NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Electrical and Electronic Engineering

GSM RADIO INTERFACE

Graduation Project
EE.. 400

Student: Mustafa Wael Ahmad (990981)

Supervisor: Prof. Dr. Fakhreddin Mamedov

Nicosia 2003

To my mother, my father, my family

Ahd

My .brC>ther~, ~rrtJaq scıJrnaan, Ibo hajjaj and

Khaled al qudah

ACKNOWLEDGMENTS

First I would like to thankprof.fakhreddin mamedov to be my advisor, I. was not able to complete thisproject for GSM Radio Interface successfully without his help, in each meeting, he answered my questions in details, I got a great deal of helpfrom his book (telecommunication).

I want to thank myfamily, especially my parents. Without their support, I would never achieve my currentposition, I anı also thankftil tomy brothers and sisters.

SpecialthankstôEng. arhjad .salnıaan *with his help, being with him make me able to cover the topics that my project is taking about. Thanks (o faculty of engineering for having such a good computational environment.*

Finally, I also would like to .thank nıy friends in the near east university: khaled tummaleh, .A1ohamnıad.R1fzieh,.Ibo .hajjqj, .jehad kishta, Qais Al-Beni, and Jamil Fakhouri,. I spentnicetimeswiththem.

:A.BS TR.ACT

GSM, the Global System Tor Mobile communications, is digital cellular communications system, which has rapidly·gained·acceptance and market share world wide, 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. The advanced ser-vices and architecture of GSM have made it a model for future third-generation cellular systems, such as UMtS. This project will give an overview of the services offered by GSM, the system architecture, the radio transmission structure, and the signaling functional architecture.

Analog cellular phones and tı.etwörkswere designed with minimal security, Which soon turneci.out to be insufficient. The GSM system provides solutions to a few important aspects of security: subscriber authentication, subscriber identity confidentiality and confidentiality ofvoice·and/dataovertheradio•path. Also the SIM module, which plays an importansrole in GSM s¢¢ürity} is discussed,

The transport oftıuıti„iti~di~\~f~}id~f~nis now a key feature of the future radio access network. The evolution of GS1VfR.a:qlp Interface is able in principle to. take benefit from end to end transfür of such appır~~t.ion.however;careful attention has .to .be taken regarding the quality perceived by the~nd user.

INTRODUCTION

A big difference between radio mobile telecommunication networks and networks with fixed links is the management of the access resources. In most fixed systems, if not all, a ~edicated communication medium exists continuously between the user's terminal and the infrastructure, even when no call is established. This special arrangement requires particular functionalities on the controlling infrastrµcture.

In this project, the radio interface between the GSM parts, managing its radio resources and the communication between its parts are discussed.

Thisproject consists of the introduction, four chapters and conclusion.
Chapter 'One introduces the architecture of the GSM network, its parts and functions for its parts. Also the controlling of the radio links and managing the radio resources.

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

Chapter three studies the int~ifa,d~ ibet~~e{\ıi)mobile stations and the fixed infrastructure. It is one of the most important: lritıffaces of the GSM system.the specification of the radio interface has an inıpörtant influence on the spectrum efficiency.

Chapter four is about the levels of radio frequency radiation from GSM Mobile Telephone Base Station

Conclusion presents the significant results, contribution of the author and future investigations.

CHAPTER ONE
ARCHITECTURE ofGSM

1.1 Overview

During the early 1980s, analog cellular telephone systems were experiencing rapid growth in Europe, particularly in Scandinavia and the United Kingdom, but also in France and Germany. Each country developed .its own system, which was. incompatible with everyone else's in equipment and operation. 'I'his -was an undesirable situation, because not only was the mobile equipment limited to operation -withinnational boundaries, which in a. unified Europe were increasingly unimportant, but there was a very limited market for each type of equipment, so economies of scale, and the subsequent savings, .coııldnot be realized.

In 1981 a joint Franco German study Was jnitiated to. develop .a common approach, which, it was hoped, would become a standard.fbrEurope. Soon after..in 1982a proposal from Nordic Telecom and 1'ıJeth~t\ttı1Jls .J>TT to the CEPT (Conference of European Post and Telecommunieatiens) to develop a new digital cellular standard that would cope with the ever. burgeoning d~ıpJındsg~.~f)?~~arıwopile?~~t'NOrks.Then a study group formedqfllled the Group Special Mot,.ile(~Ş~.tQ/ı§tllQY an4.ge.yelopa pan-European public land mobile system. The proposed system had tômeet certain criteria:

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

In 1989, GSM responsibility was transferred to the European Telecommunication Standards Institute (ETSI), and phase I ofthe GSM specifications was published in 1990. Commercial service was .stwted in mid-1991, and by 1993 there were 36 GSM networks in

22 countries. Although standardized in Europe, GSM is not only a European standard. Over 200 GSM networks (including DCS1800 and PCS1900) are operational in 110 countries around the world. In the beginning of 1994, there were 1.3 million subscribers woı1d)Vide, which had grown to more than 55 million by October 1997. With NorthAmerica.makinga delayed entry into the GSM field with a derivative of GSM called PCS 1900, GSM systems exist on every continent, and the acronym GSM now aptly stands for Global System for Mobile communications.

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

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

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

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

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

1.2 History of the Cellular Mobile Radio and GSM

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

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

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

- Spectrum efficiency
- International roaming
- Low mobile and base stations costs
- Good subjective voice quality
- Compatibility with other systems such as ISDN (Integrated Services Digital Network)

- Ability to support new services

Unlike the existing cellular systems, which were developed using an analog technology, the GSM system was developed using a digital technology. The reasons for this choice are e~plaıried in section 3.

In 1989 the responsibility for the GSM specifications passed from the CEPT to the European Telecommunications Standards Institute (ETSI). The aim of the GSM specifications -is to describe the functionality and the interface for each component of the system, and to provide guidance on the design of the system. These specifications will then standardize the system in order to guarantee the proper networking between the different elements of the GSM system. In 1990, the phase I of the GSM specifications was published but the commercial use of GSM did not start until mid 1991.

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

Table 1.1 Events in the development of GSM

Year	Events
1982	CEPT establishes a GSM group in order to develop the standards for a pan-European cellular mobile system
1985	Adoption of a list of recommendations to be generated by the group
1986	Frorıheairinterface TDMA is chosen as access method (in fact, it will be used with FDMA} Initial'[
1987	Memorandum of Understanding (MoU) signed by telecommunication operators] (representing 12 countries)
1988	Validıili~~ ~fth~ GSM ~;~~

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 acceptaıice-of'the GSM system is illustrated with the following figures:

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

Since the appearance of GSM, Other digital mobile systems have been developed. The table 2 charts the .diffȩ.retıt môbıle ceilula.t' systems developed Since the commercial launch of cellular systems.

Tabıe!ı.2Mobile Cellular Systems

I~;;	JM;b,I;c~II~I;s~;;;	]
!1981	!Nordic Mobile Telephony (NMT), 450>	J
{1983	•lAmerican Mobile Phone System (AMPS)	j
If;~::	1~';t~';'1~';~~';~~1~';~A~s)RadioCOD12ooc-N~	Ji
	11~';~-~';C~'.I~'.'~'';'~~~''~''~~tio~., Nom ~eri:M Dig:~ cOHu]	

1994	Personal Digital Cellular (PDC) or Japanese Digital Cellular (JDC)
1995	Personal Communications Systems (PCS) 1900- Canada>
1996	PCS-United States of America>

1.3 Architecture of the GSM Network

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

GSM technical specifications define the different entities that form the GSN-f network by defining their functions and iıterface requirements.

