMA) and time division multiple access (TDMA) cannot be used to separate signals from one cell to the next since the effects of both vary with position and this would make signal separation practically impossible. Time division multiple access, however, is used in combination with either FDMA or CDMA in a number of systems to give multiple channels within the coverage area of a single cell.

In the case of our taxi company, each radio has a knob. The knob acts as a channel selector and allows the radio to tune to different frequencies. As the drivers move around, they change from channel to channel. The drivers know which frequency covers approximately what area, when they don't get a signal from the transmitter, they also try other channels until they find one which works. The taxi drivers only speak one at a time, as invited by the operator (in a sense TDMA)..

4.4.1 Broadcast Messages and Paging

Practically every cellular system has some kind of broadcast mechanism. This can be used directly for distributing information to multiple mobiles, commonly, for example in mobile telephony systems, the most important use of broadcast information is to set up channels for one to one communication between the mobile transceiver and the base station. This is called paging.

The details of the process of paging vary somewhat from network to network, but normally we know a limited number of cells where the phone is located (this group of cells is called a location area in the GSM system or Routing Area in UMTS). Paging takes place by sending the broadcast message on all of those cells. Paging messages can be used for information transfer. This happens in pagers, in CDMA systems for sending SMS messages, and in the UMTS system where it allows for low downlink latency in packet-based connections.

Our taxi network is a very good example here. The broadcast capability is often used to tell about road conditions and also to tell about work which is available to anybody. On the other hand, typically there is a list of taxis waiting for work. When a particular taxi comes up for work, the operator will call their number over the air. The taxi driver acknowledges that they are listening, then the operator reads out the address where the taxi driver has to go.

4.4.2 Frequency Reuse

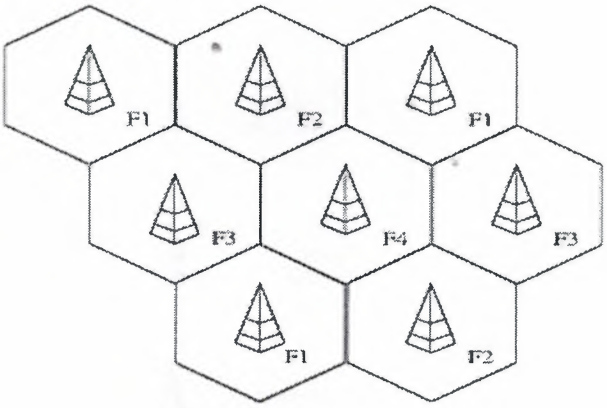

Figure: 4.3 Frequency reuse in a cellular network

The increased capacity in a cellular network, compared with a network with a single transmitter, comes from the fact that the same radio frequency can be reused in a different area for a completely different transmission. If there is a single plain transmitter, only one transmission can be used on any given frequency. Unfortunately, there is inevitably some level of interference from the signal from the other cells which use the same frequency. This means that, in a standard FDMA system, there must be at least a one cell gap between cells which reuse the same frequency.

The frequency reuse factor is the rate at which the same frequency can be used in the network. It is 1/n where n is the number of cells which cannot use a frequency for transmission. A common value for the frequency reuse factor is 7.

Code division multiple access-based systems use a wider frequency band to achieve the same rate of transmission as FDMA, but this is compensated for by the ability to use a frequency reuse factor of 1. In other words, every cell uses the same frequency and the different systems are separated by codes rather than frequencies.

Depending on the size of the city, a taxi system may not have any frequency-reuse in its own city, but certainly in other nearby cities, the same frequency can be used. In a big city, on the other hand, frequency-reuse could certainly be in use.

4.4.3 Movement From Cell to Cell and Handover

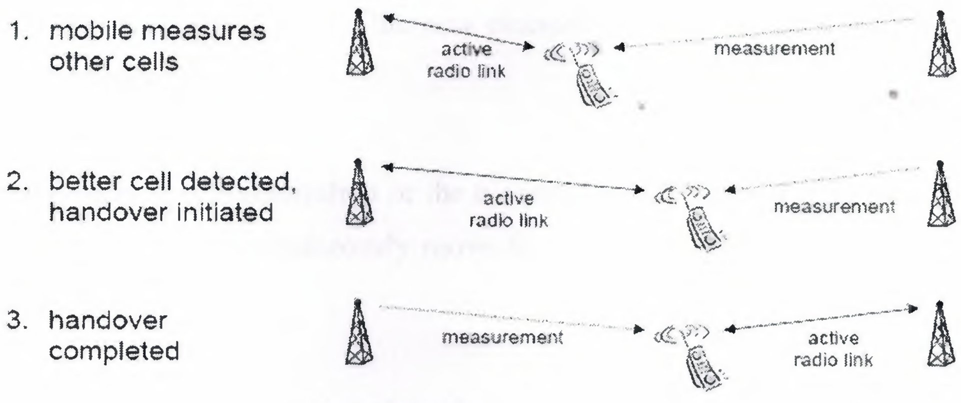

Figure 4.4 :Movement from cell to cell and handover

The use of multiple cells means that, if the distributed transceivers are mobile and moving from place to place, they also have to change from cell to cell. The mechanism for this differs depending on the type of network and the circumstances of the change. For example, if there is an ongoing continuous communication and we don't want to interrupt it, then great care must be taken to avoid interruption.