The GSM network can be divided into four main parts:

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

The architecture of the GSM network is presented in figure 1.1.

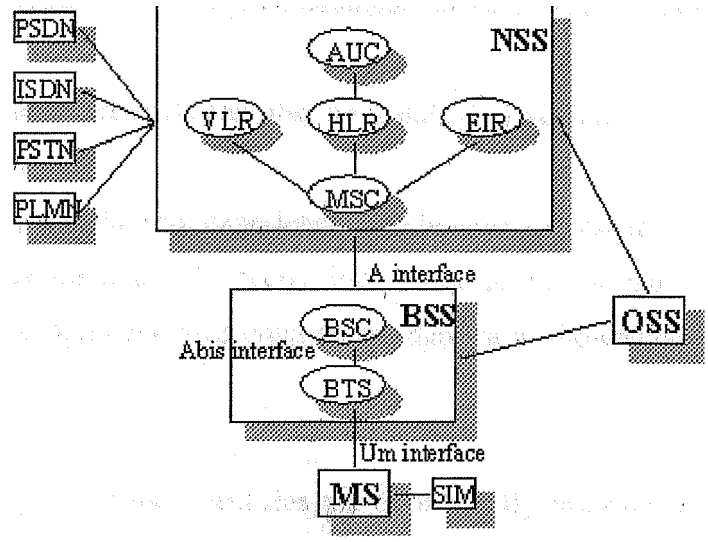


Figure 1.1 Architecture of the GSM network

1.3.1 Mobile Statföıı

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 irr~spectıv'eof 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 phdne, make calls from that phone, or receive other subscribed services.

The mobile equiprn.eııt is uniquely idehtified by the International Mobile Equipment Identity (IMEi). The SIM card contains the Iııfümational Mobile 'Subscriber Identity (IMSI), idı::htifying the subscriber, a secret key :för 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 ideııtitynutf(bel".

- The Terminal

There are different types of terrniıılli distirıguislıed prirtcipa1 1y by tlı~ir power and application:

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

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

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

- **The** SIM

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

Another advantage of the.\~IlVI card is the mobility of the users. In fact, the only element that personalizes a terminal is the SIM card. Therefore, the user can have access to its subscribed services in a,11ytetrninaJ using its SIM card.

1.3.2 The Base Station Subsystem

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

The BTS houses the radio transceivers that define a cell and handles the radio link protocols with the Mobile Station. In a large urban area, there will potentially be a large number of BTSs deployed. The requirements for a BWS are ruggedness, reliability, portability, and minimum cost. BTS is responsible for providing layers 1 and 2 of the radio

interface; that is, an error-corrected data path. Each BTS has at least one of its radio channels assigned to carry control signals in addition to traffic.

The BSC manages the radio resources for one or more BTSs. It .is responsible for the management of the radio resource within a region. Its main functions are to allocate and contreltraffic channels, control frequency hopping, undertake handovers (except to .cells outside its region} and provide radio .performance ...measunements. Once.the mobile has accessed, and synchronized with, a BTS the BSC will allocate it a dedicated bi-directional signaling channel· and will şet up a route to the Mobile services Switching Center (MSC). The BSC also translates the 13 KBPS voice channel.used over the radio link to the 'standard 64 KBPS channel used by the Public Switched Telephone Network or ISDN.

BSS connects the Mobile Station and the NSS.It .is in charge of the transmission and reception. The BSS can be divided into two parts:

I-The Base TransceiverStation(BTS) or Base Station.

2-TheBase Station·Cöntroller (BSC):

- The Base TransceiveriStatiôıı

The BTS corresporıds'tö the transceivers and antennas used in each cell of the network. A BTS is usually placed<itıthe·cetıter of a cell. Its transmitting power definesthe.size of a cell. Each BTS has between one and sixteen transceivers depending on the density of users in the cell.

- The Bast, Station Controller

TheBSC çbntrols a-gröupof B'I'S and mamıgestheir.radio resources.ABSC.is principally in charge öf handôvers, frequency hopping, exchange functions and control of the radio rreqüen.cy power levels ôfthe BTSs.

1.3.3 The Network and Switching Subsystem

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

The Home Location Register (HLR) and Visitor Location Register (VLR), together with the MSC, provide thecall.routing.and (possibly fütetnational) roaming capabilities of CtSM. The BLR contains all the administrative information of each subscriber registered in the corresponding GSM network,alongwiththe current location of the mobile. It also contains a unique authentication key and associated challenge/response generators.

The current location of the ındbile 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 oneHLRper GSM network, although it may be implemented as a distributed database.

The VLR contains selected administrative information from the HLR, necessary for call control and provision of the subscribed services, for each mobile currently located in the geographical area controlled by ·•the VLR. Although each functional 'entity can be implemented as an independent unit, most manufacturers of switching equipment implement one VLR together with one MSC, so that the geographical'area controlled by the MSC corresponds to that controlled by the VLR, simplifying the signaling required.

authentication and security purposes. The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment.on the network

Mobile Equipment Identity (IMEI) ... An IlVIEI is. marked as invalid if it has been reported stolen or is nottype approved. The.Authentication Canter isa protected database that stores a copy of the secret key stored in each subscriber's SIM card, which. is used for authentication and ciphering of the radio channel.

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

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

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

- **The G#feway/Nfobm~seryic~sŞwitchhıg•Center·(GMSC)**

A gateway is a node interconnec:tihgtwo networks. The GMSC is the intepfacebetweeıı the mobile cellular network and the PSTN. It isirı charge of r9uting çalls from the fixed network towards a GSM user, The. GMSC is often implemented in the same machines as the MSC.

- **Home** Location **:Register(HLR)**

The HLR is considered as a very important database that stores information öf the subscribers belonging to the covering area of a MSC. It also stores the current location of these subscribers apd the.seryices to }Y9!Ch they have access. The location of the subscriber corresponds to the SS7 address of the Visitor Location Register (VLR) associated to the terminal

- Visitor Location Register (VLll)

The VLR contains information from a subscriber's HLR necessary in order to provide the subscribed services to visiting users. When asubscriberenters the covering area of a new MSC, the VLR associated to this MSC will request information about the new subscriber to its corresponding HLR. The VLR will then have enough information in order to assure the subscribed services without needing to ask the HLR each time a communication is established.

The VLR is always implemented together with a MSC; so the area under control of the MSC is also the area under control of the VLR.

- The Authentication **Center (AuC)**

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

- The Equipment Identity/Register (EIR)

The EIR is also used for security purposes. It is a register containing information about the mobile equipmetıts. More particularly, it contains a list. of all valid:terminals. A terminal is identified by its International Mobile Equipnıentideıitity (IMEI). The ElR'allows then to forbid calls from stolen or unauthorized terminals (e.g., aterminal Which does not respect the specifications concerning the outputRF power).

- The GSMinterworkingUnit (GIWU)

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

1.3.4 The Operation and Support Subsystem (OSS)

The OSS is cörnected to the different components of the NSS and to the BSC, in order to control and monitor the GSM system. It is also in charge of controlling the traffic load of the BSS.

However, the increasing number of base stations, due to the development of cellular radio networks, has provoked that some of the maintenance tasks are transferred to the BTS. This transfer decreases considerably the costs of the maintenance of the system.

1.4 The Geographical Areas of The GSM Network

The figure 1.2 presents the different a.rea.s that form a GSM network.

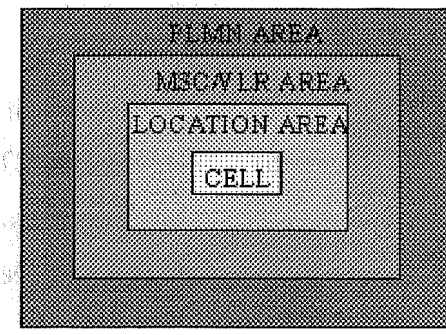


Figure 1.2 GSM Network Areas

As it has already been explained a cell, identified by its Cell Global Identity number (CGI), corresponds to the radio coverage of a base transceiver station. A Location Area (Lf\..), identified by its Location Area Identity (LAI) number, is a group of ceHs served by a single MSC/VLR. A group of location areas under the control of the same J\1SC/VLR defines the MSC/VLR area. A Public Land Mobile Network (PLMN) is the,
Area served by one network operator

1.5 The GSM Functions

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

- Transmission.
- Radio Resources management (RR).
- Mobility Management (MM).

- Communication Management (CM).
- Operation, Administration andMaintenance (OAM).

1.5.1 Transmission

The transmission function includes two sub-functions:

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

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

l,5.2 Radio Resources Management (RR)

The role of the RR'function is to establish, maintain and release communication links between mobile stations and the MSC. The elements that are mainly concerned with the RR function are the mobile station and the base station. However, as the RR function is also in charge of maintaining a connection even if the user moves from one cell to another, the MSC, in charge of handovers, is also concerned with the RR functions.

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

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

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

- **Handover:**

Movements can produce the need to change the channel or cell, especially when the quality of the communication is decreasing. This procedure of changing the resources is called handover. Four differenttypes of handovers can be distinguished:

1- Handover of channels in the same cell.

2- Handover of cells controlled by the same BSC.

3- Handover of cells belonging to the same. MSC but controlled by different BSCs.

4- Handover of cells controlled by different MSCs.

Handovers are mainly controlled by the. MSC. However in order to avoid unnecessary signaling information, the first two types of handovers are managed by the concerned BSC (in this case, the MSC is only notified of the handover).

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

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

1.5.3 Mobility Management

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

- Location Management

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

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

A 'locatien-updating is also performed periodically. If after the updating time period, the mobile station has not registered, it is then deregistered.
Whena mobile station is powered off, it performs an IMSI detach procedure in order to tell the network that it is no longer connected.

- Authentication-And Security

The authentication procedure involves the SIM card and the Authentication Center. A secret key,·. stored in the SIM card and the AuC, and a ciphering algorithm called A3 are used in order to verifythe authenticity ofthe user. The mobile station and the AuC compute a SRES using the secret key, the algorithm A3 and a random number generated bythe AuC. If the two computed SRES 'are the:satne, the subscriber is authenticated. The different servicesto which the subscriber has access are also checked.
Another security procedure is to check the equipment identity. If the IMEI number of the mobile is authorized in the BIR, the mobile statioıtisallowed to connect the network.

In order to assure user confidentiality, the user is registered with a Temporary Mobile Subscriber Identity (TMSI) after its first location update procedure.

The SIM card and the Authentication Center are used for the authentication procedure involves the SIM card and the Authentication Center. A secret key, stored in the SIM card and the AuC, and a ciphering algorithm called AJ are used in order to verify the authenticity of the user. The mobile station and the AuC compute a SRES using the secret key, the algorithm A3 and a random number generated by the AuC. If the two computed SRES are the same, the subscriber istauthenticated. The different services to which the subscriber has access are also checked.

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

1.5.4 Communication.Management (CM)

The CM function is responsible for:

I-Call. control.

2 - Supplementary Services management.

3 -Short Message Services.management.

- **Call Control(CC)**

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

1-A'country. code

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

3-A code corresponding to the subscriber's HLR

The call is then passed to the GMSC (if the call is originated from a fixed network), which knows the HLR corresponding to a certain MISDN number. The GMSC asks the HLR for information helping to the call routing. The HLR requests this information from the subscriber's current VLR. This VLR allocates temporarily a Mobile Station Roaming Number (MS~ for the call. The MSRN number is the information returned by the HLR to the GMSC. Thanks to the MSRN number, the call is routed to subscriber's current MSC/VLR. In the subscriber's current LA, the mobile is paged.

- Supplementary Services.Management

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

- Short Message Services management

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

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

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

1.5.5 Operation, Administration AndMainteııance (OAM)

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

lr The components of the BSS and NSS provide the operator with all the information it needs. This information is then passed t0 the OSS, which is in charge of analyzing it and control the network.

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

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

1.6 How Does It Work

1.6.1 Make Call

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

1.6.2 Call lnitialization

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

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

1.6.3 Authentication

The authentication process is very powerful and is based on advanced cryptographic principles. It especially protects the network operators from fraudulent use of their services. It does not however protect the user from eavesdropping. The Time Division Multiple Access (TDMA) nature of GSM coupled with its frequency hopping facility will make it very difficult for an eavesdropper to lookonto the correct signal however and thus there is 4 much higher degree of inherent security in the system than is found in today's analogue systems. Nevertheless for users who need assurance of a secure transmission, GSM offers encryption over the air interface. This is based on a public key encryption principle and provides very high security.

1.6.4 Call Set-up

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

1.6.5 Handover

GSM employs mobile-assisted handover. In this technique the mobile continuously monitors other base stations in its vicinity, measuring signal strength and error rate. These measurements are combined into a single function and the identities of the best six base stations are transmitted back to the system. The network can then decide when to initiate handover. The use of bit error rate, in addition to signal strength, adds considerably to the ability of the network to make informed handover decisions and iş another example of the advantage of digital transmission over analogue. The BSC can initiate and execute handover if both BTS's are under its own control. In this instance the BSC can be

considered as the manager of a specific group of radio frequencies for a geographic region and can control that resource to maximize its utilization. Alternatively and whenever handover must take place to a cell outside the control of the BSC, the MSC controls and executes handover.

CHAPTER TWO

FROM SOURCE INFORMATION TO RADIO **WAVES**

2.1 Introduction

The figure 2.1 presents the different operations that have to be performed in order to pass from the speech source to radio waves and vice versa.

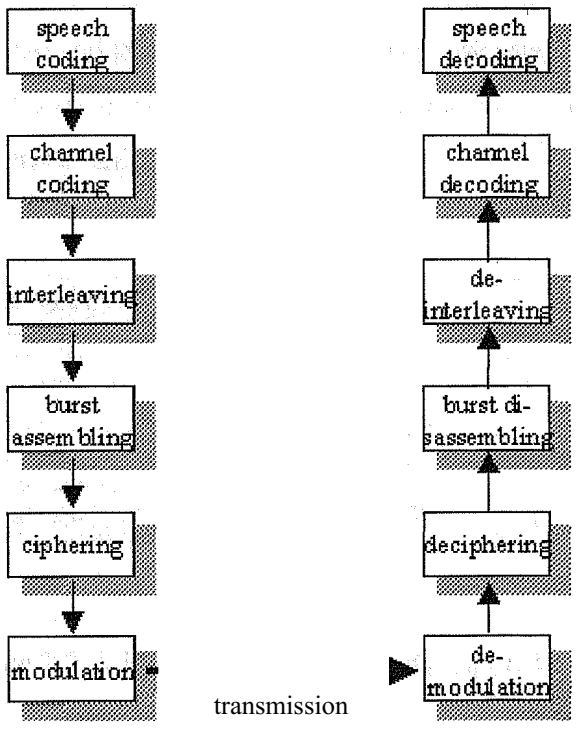


Figure 2.1 From Speech Source To Radio Waves

If .the source of information is data and not speech, the speech coding will not be performed.