In this case there must be clear coordination between the base station and the mobile station. Typically such systems use some kind of multiple access independently in each cell, so an early stage of such a handover (handoff) is to reserve a new channel for the mobile station on the new base station which will serve it. The mobile then moves from the channel on its current base station to the new channel and from that point on communication takes place.

The exact details of the mobile system's move from one base station to the other varies considerably from system to system. For example, in all GSM handovers and W-CDMA inter-frequency handovers the mobile station will measure the channel it is meant to start using before moving over. Once the channel is confirmed okay, the network will command the mobile station to move to the new channel and at the same time start bi-directional communication there, meaning there is no break in communication.

In CDMA2000 and W-CDMA same-frequency handovers, both channels will actually be in use at the same time (this is called a soft handover or soft handoff). In IS-95 inter-frequency handovers and older analog systems such as NMT it will typically be impossible to measure the target channel directly whilst communicating. In this case other techniques have to be used such as pilot beacons in IS-95. This means that there is almost always a brief break in the communication whilst searching for the new channel followed by the risk of an unexpected return to the old channel.

If there is no ongoing communication or the communication can be interrupted, it is possible for the mobile station to spontaneously move from one cell to another and then notify the network if needed.

In the case of the primitive taxi system that we are studying, handovers won't really be implemented. The taxi driver just moves from one frequency to another as needed. If a specific communication gets interrupted due to a loss of a signal then the taxi driver asks the controller to repeat the message. If one single taxi driver misses a particular broadcast message (e.g. a request for drivers in a particular area), the others will respond instead. If nobody responds, the operator keeps repeating the request.

The effect of frequency on cell coverage means that different frequencies serve better for different uses. Low frequencies, such as 450 MHz NMT, serve very well for countryside coverage. GSM 900 (900 MHz) is a suitable solution for light urban coverage. GSM 1800 (1.8 GHz) starts to be limited by structural walls.

This is a disadvantage when it comes to coverage, but it is a decided advantage when it comes to capacity. Pico cells, covering e.g. one floor of a building, become possible, and the same frequency can be used for cells which are practically neighbours. UMTS, at 2.1 GHz is quite similar in coverage to GSM 1800. At 5 GHz, 802.11a Wireless LANs already have very limited ability to penetrate walls and may be limited to a single room in some buildings. At the same time, 5 GHz can easily penetrate windows and goes through thin walls so corporate WLAN systems often give coverage to areas well beyond that which is intended.

Moving beyond these ranges, network capacity generally increases (more bandwidth is available) but the coverage becomes limited to line of sight. Infra-red links have been considered for cellular network usage, but as of 2004 they remain restricted to limited point-to-point applications.

Cell service area may also vary due to interference from transmitting systems, both within and around that cell. This is true especially in CDMA based systems. The receiver requires a certain signal-to-noise ratio. As the receiver moves away from the transmitter, the power transmitted is reduced. As the interference (noise) rises above the received power from the transmitter, and the power of the transmitter cannot be increased any more, the signal becomes corrupted and eventually unusable. In CDMA-based systems, the effect of interference from other mobile transmitters in the same cell on coverage area is very marked and has a special name, cell breathing.

Old fashioned taxi radio systems, such as the one we have been studying, generally use low frequencies and high sited transmitters, probably based where the local radio station has its mast. This gives a very wide area coverage in a roughly circular area surrounding each mast.

Since only one user can talk at any given time, coverage area doesn't change with number of users. The reduced signal to noise ratio at the edge of the cell is heard by the user as crackling and hissing on the radio.

To see real examples of cell coverage look at some of the coverage maps provided by real operators on their web sites; in certain cases they may mark the site of the transmitter, in others it can be located by working out the point of strongest coverage.

4.4.4 Cellular Telephone

Figure: 4.5 Cell site

The most common example of a cellular network are mobile phone (cell phone) networks. A mobile phone is a portable telephone which receives or makes calls through a cell site (base station), or transmitting tower. Radio waves are used to transfer signals to and from the cell phone. Large geographic areas (representing the coverage range of a service provider) are split up into smaller cells to deal with line-of-sight signal loss and the large number of active phones in an area. Each cell site has a range of .25 to 20 or more miles, but more typically .5 to 5 miles, and overlaps other cell sites. All of the cell sites are connected to cellular telephone exchanges "switches", which in turn connect to the public telephone network or another switch of the cellular company.

As the phone user moves from one cell area to another, the switch automatically commands the handset and a cell site with a stronger signal (reported by the handset) to go to a new radio channel (frequency). When the handset responds through the new cell site, the exchange switches the connection to the new cell site.

With CDMA technology, the process is different. Multiple CDMA handsets share a specific radio channel; the signals are separated by using a pseudonoise code (PN code) specific to each phone. As the user moves from one cell to another, the handset sets up radio links with multiple cell sites (or sectors of the same site) simultaneously. This is known as "soft handoff" because, unlike with traditional cellular technology, there is no one defined point where the phone switches to the new cell.