2.2 The GSM Speech Coding

The 'full rate speech coder in GSM is· described as Regular Pulse Excitation with Long Term Prediction (GSM 06. 10 RPE-LTP). A good overview ofthis algorithm has been done by Jutta Deeper and Carsten Barman at the Technical University ofBerlin.

Moreover, they have developed a software implementation ofthe GSM 06. 10 speech code, which is available in the public d6föairi. Basically, the encoder divides the speech info short-term predictable parts, longğ--t~rrtpredictable part and the remaining residual pulse. Then, it encodes that pulse and parameters for the two predictors. The decoder reconstructs the speech by passing the residual pulse, first through the long-term prediction filter, and then through the short-term.predictor, see Figure 2.2.

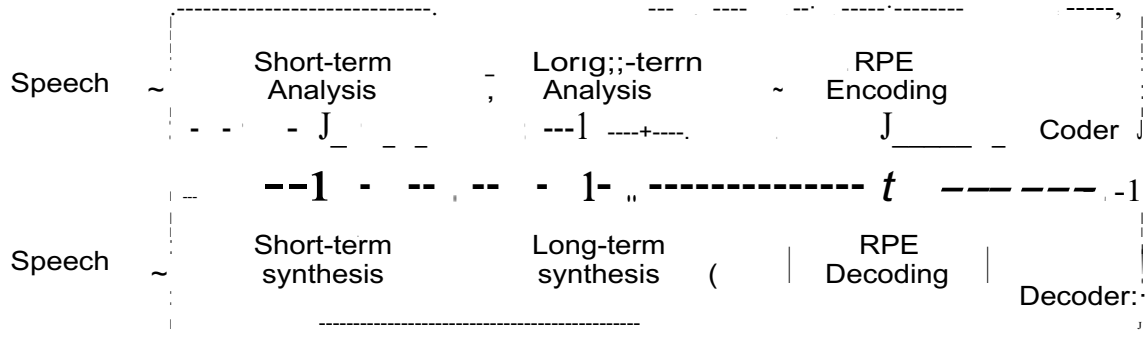


Figure 2.2 A Block Diagram Ofthe GSM 06. 10 Code

Note that the Phase 2 ofGSM defines a new half rate speech encoder (GSM 06.20 RPE-LTP).

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

1-A good speech quality, at least as good as the one obtained with previous cellular systems.

2- To reduce the redundancy in the sounds of the voice. This reduction is essential due to the limited capacity of transmission of a radio channel.

3- The speech code must not be very complex because complexity is equivalent to high costs.

The final choice for the GSM speech code is a code named RPE-LTP (Regular Pulse Excitation Long-Temi Prediction). This code uses the information from previous samples (this information does not change very quickly) in order to predict the current sample. The speech signal is divided into blocks of 20 ms. these blocks are then passed to the speech code, which has a rate of 13 kbps, in order to obtain blocks of 260 bits.

2.3 Th~GSM Channel Coding

Channel coding introduces redundancy into the data flow in order to allow the detection or even the correction of bit errors introduced during the transmission .The speech coding algorithm produces a speech block of 260 bits every 20 ms (i.e. bit rate 13 kbit/s). In the decoder, these speech blocks are decoded and converted to l3 bit uniformly coded speech samples. The 260 bits of the speech block are classified into two groups. The 78 Class II bits are considered of less importance arid are unprotected. The 182 Class I bits are split into 50 Class Ia bits and 132 Class lb bits (See Figure2.3)

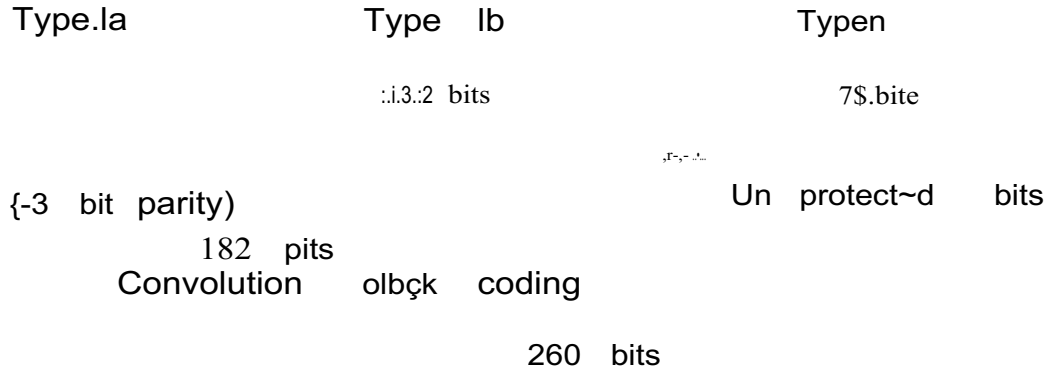


Figure 2.3 Audio Sample: 1 Block= 260 bits (20 ms)

Class Ia bits are first protected by 3 parity bits for error detection. Class lb bits are then added together with 4 tail bits before applying the convolution code with rate *r=l/2* and constraint.length *K*=5. The resulting 378. bits are then added to the 78 unprotected Class II .pits resulting in a complete coded speech'frame of456 bits (see Figure 2.4).

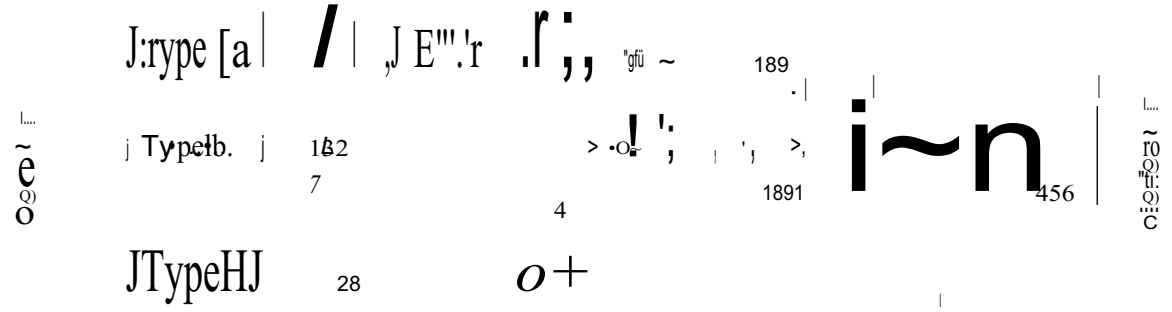


Figure 2.4 TCH/FS Ttansmission Mode

Channel coding adds redundancy bits to .the original information in order to detect and correct, ifpossible, errors occurred during-thetransmission,

2.3.1 Channel Coding For The GSM Data.TCH Channels

The channel coding is performed using two cedes: a block code and a convolution.

The block code corresponds to the block code defined in the GSM Recommendations 05.03. The block code receives an input block of 240 bits and adds four zero tail bits at the end ofthe input block. The output ofthe block code is consequently a block of244 bits.

A convolution code adds redundancy bits in order to protect the information. A convolution encoder contains memory, This property differentiates a convolution code from a block code. A convolution code cart be defined by three variables: n, k and K. The value n corresponds to the number ofbits at the output ofthe encoder, k to the number ofbits at the input öfthe block and K to the memory ofthe encoder. The ratio, R, ofthe code is defined as follows: R = kin. Let's consider a convolution code with the following values: k i's equal

to 1, n to 2 and K to 5. This convolution code uses then a rate of R = 1/2 and a delay of K = 5, which means that it will add a redundant bit for each input bit. The convolution code uses 5 consecutive bits in order to compute the redundancy bit. As the convolution code is a 1 1 2 rate convolution code, a block of 488 bits is generated. These 488 bits are punctured in order to produce a block of 456 bits. Thirty-two bits, obtained as follows, are not transmitted:

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

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

2.3.2 Channel Coding For the GSM Speech Channels

Before applying the channel coding, the 260 bits of a GSM speech frame are divided in three different classes according to their.function and importance. The most important class is the class Ia containing 50 bits. Next in importance is the class lb, which contains 132 bits. The least important is the class II, which contains the remaining 78 bits. The different classes are coded differently. First of all, the class Ia bits are block-coded. Three parity bits, used for error detection, are added to the 50 class Ia bits. The resultant 53 bits are added to the class lb bits. Four zero bits are added to this block of 185 bits (50+3+132). A convolution code, with r = 1/2 and K = 5, is then applied, obtaining an output block of 378 bits. The class II bits are added, without any protection, to the output block of the convolution coder. An output block of 456 bits is finally obtained.

2.3.3 Channel Coding For the GSM Control Channels

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

2.3.4 Error Detecting Codes

The GSM standard uses a 3-bit error redundancy code to enable assessment of the correctness of the bits, which are more sensitive to errors in the speech frame (the category Ia 50-bits). If one of these bits are wrong, this may create a loud noise instead of the 20 ms speech slice. Detecting such errors allows the corrupted block to be replaced by something less disturbing (such as an extrapolation of the preceding block).

The polynomial representing the detection code for category Ia bits is:

$$G(X) = X3 + X + l \tag{2}$$

At the receiving side, the same operation is done and if the remainder differs, an error is detected and the audio frame is eventually discarded.

2.3.5 Convolution Coding /Decoding

Convolution coding consists in transmitting the results of convolutions of the source sequence. using different convolution formulas. The GSM convolution code consists in adding 4 bits (set to "O") to the initial 185 bit sequence and then applying two different convolutions: polynomials are respectively

$$GJ(X) = = X4 + X3 + J \tag{3}$$

$$G2(X) = X4 + X3 + X + l. \tag{4}$$

The final result is composed of twice 189 bits sequences, see Figure 2.2.

Convolution decoding can be performed using a Viterbi algorithm .A Viterbi decoder logically explores in parallel every possible user data in sequence. It encodes and compares each one against the received sequence and picks up the' clôsest match: it is a maximum likelihood decoder. To reduce the complexity (the number of possible data sequence double with each additional data bit), the decoder recognizes at each point that certain sequences cannot belong to the maximum likelihood path and it discards them.

The encoder memory is limited to K bits; a Viterbi decoder in steady-state operation keeps only *2 Kr-I* paths. Its complexity increases f'f,pmwntiallywith the constraint lfn~h K.

The GSM convolution-coding rate per data flow is 378 bits each 20 ms, i.e.: 18.9 kb/s. However, before modulate this signal; the 78 unprotected Class II bits are added (see Figure 2.2). So, the GSM bit rate per flow is 456 bits each 20 ms i.e. 22.8 kb/s.
Note that there is software Viterbi decoder developed by Phil Karn, from Qualcomm Inc., which supports the *(K=7, r=J/2)* NASA standard code.

2.4 **Interleaving**

Interleaving is meant to de-correlate the relative positions of the bits respectively in the code words and in the modulated radio bursts. The aim of the interleaving algorithm is to avoid the risk of loosing consecutive data bits. GSM blocks of full rate speech are interleaved on 8 bursts: the 456 bits of one block are split into 8 bursts in sub-blocks of 57 bits each. A sub-block is defined as either the odd- or the even-numbered bits of the coded data within one burst. Each sub-blocks of 57 bits is carried by a different burst and in a different TDMA frame. So, a burst contains the contribution of two successive speech blocks. A and B. In order to destroy the proximity relations between successive bits, bits of block A use the even positions inside the burst and bits of block B, the odd positions (see Figure 2.4).

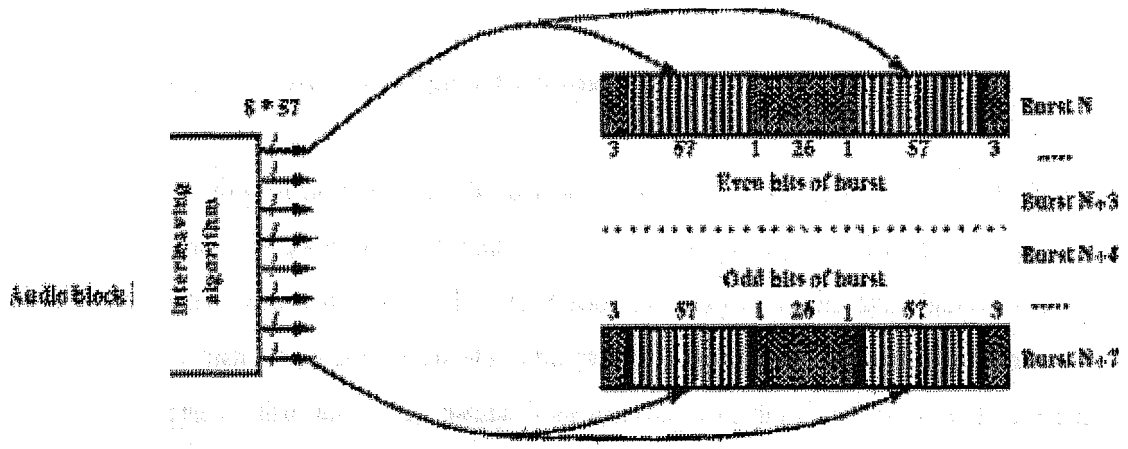


Figure 2.4111.terleaving Operation

De-interleaving consists in perfotminğ" the· reverse operation. The major drawback of interleaving is the corresponding delay: transmission time from the first burst to the last one in a block is equal to 8 TDMA frames (i.e. about 37 ms).

Rearrange· a group ofbitSiı ä particular-way. It is used in combination with FEC codes in order to improve the performance of the error correction mechanisms. The interleaving decreases the possibility oflosing whole-bursts duringthe transmission, by dispersing the errors: Being the errors less concentrated, itisthen easier to correct them.

A burst in GSM transmits two blocks of 57 data bits each. Therefore the 456 bits correspondingto the output ofthe channel coder fit into four bursts (4*114 = 456). The 456 bits are divided into eight blocks of 5'7 bits. The first bloek of 57 bits contains the bit numbers (0, 8, 16...448), the second onethe'bit numbers (1, 9, 17...449), etc. The last block of 57 bits will then contain the bit numbers (7, 15...455). The first four blocks of 57 bits are placed .in-theeven-numbered bits of four bursts. The other four blocks of 57 bits are placed in the odd-numbered bits of the same four bursts. Therefore the interleaving depth of the GSM interleaving for control channels is four and a new data block starts every four bursts. The interleaver for control channels is called a block rectangular interleaver.