Modern mobile phones use cells because radio frequencies are a limited, shared resource. Cell-sites and handsets change frequency under computer control and use low power transmitters so that a limited number of radio frequencies can be reused by many callers with less interference. CDMA handsets, in particular, must have strict power controls to avoid interference with each other. An incidental benefit is that the batteries in the handsets need less power.

Since almost all mobile phones use cellular technology, including GSM, CDMA, and AMPS (analog), the term "cell phone" is used interchangeably with "mobile phone"; however, an exception of mobile phones using cellular technology is satellite phones.

Old systems predating the cellular principle may still be in use in places. The most notable real hold-out is used by many amateur radio operators who maintain phone patches in their clubs' VHF repeaters.

There are a number of different digital cellular technologies, including: Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), Code Division Multiple Access (CDMA), Evolution-Data Optimized (EV-DO), Enhanced Data Rates for GSM Evolution (EDGE), 3GSM, Digital Enhanced Cordless Telecommunications (DECT), Digital AMPS (IS-136/TDMA), and Integrated Digital Enhanced Network (iDEN).

4.5 Architecture of the GSM Network

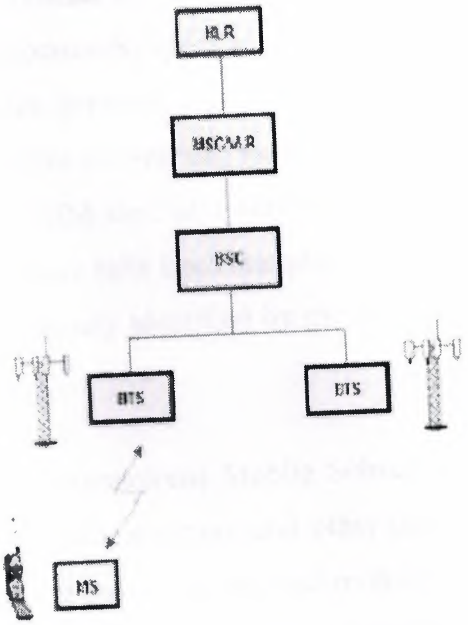

Figure 4.6: The structure of the network

A GSM network is composed of several functional entities, whose functions and interfaces are defined. The GSM network can be divided into three 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. Not shown is the Operations and Maintenance center, which oversees the proper operation and setup of the network. The Mobile Station and the Base Station Subsystem communicate across the Um interface, also known as the air interface or radio link. The Base Station Subsystem communicates with the Mobile service Switching Center across the A interface.

4.5.1 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.

4.5.2 Base Station Subsystem

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

The Base Transceiver Station houses the radio tranceivers that define a cell and handles the radiolink 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.

The Base Station Controller manages the radio resources for one or more BTSs. It handles radiochannel setup, frequency hopping, and handovers, as described below. The BSC is the connection between the mobile and the Mobile service Switching Center (MSC). The BSC also translates the 13 kbps voice channel used over the radio link to the standard 64 kbps channel used by the Public Switched Telephone Network or ISDN.

4.5.3 Network 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 conjuction with several functional entities, which together form the Network Subsystem.

The MSC provides the connection to the public fixed network (PSTN or ISDN), and signalling between functional entities uses the ITUT Signalling 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 callrouting 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.

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 Visitor Location Register 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 signalling required. Note that the MSC contains no information about particular mobile stations - this information is stored in the location registers.

The other two registers are used for authentication and security purposes. The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI). An IMEI is marked as invalid if it has been reported stolen or is not type approved. The Authentication Center 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.

4.6 Network Aspects

Ensuring the transmission of voice or data of a given quality over the radio link is only half the problem in a cellular mobile network. The fact that the geographical area covered by the network is divided into cells necessitates the implementation of a handover mechanism. Also, the fact that the mobile can roam nationally and internationally in GSM requires that registration, authentication, call routing and location updating functions exist in the GSM network.

The signalling protocol in GSM is structured in three layers . Layer 1 is the physical layer, which uses the channel structures discussed above. Layer 2 is the data link layer. Across the Um interface, the data link layer uses a slight modification of the LAPD protocol used in ISDN, called LAPDm. Across the A interface, the lower parts of Signalling System Number 7 are used. Layer 3 is subdivided into 3 sublayers.

- Radio Resources Management

  controls the setup, maintenance, and termination of radio channels
- Mobility Management

  manages the location updating, handovers, and registration procedures, discussed below
- Connection Management

  handles general call control, similar to CCITT Recommendation Q.931, and provides supplementary services.

Signalling between the different entities in the network, such as between the HLR and VLR, is accomplished throught the Mobile Application Part (MAP). Application parts are the top layer of Signalling System Number 7. The specification of the MAP is complex. It is one of the longest documents in the GSM recommendations, said to be over 600 pages in length .

4.6.1 Handover

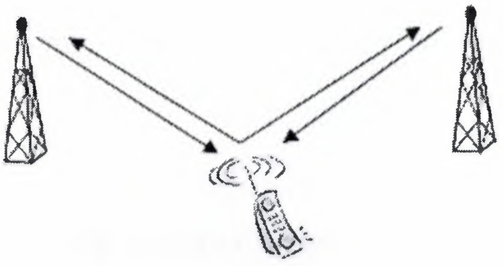

Figure 4.7: Handover

Handover, or handoff as it is called in North America, is the switching of an ongoing call to a different channel or cell. There are four different types of handover in the GSM system, which involve transferring a call between

- channels (time slots) in the same cell,
- cells (Base Transceiver Stations) under the control of the same Base Station Controller (BSC),
- cells under the control of different BSCs, but belonging to the same Mobile services Switching Center (MSC), and
- cells under the control of different MSCs.

The first two types of handover, called internal handovers, involve only one Base Station Controller (BSC). To save signalling bandwidth, they are managed by the BSC without involving the Mobile service Switching Center (MSC), except to notify it at the completion of the handover. The last two types of handover, called external handovers, are handled by the MSCs involved. Note that call control, such as provision of supplementary services and requests for further handoffs, is handled by the original MSC.

Handovers can be initiated by either the mobile or the MSC (as a means of traffic load balancing). During its idle time slots, the mobile scans the Broadcast Control Channel of up to 16 neighboring cells, and forms a list of the six best candidates for possible handover, based on the received signal strength. This information is passed to the BSC and MSC, and is used by the handover algorithm.

The algorithm for when a handover decision should be taken is not specified in the GSM recommendations. There are two basic algorithms used, both closely tied in with power control. This is because the BSC usually does not know whether the poor signal quality is due to multipath fading or to the mobile having moved to another cell. This is especially true in small urban cells.

The 'minimum acceptable performance' algorithm gives precedence to power control over handover, so that when the signal degrades beyond a certain point, the power level of the mobile is increased. If further power increases do not improve the signal, then a handover is considered. This is the simpler and more common method, but it creates 'smeared' cell boundaries when a mobile transmitting at peak power goes some distance beyond its original cell boundaries into another cell.

The 'power budget' method uses handover to try to maintain or improve a certain level of signal quality at the same or lower power level. It thus gives precedence to handover over power control. It avoids the 'smeared' cell boundary problem and reduces cochannel interference, but it is quite complicated.

4.6.2 Location Updating and Call Routing

The MSC provides the interface between the GSM mobile network and the public fixed network. From the fixed network's point of view, the MSC is just another switching node. However, switching is a little more complicated in a mobile network since the MSC has to know where the mobile is currently roaming - and in GSM it could even be roaming in another country. The way GSM accomplishes location updating and call routing to the mobile is by using two location registers: the Home Location Register (HLR) and the Visitor Location Register (VLR).

Location updating is initiated by the mobile when, by monitoring the Broadcast Control Channel, it notices that the locationarea broadcast is not the same as the one previously stored in the mobile's memory. An update request and the IMSI or previous TMSI is sent to the new VLR via the new MSC. A Mobile Station Roaming Number (MSRN) is allocated and sent to the mobile's HLR (which always keeps the most current location) by the new VLR. The MSRN is a regular telephone number that routes the call to the new VLR and is subsequently translated to the TMSI of the mobile. The HLR sends back the necessary call-control parameters, and also sends a cancel message to the old VLR, so that the previous MSRN can be reallocated. Finally, a new TMSI is allocated and sent to the mobile, to identify it in future paging or call initiation requests.

With the above locationupdating procedure, call routing to a roaming mobile is easily performed. The most general case is a call from a fixed network (Public Switched Telecommunications Network or Integrated Services Digital Network) is placed to a mobile subscriber.

Using the Mobile Subscriber's telephone number (MSISDN, the ISDN numbering plan specified in the ITUT E.164 recommendation), the call is routed through the fixed land network to a gateway MSC for the GSM network (an MSC that interfaces with the fixed land network, thus requiring an echo canceller). The gateway MSC uses the MSISDN to query the Home Location Register, which returns the current roaming number (MSRN). The MSRN is used by the gateway MSC to route the call to the current MSC (which is usually coupled with the VLR). The VLR then converts the roaming number to the mobile's TMSI, and a paging call is broadcast by the cells under the control of the current BSC to inform the mobile.

4.7 Public Switched Telephone Network (PSTN)

The public switched telephone network (PSTN) is the network of the world's public circuit-switched telephone networks, in much the same way that the Internet is the network of the world's public IP-based packet-switched networks. Originally a network of fixed-line analog telephone systems, the PSTN is now almost entirely digital, and now includes mobile as well as fixed telephones.

The PSTN is largely governed by technical standards created by the ITU-T, and uses E.163/E.164 addresses (known more commonly as telephone numbers) for addressing.

4.7.1 Architecture and Context

The PSTN was the earliest example of traffic engineering to deliver Quality of Service (QoS) guarantees. A.K. Erlang (1878–1929) is credited with establishing the mathematical foundations of methods required to determine the amount and configuration of equipment and personnel required to deliver a specific level of service.

In the 1970s the telecommunications industry conceived that digital services would follow much the same pattern as voice services, and conceived a vision of end-to-end circuit switched services, known as the Broadband Integrated Services Digital Network (B-ISDN). The B-ISDN vision has been overtaken by the disruptive technology of the Internet.
Only the very oldest parts of the telephone network still use analogue technology for anything other than the last mile loop to the end user, and in recent years digital services have been increasingly rolled out to end users using services such as DSL, ISDN and Cable modem systems.