2.4.1 Interleaving For the. GSM Speech Channels

The block of 456 bits, obtained after the channel coding, is then divided in eight blocks of 57 bits in the same way as it is explained in the previous paragraph. But these eight blocks of 57 bits are distributed differently. The first four blocks of 57 bits are placed in the even-numbered bits of four consecutive bursts. The other four blocks of 57 bits are placed in the odd-numbered bits of the next four bursts. The interleaving depth of the GSM interleaving for speech channels is then eight. A new data block also starts every four bursts. The interleaver for speech channels is called a block diagonal interleaver.

2.4.2 Interleaving For the GSM Data TCH Channels

A particular interleaving scheme, with an interleaving depth equal to 22, is applied to the block of456 bits obtained after the channel coding. The block is divided into 16 blocks of 24 bits each, 2 blocks of 18 bits each, 2 blocks of 12 bits each and 2 blocks of 6 bits each. It is spread over 22 bursts in the following way:

l-the first and the twenty-second bursts carry one block of 6 bits each

2-the second and the twenty-first bursts carry one block of 12 bits each

3-the third and the twentieth bursts carry one block of 18 bits each

4-from the fourth to the nineteenth burst, a block of 24 bits is placed in each burst

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

2.5 Burst Assembling

The burst assembling procedure is in charge of grouping the bits into bursts.

2.6 Ciphering / Deciphering

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

Ciphering is achieved by performing an "exclusive or" operation between a pseudo-random bit sequence and 114 useful bits of a normal burst (i.e. all information bits except the 2 stealing flags). The pseudo-random sequence is derived from the burst number and a key session established previously through signaling means. Deciphering follows exactly the same operation.

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

2"-7 Modulation

The modulation chosen for the GSM system is the Gaussian Minimum Shift Keying (GMSK),

The aim of this section is not to describe precisely the GMSK modulation as it is too long and it implies the presentation of too many mathematical concepts. Therefore, only brief aspects of the GMSK modulation are presented in this section.

The GMSK modulation has been chosen as a compromise between spectrum efficiency, complexity and low spurious radiations (that reduce the possibilities of adjacent channel interference). The GMSK modulation has a rate of 270 5/6 kbauds and a BT product equal to 0.3. Figure 5 presents the principle of a GMSK modulator.

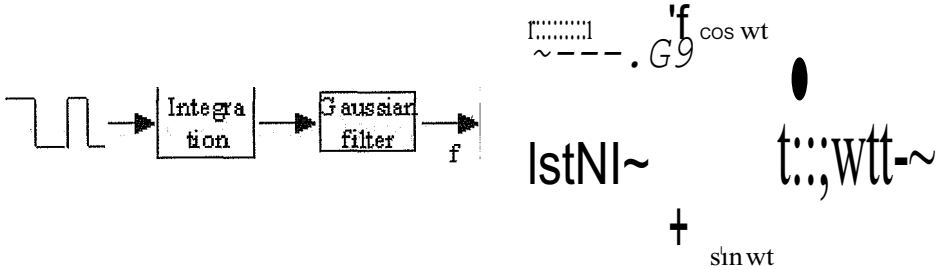


Figure 2.5 GMSK Modulator

GSM uses the Gaussian Modulation Shift Keying (GMSK) with

I-modulation index (deviation ratio) h = $Tb(f1 - f2)$ = 0.5

2-BT (filter bandwidth times bit period) equal to *0.3*

3-modulation rate of 271 (270 5/6) kbauds

The GMSK mqdulation has been chosen as a compromise between a fairly high spectrum efficiency (of the order of *1* bit/Hz) and a reasonable demodulation complexity. The constant envelope allows the use of simple power amplifiers and the low out-of-band radiation minimizes the effect of adjacent channel interference. GMSK differs from Minimum Shift Keying (MSK) in that a pre-modulation Gaussian filter is used. The time-domain impulse response of the filter is described in Equation (1), where $k1 = \frac{1[}{-v2In2}$,

and $h(t) = \frac{k_1 B}{\sqrt{\pi}} e^{-k_1^2 B^2 t^2}$ and $\mu = 0$, therefore

$$\sigma = \frac{\sqrt{2}}{k_1 B} \tag{5}$$

And B is the half-power bandwidth. The Viterbi algorithm can also be used as a Maximum Likelihood Sequence Estimator (MLSE) equalizer. So a GSM receiver can contain two different implementations of the Viterbi algorithm.

2.8 RF Power Levels

Radio equipment in GSM can be classified by the various power classes that correspond to different transmitter power levels. Table 1.1 shows the characteristics of each power class for both mobile stations and base stations. The minimum mobile station power level is *20* mW *(13* dBm).

Table 2.1 Power Levels In The GSM System

Power Class	Maximum Power of a Mobile Station / (dBm)	Maximum Power of a Base Station / (dBm)
1	*20 W(43)*	*320W* (55)
2	*8W(39)*	*160* W(52)
3	5W(37)	*80 W.(49)*
4	*2* W *(33)*	*40W(46)*
5	*O.SW (29)*	*20W(43)*
6		*JOW (40)*
7		5W *(37)*
8		*2.5* W *(34)*

2.9 Discontinuous Transmission (DTX)

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

1- The Voice Activity Detection (VAD), which has to determine whether the sound represents speech or noise; even if the background noise is very important. If the voice signal is considered as noise, the transmitter is turned off producing then, an unpleasant effect called clipping.

2- The comfort noise. An inconvenient of the DTX function is that when the signal is considered as noise, the transmitter is turned off and therefore, a total silence is heard at the receiver. This can be very annoying to the user at the reception because it seems that the connection is dead. In order to overcome this problem, the receiver creates a minimum of background noise called comfort noise. The comfort noise eliminates the impression that the connection is dead.

2.10 Timing Advance

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

2.llPower Control

At the same time the base stations perform the timing measurements, they also perform measurements on the power level of the .different mobile stations. These power levels are adjusted so that the power is nearly the same for each burst.

A base station also controls its power level. The mobile station measures the strength and the quality of the signal.between itself and the base station. If the mobile station does not receive correctly the signal, the base station changes its power level.

2.12 Discontinuous Reception

It is a method used to conserve the mobile station's power. The paging channel is divided into sub channels corresponding to single mobile stations. Each mobile station will then only 'listen' to its sub channel and will stay in the sleep mode during the other sub channels of the paging channel.

2.13 Multipath and Equalization

At the GSM frequency bands, radio waves reflect from buildings, cars, hills, etc. So not only the 'right' signal (the output signal of the emitter) is received by an antenna, but also many reflected signals, which corrupt the information, with different phases.

An equalizer is in charge of extracting the 'right' signal from the received signal. It estimates the channel impulse response of the GSM system and then constructs atf)in.vetse filter. The receiver knows which training sequence itı:ntlst wait for. The eqtt.alizerwill.then., comparing the received training sequence with the training sequence it was<expecting, compute the coefficients of the channel impulse response. In order to extract the'right' signal, the received signal is passed through the inverse filter.

2.14 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 servıces:

1-El: 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.

2.14.1 Teleservices

1- Telephony (El® Eh).

2- Facsimile group 3 (El).

3- Emergency calls (El® Eh).

4-Teletex.

Short Message Services (El, E2, A). Using these services, a message of a maximum of 160 alpµanumeric 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 aıı answering macµine.

2.14.2 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 (El).