Many observers believe that the long term future of the PSTN is to be just one application of the Internet - however, the Internet has some way to go before this transition can be made. The QoS guarantee is one aspect that needs to be improved on in the Voice over IP (VoIP) technology.

There are a number of large private telephone networks which are not linked to the PSTN, usually for military purposes. There are also private networks run by large companies which are linked to the PSTN only through limited gateways, like a large private branch exchange (PBX) system.

4.7.2 Digital Channel

Although the network was created using analog voice connections through manual switchboards, automated telephone exchanges replaced most switchboards, and later digital switch technologies were used. Most switches now use digital circuits between exchanges, with analog voice used to connect to many telephones.

The basic digital circuit in the PSTN is a 64-kilobits-per-second channel, originally designed by Bell Labs, called Digital Signal 0 (DS0). To carry a typical phone call from a calling party to a called party, the audio sound is digitized at an 8 kHz sample rate using 8-bit pulse code modulation (PCM). The call is then transmitted from one end to another via telephone exchanges. The call is switched using a signaling protocol (SS7) between the telephone exchanges under an overall routing strategy.

The DS0s are the basic granularity at which switching takes place in a telephone exchange. DS0s are also known as timeslots because they are multiplexed together using time-division multiplexing (TDM). Multiple DS0s are multiplexed together on higher capacity circuits, such that 24 DS0s make a DS1 signal, which when carried on copper is the well-known, T-carrier system, T1 (the European equivalent is an E1, containing 32 64 kbit/s channels). In modern networks, this multiplexing is moved as close to the end user as possible, usually into cabinets at the roadside in residential areas, or into large business premises.

The timeslots are conveyed from the initial multiplexer to the exchange over a set of equipment collectively known as the access network. The access network and inter-exchange transport of the PSTN use synchronous optical transmission (SONET and SDH) technology, although some parts still use the older PDH technology.

Within the access network, there are a number of reference points defined. Most of these are of interest mainly to ISDN but one – the V reference point – is of more general interest. This is the reference point between a primary multiplexer and an exchange. The protocols at this reference point were standardised in ETSI areas as the V5 interface.

4.7.3 U.S. Telephone Switch Hierarchy

In order to organize Direct Distance Dialing (DDD) AT&T divided the various switches in its network in to a hierarchy containing five levels (or classes).

- Class 1

Exchanges were international gateways - handing off and receiving traffic from outside the USA and Canadian networks.

- Class 2

Exchanges were tandem exchanges which interconnected whole regions of the AT&T network.

- Class 3

Exchanges were tandem exchanges connecting major population centres within particular region of the AT&T network.

- Class 4

Exchanges were tandem exchanges connecting the various areas of a city or towns in a region.

- Class 5

Exchanges were those to which subscribers and end-users telephone lines would connect.
In modern times only the terms Class 4 and Class 5 are much used, as any tandem office is referred to as a Class 4. This change was prompted in great part by changes in the power of switches and the relative cost of transmission, both of which tended to flatten the switch hierarchy.

4.8 GSM Services

GSM services are a standard collection of applications and features available to mobile phone subscribers all over the world. The GSM standards are defined by the 3GPP collaboration and implemented in hardware and software by equipment manufacturers and mobile phone operators. The common standard makes it possible to use the same phones with different companies' services, or even roam into different countries. GSM is the world's most dominant mobile phone standard.

The design of the service is moderately complex because it must be able to locate a moving phone anywhere in the world, and accommodate the relatively short battery life, limited input/output capabilities, and weak radio transmitters on mobile devices.

4.8.1 Accessing a GSM Network

In order to gain access to GSM services, a user needs three things:
A subscription with a mobile phone operator. This is usually either a Pay As You Go arrangement, where all GSM services are paid for in advance, or a Pay Monthly option where a bill is issued each month for *line* rental, normally paid for a month in advance, and for services used in the previous month.

A mobile phone which is GSM compliant and operates at the same frequency as the operator. Most phone companies sell phones from third-party manufacturers.
A SIM card which is issued by the operator once the subscription is granted. The card comes pre-programmed with the subscriber's phone "identity" and will be used to store personal information (like contact numbers of friends and family).

After subscribers sign up, information about their phone's identity and what services they are allowed to access are stored in a "SIM record" in the Home Location Register (HLR). The Home Location Register is a database maintained by the "home" phone company for all of its subscribers. It is used to answer queries like, "Where on the mobile phone network is the device associated with this phone number?" and "What services is this subscriber paying for?"

Once the SIM card is loaded into the phone and it is powered on, it will search for the nearest mobile phone mast, also called a Base Transceiver Station or BTS. If a mast can be successfully contacted, then there is said to be coverage in the area.

Stationary phones are always connected to the same part of the phone network, but mobile phones can "visit" any part of the network, whether across town or in another country via a foreign provider. Each geographic area has a database called the Visitors Location Register (VLR) which contains details of all the local mobiles. Whenever a phone attaches, or visits, a new area, the *Visitors* Location Register must contact the Home Location Register.

The Visitors LR will tell the Home LR where the phone is connected to the network (which VLR), and will ask it for a copy of the SIM record (which includes, for example, what services the phone is allowed to access). The current cellular location of the phone (i.e. which

BTS it is at) is entered into the VLR record and will be used during a process called paging when the GSM network wishes to locate the mobile phone.

Every SIM card contains a secret key, called the Ki, which it uses to prove its identity to the phone network (to prevent theft of services) upon first contact. The network does this by consulting the Authentication Center of the "home" phone company, which also has a copy of the secret key. (Though the authentication is accomplished without transmitting the key directly.)

Every phone contains a unique identifier (different from the phone number, which is associated at the HLR with the removable SIM card), called the International Mobile Equipment Identity (IMEI). When a phone contacts the network, its IMEI is supposed to be checked against the global Equipment Identity Register to locate stolen phones and facilitate monitoring.

4.8.2 Voice Calls

- How outgoing calls are made from a mobile:

Once a mobile phone has successfully attached to a GSM network as described above, calls may be made from the phone to any other phone on the global Public Switched Telephone Network assuming the subscriber has an arrangement with their "home" phone company to allow the call.

The user dials the telephone number, presses the *send* or *talk* key, and the mobile phone sends a call setup request message to the mobile phone network via the mobile phone mast (BTS) it is in contact with.

The element in the mobile phone network that handles the call request is the Visited Mobile Switching Center (Visited MSC). The MSC will check against the subscriber's temporary record held in the Visitor Location Register to see if the outgoing call is allowed. If so, the MSC then routes the call in the same way that a telephone exchange does in a fixed network.

If the subscriber is on a Pay As You Go tariff, then an additional check is made to see if the subscriber has enough credit to proceed. If not, the call is rejected. If the call is allowed to continue, then it is continually monitored and the appropriate amount is decremented from the subscriber's account. When the credit reaches zero, the call is cut off by the network. The systems that monitor and provide the prepaid services are not part of the GSM standard services, but instead an example of intelligent network services that a mobile phone operator may decide to implement in addition to the standard GSM ones.

- How incoming calls are made to a mobile:

Step One: Contact the Gateway MSC
When someone places a call to a mobile phone, they dial the telephone number (also called a MSISDN) associated with the phone user and the call is routed to the mobile phone operator's Gateway Mobile Switching Centre. The Gateway MSC, as the name suggests, acts as the "entrance" from exterior portions of the Public Switched Telephone Network onto the provider's network.

As noted above, the phone is free to roam anywhere in the operator's network or on the networks of roaming partners, including in other countries. So the first job of the Gateway MSC is to determine the current location of the mobile phone in order to connect the call. It does this by consulting the Home Location Register (HLR), which, as described above, knows which Visitor Location Register (VLR) the phone is associated with, if any.

Step Two: Determine how to route the call
When the HLR receives this query message, it determines whether the call should be routed to another number (called a divert), or if it is to be routed directly to the mobile.
If the owner of the phone has previously requested that all incoming calls be diverted to another number, known as the Call Forward Unconditional (CFU) Number, then this number is stored in the Home Location Register. If that is the case, then the CFU number is returned to the Gateway MSC for immediate routing to that destination.

If the mobile phone is not currently associated with a Visited Location Register (because the phone has been turned off or is not in range) then the Home Location Register returns a number known as the Call Forward Not Reachable (CFNRc) number to the Gateway MSC, and the call is forwarded there. Many operators may set this value automatically to the phone's voice mail number, so that callers may leave a message. The mobile phone may sometimes override the default setting.

Finally, if the Home Location Register knows that the phone is in the jurisdiction of a particular Visited Location Register, then it will request a temporary number (called an MSRN) from that VLR. This number is relayed to the Gateway MSC, which uses it to route the call to another Mobile Switching Center, called the Visiting MSC.

Step Three: Ringing the phone

When the call is received by the Visiting MSC, the MSRN is used to find the phone's record in the Visited Location Register. This record identifies the phone's location area. Paging occurs to all mobile phone masts in that area. When the subscriber's mobile responds, the exact location of the mobile is returned to the Visited MSC. The VMSC then forwards the call to the appropriate phone mast, and the phone rings. If the subscriber answers, a speech path is created through the Visiting MSC and Gateway MSC back to the network of the person making the call, and a normal telephone call follows.

It is also possible that the phone call is not answered. If the subscriber is busy on another call (and call waiting is not being used) the Visited MSC routes the call to a pre-determined Call Forward Busy (CFB) number. Similarly, if the subscriber does not answer the call after a period of time (typically 30 seconds) then the Visited MSC routes the call to a pre-determined Call Forward No Reply (CFNRy) number. Once again, the operator may decide to set this value by default to the voice mail of the mobile so that callers can leave a message.

- Voice charges:

In the United States and Canada, callers pay the cost of connecting to the Gateway MSC of the subscriber's phone company, regardless of the actual location of the phone. As mobile numbers are given standard geographic numbers according to the North American Numbering Plan, callers pay the same to reach fixed phones and mobile phones in a given geographic area. Mobile subscribers pay for the connection time (typically using in-plan or prepaid minutes) for both incoming and outgoing calls. For outgoing calls, any long distance charges are billed as if they originate at the GMSC, even though it is the Visiting MSC which completes the connection to the PSTN. Plans that include nationwide long distance and/or nationwide roaming at no additional charge over "local" outgoing calls are popular.