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

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

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

2.14.3 Supplementary Services

Call Forwarding (El). 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 (El).

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

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

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

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

-Call holds (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.

- Çonnected 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.

CHAPTER THREE
The GSMRADIO INTERFACE

3.1 Introduction

The radio interface is the interface between the mobile stations and the fixed infrastructure. It is one of the ınqst 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 pan;jctı1arly in aspects such as the capacity of the system and the ted.1.riiquesused in order to d~pr~·. se the··· i···t···erference,a,ıdto i°/prove thefrequency reuse .sclı1,me. Thespecification of the radio intt:ı;f~~~ has then an imp9ırtant influence on the spectrum efficiency.

3.2 Frequency Allocation

Twocfreqaencybanps, ôf25 MHz e~ch one, have been.allocated for the •GSM system:

1-Fhe band 890-915 MHz has been allocated for the<ttplink directiôfüi(transnıittirrg from the mobile station to the base station).

2-The band 93 5-960 MHz has been allocated for the d0wnlinkdirection (trartsmitti:riğ from the base station to the mobile station).

But not allthe countries can use the whole GSM frequency bands. This is duc,:.pr:in~il[?.~llyto military reasons and to theexistence-of previous analog systems using part oftheitwo·25 MHz frequency bands.

3.3 Multiple Access Scheme

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

3.2.1 FDMA atıdTDMA

Using FDMA, a frequency is assigned to a user. So the larger the number ofaısers 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 witl:ta 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 carrierfrequencyis 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 klfz, into 8 bursts. A burst is the unitoftim.e in a TDMA system, and-it lasts approximately 0.577 ms. A TDMA frarne.is formed with 8 bursts. and lasts, consequently, 4.615 ms: Each -of the eight .bursts,;thatform.<a TDMA frame, are then assigned-to a sinğle.user.

3.4 GSM Channel Structure

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

It also distinguishes 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. Ina GSM system no RF channel and no slot is dedicated to a priori to the exclusive use ofanything (any RF channel can be used for number ofdifferent uses).

Logical channels are divided into two categories:

I) Traffic Channels (TCHs)

ii) Control Channels.

A channel corresponds to the re:cürrehce 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 ,sc,111.e- channel maintenance tasks, We have already iıtrôdticed the physical channels used iıı GSM,'namely 8 burst periods per frameon afi FBMAcarrier.

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 ll;the burst period acts as a TCH, In frame 12, it acts asameans 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 periedrü) is used in a similarly manner to separate when different "types" of signalling information (or channels) are transmitted

3.4.1 Traffic Channels (TC)

A traffic channel (TCH) is used to carry speech and data traffic. Traffic channels are defined using. a 26-frame multiframe, or group of 26 TDMA frames,>The.lengthiOfa/26-frame multiframe is 120 ms, which. is how the length of a burst pepiôd<is 9~:fitıed (120 ms divided by 26 frames divided by 8 bı.ırst periods per frame). Out ofthe26 frames, 24 are used for traffic, 1 is usyd for the Sl9w Associated Control Channel (SACCH) and 1 is currently unused. TCHs·for the ·uplinkand}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 Brlı) 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 2,6-Multiframe. The Zô-Multiframe lasts consequently 120 ms. In this 26-Mıntifr'<:1111e structure, the traffic channels for the downlink and uplink are separated by 3 bur$tS.. 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.ı'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 theişystertı, .are .also grouped in a 26-Multiframe *pıut* the internal structure is different, TCII.areı:ılsq.qlcı.ssified accord to the type of traffic that.they areçı:ırryiıng

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 perburstperiod)

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

3.4.2 Control Channels

Basic structure of Control channel

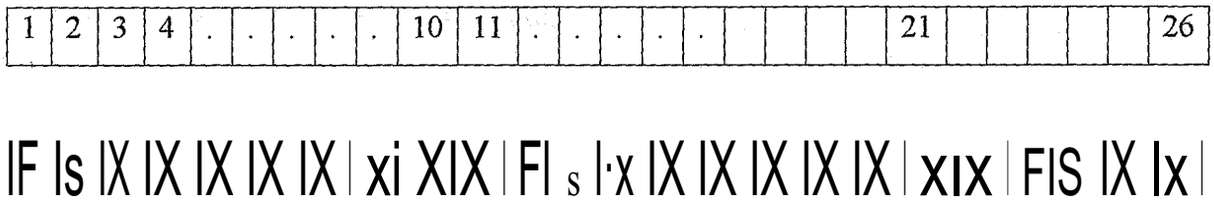


Figure 3.1 Basic structure of Controlchannel

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:

I-Broadcast Channels (BCE-I)

2-Common Control Channels (CCCH)

3-Dedicated Control Channels (DCCH)

4-Associated Control Chanp_els (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 sta.tio11 the training Sequence needed in ôrde:rto<.deriıôdula'.ithe information transmitted by the base. station,,Broadcast channels are transmitted/by the base station to convey "information" to.ALL MS iri the cell Three different "logicaP'BCH exist information necessary for the MS tô registeritı 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 slotl 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 coınınuıı.cationand is unidirectional; there is no corresponding uplink. The signal strength-is .cotıtinµously measured by all mobiles which may seek a hand over from its present cell and thus itis 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. peı.i.qd 0 on only one (non-hopping) carrier in a cell The BCCH is a point-to-multipoint unidireptional contre>k.channel from the fixed subsystem to MS that is intended to broadcast a variety of informı:ıJion to. MSs, including information

necessary for the MS to register in the system. BCCH has 51 bursts. BCCH is dedicated to slot 1 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 ofBTS). 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 pcirıt-tcsmultipoint (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:
I-paging channel (PCH)
Which is used to search (page) the MS in the downlink direction; .. The.Paging Channel (PCH). It is Used to alertthemobile.station of an incoming call

2-random access channel (RACH)

The Random Access Channel ~CH), which. is used by the môbife sfatiôri fo<request access to the network which is us~~\by MS to' r~quest of" a:ll 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. Acombined paging and access grant channel is designated as PAGCH. The Access Grant Channel (AGCH). It is used, by the base station, to inform r;,the mobile station about which channel it should use. This channel is the answer of a base ·Tzfgtation to a RACH from the mobile station ıAccess Grant Channel (AGCH) is used by· BS to tell MS which OCH to use after it has sent a message over.the RACH

- **Dedicated Control Channels (DCCH)**

TheStandalone Dedicated Control Channels (SDCCH) are allocated to specific mobiles to exchange information with.ehe networkfor.a specific duration

A typical use offhe SDCCHwould be to exchange signalling relating to a call set up.

ADCCH 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 ofDCCH can be defined:

Twotypes ofDCCHs used are:

1- Standalone DCCH (SDCÇH)

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-ever 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:

I-Slow ACH (SACCH) whiçh 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 'I'ÇH: .bursts (frames) to convey "urgent" signalling information (e.g, handover, power coıntrol, timing advance) The Fast Associated Control Channels (FACCH) replace all.or part9f 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 0£ a CCR. 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 mod.e./.Tlıig nıe.a,ns.Jhat.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 atthehaiıd over. The user will not hear the interruption ofthe speech since it lasts only for·20 ms and cannot sensed by human ears.