Mobile networks in Europe, Asia and Australia only charge their subscribers for outgoing calls. Incoming calls are free to the mobile subscriber; however, callers typically pay a higher rate when calling mobile phones. Special prefixes are used to designate mobile numbers so that callers are aware they are calling a mobile phone and therefore will be charged a higher rate.

From the caller's point of view, it does not matter where the mobile subscriber is, as the technical process of connecting the call is the same. If a subscriber is roaming on a different company's network, the subscriber, instead of the caller, may pay a surcharge for the connection time. International roaming calls are often quite expensive, and as a result some companies require subscribers to grant explicit permission to receive calls while roaming to certain countries.

When a subscriber is roaming internationally and a call is forwarded to his or her voice mail, such as when his or her phone is off, busy, or not answered, he or she may actually be charged for *two* simultaneous international phone calls—the first to get from the GMSC to the VMSC and the second to get from the VMSC to the Call Forward Busy or Call Forward No Reply number (typically the voice mailbox) in the subscriber's country.

However, some networks' GMSCs connect unanswered calls directly, keeping the voice signal entirely within the home country and thus avoiding the double charge.

- How speech is encoded during mobile phone calls:

During a GSM call, speech is converted from analogue sound waves to digital data by the phone itself, and transmitted through the mobile phone network by digital means. (Though older parts of the fixed Public Switched Telephone Network may use analog transmission.)

The digital algorithm used to encode speech signals is called a codec. The speech codecs used in GSM are called Half-Rate (HR), Full-Rate (FR), Enhanced Full-Rate (EFR) and Adaptive

Multirate (AMR). All codecs except AMR operate with a fixed data rate and error correction level.

4.8.3 Data Transmission

The Public Switched Telephone Network (PSTN) is essentially a collection of interconnected systems for taking an *audio* signal from one place and delivering it to another. Older analogue phone networks simply converted sound waves into electrical pulses and back again. The modern phone system digitally encodes audio signals so that they can be combined and transmitted long distances over fiber optic cables and other means, without losing signal quality in the process. When someone uses a computer with a traditional modem, they are encoding a (relatively slow) data stream into a series of audio chirps, which are then relayed by the PSTN in the same way as regular voice calls.

This means that computer data is being encoded as phone audio, which is then being re-encoded as phone system data, and then back to phone quality audio, which is finally converted back to computer data at the destination.

GSM voice calls are essentially an extension of the PSTN, dealing only with audio signals. Behind the scenes, we know these audio channels happen to be transmitted as digital radio signals.

The GSM standard also provides separate facilities for transmitting digital data *directly*, without any of the inefficient conversions back and forth to audio form. This allows a mobile "phone" to act like any other computer on the Internet, sending and receiving data via the Internet Protocol or X.25.

The mobile may also be connected to a desktop computer, laptop, or PDA, for use as a network interface. (Like a modem or ethernet card, but using a GSM-compatible data protocol instead of a PSTN-compatible audio channel or an ethernet link to transmit data.) Newer GSM phones can be controlled by a standardised Hayes AT command set through a serial cable or a wireless link (using IrDA or Bluetooth). The AT commands can control anything from ring tones to data compression algorithms.

In addition to general Internet access, other special services may be provided by the mobile phone operator, such as SMS.

- Circuit-switched data protocols:

A circuit-switched data connection reserves a certain amount of bandwidth between two points for the life of a connection, just as a traditional phone call allocates an audio channel of a certain quality between two phones for the duration of the call. (But remember that in the GSM system, there is no need to use audio signals to create data connections, even circuit-switched ones. The idea of a circuit-switched data connection being like a phone call is just an analogy to help explain the idea.)

Two circuit-switched data protocols are defined in the GSM standard, and they have not-very-creative names: Circuit Switched Data (CSD) and High-Speed Circuit-Switched Data (HSCSD). These types of connections are typically charged on a per-second basis, regardless of the amount of data sent over the link. This is because a certain amount of bandwidth is dedicated to the connection regardless of whether or not it is needed.

Circuit-switched connections do have the advantage of providing a constant, guaranteed quality of service, which is useful for real-time applications like video conferencing.

- General Packet Radio Service (GPRS):

A packet-switched connection chops data into distinct chunks, known as packets, which may arrive at their destination via different routes, at different times, out of sequence, or (hopefully only occasionally) not at all. An intermediate protocol, like TCP, might be used to ensure the original data stream is reassembled at the destination (by putting packets in order and retransmitting missing ones, if necessary).

The General Packet Radio Service (GPRS) is a packet-switched data transmission protocol which was incorporated into the GSM standard in 1997. It is backwards-compatible with systems that use pre-1997 versions of the standard. GPRS does this by sending packets to the local mobile phone mast (BTS) on channels not being used by circuit-switched voice calls or data connections. Multiple GPRS users can share a single unused channel because each of them uses it only for occasional short bursts.

The advantage of packet-switched connections is that bandwidth is only used when there is actually data to transmit. This type of connection is thus generally billed by the kilobyte instead of by the second, and is usually a cheaper alternative for applications that only need to send and receive data sporadically, like instant messaging.

GPRS is usually described as a *2.5G* technology; see the main article for more information.

- Short Message Service (SMS):

The GSM standards first defined the structure of a Short Message, and provide a means of transmitting messages between mobile devices and Short Message Service Centres via the Short Message Service (SMS). SMS messages may be carried between phones and SMSCs by any of the circuit-switched or packet-switched methods described above or, more typically, by the MAP protocol through the SS7 signaling channel used for call setup.

SMSCs can be thought of as central routing hubs for Short Messages. Many mobile service operators use their SMSCs as gateways to external systems, including the Internet, incoming SMS news feeds, and each other (often using the de facto SMPP standard).
The SMS standard is also used outside of the GSM system; see the main article for details.

4.8.4 Supplementary Services

GSM supports a comprehensive set of supplementary services that complement and support the telephony and data services described above. They are all defined in GSM standards. (See GSM codes for supplementary services) A partial listing of supplementary services follows.

- Call Forwarding. This service gives the subscriber the ability to forward incoming calls to another number if the called mobile unit is not reachable, if it is busy, if there is no reply, or if call forwarding is allowed unconditionally.

- Barring of Outgoing Calls. This service makes it possible for a mobile subscriber to prevent all outgoing calls.

- Barring of Incoming Calls. This function allows the subscriber to prevent incoming calls. The following two conditions for incoming call barring exist: baring of all incoming calls and barring of incoming calls when roaming outside the home PLMN.

- Advice of Charge (AoC). The AoC service provides the mobile subscriber with an estimate of the call charges. There are two types of AoC information: one that provides the subscriber with an estimate of the bill and one that can be used for immediate charging purposes. AoC for data calls is provided on the basis of time measurements.

- Call Hold. This service enables the subscriber to interrupt an ongoing call and then subsequently reestablish the call. The call hold service is only applicable to normal telephony.

- Call Waiting. This service enables the mobile subscriber to be notified of an incoming call during a conversation. The subscriber can answer, reject, or ignore the incoming call. Call waiting is applicable to all GSM telecommunications services using a circuit-switched connection.

- Multiparty service. The multiparty service enables a mobile subscriber to establish a multiparty conversation - that is, a simultaneous conversation between three and six subscribers. This service is only applicable to normal telephony.

- Calling Line Identification presentation/restriction. These services supply the called party with the integrated services digital network (ISDN) number of the calling party. The restriction service enables the calling party to restrict the presentation. The restriction overrides the presentation.

- Closed User Groups (CUGs). CUGs are generally comparable to a PBX. They are a group of subscribers who are capable of only calling themselves and certain numbers.

- Explicit Call Transfer (ECT). This service allows a user who has two calls to connect these two calls together and release its connections to both other parties.

4.9 Summary

This chapter presents, Overview of GSM Cellular Network, Mobile Network, GSM Network coverage, General Characteristics Of Networking, Architecture of the GSM Network, Network Aspects, Public switched telephone network (PSTN), GSM services.

5.CONCLUSION

GSM, the Global System for Mobile communications, is a digital cellular communications system which has rapidly gained acceptance and market share worldwide, although it was initially developed in a European context. In addition to digital transmission, GSM incorporates many advanced services and features, including ISDN compatibility and worldwide roaming in other GSM networks.

In GSM system, security mechanism is good enough. Security feature should be compatible with signaling system, so the consequence is on the distance of security information movement on GSM system. Therefore, the extra connection must be reduced for security purposes. Operator has independency to offer and do some security aspects in its network, but if doing this feature selection, it has to be done exactly or take every security features, so there will not a problem in future.

The GSM system, and its sibling systems operating at 1.8 GHz (called DCS1800) and 1.9 GHz (called GSM1900 or PCS1900, and operating in North America), are a first approach at a true personal communication system. The SIM card is a novel approach that implements personal mobility in addition to terminal mobility.

Together with international roaming, and support for a variety of services such as telephony, data transfer, fax, Short Message Service, and supplementary services, GSM comes close to fulfilling the requirements for a personal communication system: close enough that it is being used as a basis for the next generation of mobile communication technology in Europe, the Universal Mobile Telecommunication System (UMTS). Another point where GSM has shown its commitment to openness, standards and interoperability is the compatibility with the Integrated Services Digital Network (ISDN) that is evolving in most industrialized countries and Europe in particular (the so-called Euro-ISDN).

GSM is also the first system to make extensive use of the Intelligent Networking concept, in which services like 800 numbers are concentrated and handled from a few centralized service centers, instead of being distributed over every switch in the country.

This is the concept behind the use of the various registers such as the HLR. GSM is a very complex standard, but that is probably the price that must be paid to achieve the level of integrated service and quality offered while subject to the rather severe restrictions imposed by the radio environment.

6.REFERENCES

[1] Mamedov, Fakhereddin , Telecommunication Lecture Note (2000)

[2]. Cheung et al., "Network Planning for Third-Generation Mobile Radio Systems," IEEE Communications Magazine 32, no. 11 (November 1994): 54-69.

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

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

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

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