3.5 Structure of 'fDMA Slot with a Frame

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

1- Normal Burst

2- Synchronization Burst

3- Frequency Correction Burst

4... Access Burst

5- Dummy Burst

3.'5.1 Normal Burst

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

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

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

3.5.2 Synchronization Burst

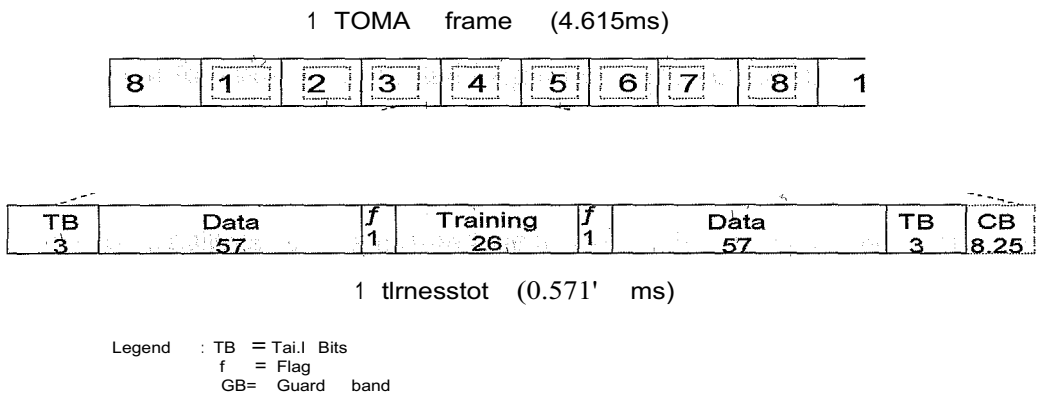


Figure **3.1** GS:M; TOMA Structure And Normal Burst Number Of Bits Per Field Below the Field Legend

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 TOMA frame number alo,ng.withthe BSIC. It is broadcast together with tl;ıe correction burst. The TOMA frame is b,rğaf.{9~st. over SCH, in order to protect the user information against eavesdropping, whi¢hisacco'mplished is ciphering the information before transmitting. The algorithm that· calcıılates the ciphering key uses a TOMA frame number as one of the parameters and therefore, eve~Jtame must have a frame üumbero:By knowing the TOMA frame number, the mobile will know what kind of logical channel is being transmitted on the control channel TSO. BSIC is also used by the mobile to check the identity Ofthe BTS when making sign~l strength measurements (to prefenttrieasurements ollcôfchaıınel cells).

3.5.3 Frequency Correction Burst

This burst is used for fr~quency synchronization of the mobile. It is eqµ.iy~l~p.tyto an un-modulated channel with a specific frequ~ııcyoffset. The repetition ofthese bursts are called FCCH.

3.5.4Access Burst

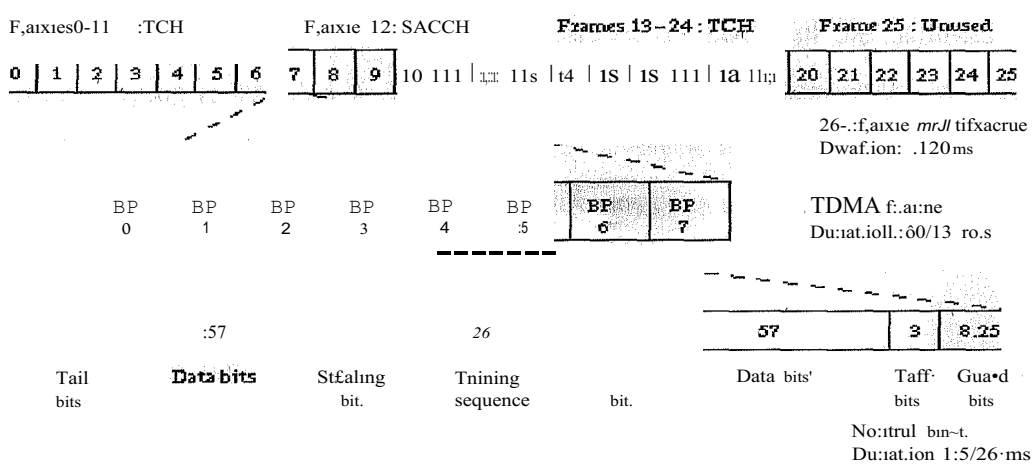
This burst is used for.random access and-longer GP to protect for burst tra:p_smissiônfrö:rı:ı a mobile that does not know the timing advance when it must access the system.

'This allows for a distance of35 km from-base to mobile. Inease the mobile is far away from the.B'I'S, the initialburst 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 followingthis.

3~5.5Dummy Burst

Ifis sent from BTS on some occasions as discussed previously which carrıes ne information and has the format same as the normal burst.

The normal burst.Js µs~d to carry speech or data information. It lasts approximately 0. 577 ms and has a length ofl56.25 bits. Its structure is presented in figure 3.2.



Fig~re 3.2 Structure ofthe 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 GSMsites)

of a burst. They are used to cover the periods of ramping up and down of the mobile's power.

The coded data bits correspond to two groups, of 57 bits each, containing signaling or user data.

The stealing flags (S) indicate, to the receiver, whether the information carried by a burst corresponds to traffic or signaling data.

The training sequence has a length of 26 bits. It is used to synchronize the receiver with the incoming information, avoiding then the negative effects produced by a multipath propagation.

The guard period (GP), with a length of 8.25 bits, is used to avoid a possible Overlapof two mobiles during the ramping time.

3.6 **Frequency Hopping**

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

There are different types of frequency hopping algorithms. The algorithm selected is sent through the Broadcast Control Channels, Even if frequency hopping can be very useful for the system, a base. station does not have to support it necessarily On the other hand, a mobile station has to accept frequency hopping when a base station decides to use it.

CHAPTER FOUR
LEVELS of RADIO FRECUENCY RADIATIÖN FROM GSM MOBILE TELEPHONE BASE STATION

4.I Introduction

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 öf these başe 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 Eneq~y (EME) Public Health Issues (CE~ffiPI-II),.as part of the public information component of .its RF EME program, considers it important that the general pµblic be informed about the RF EME levels tp yYhiçh they may be. exposed. Accorcl~ngly,the. CEMEPHI requested the Australian•.Radiation Protection and Nuclear Safety Agency (ARPANSA) to carry out a survey .of the.RF El\IB levels in the vjdriJtY of nıobile. telephone base stations. This report prt>yig~~ information on the levels of RFradiation from RF transmitter toyvers:(!Ja,est.ati<nxs)J~ which members ofthe public may be exposed. Reviews on the potential healthtisks of RF radiation are available elsewhere.

A survey .on RF EME in and around five Vancouver.schools by 1flj.ansandoteet 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 br.oadcasts. A US study by Petersen and Testagrossa (1992) characterized RF EME fields in the vicinity of several frequencies 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/rn 2 per transmitter. Hence, in a worst-oase scenario of 96 transmitters operating .at.an Effective radiated power (ERP) of 100 watts per transmitter; the aggregate maxlmumpower-density was estimated by Petersen and Testagrossa to be below O.Ol W/rn$_2$. 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 biiildirıgs with.antennas, were not exceeded'.

The purpose of the work reported here is to provide data on RF EME levels at independently nominated sites,' over the range öf the digital Global System for Mobile communication (GSM) mobile telephone base stations frequency· hand (935 - 960 MHz), and to make cönipafisoris wıth the limitfor non-occupational exposure specified in the relevant Australian exposure standard. The Radio communications (Electromagnetic Radiati61'1Hürnah:Expôstıfe}Standard1999 adopted by the Australian Communications Authority (ACA) requires mobile phones and mobile phone base stationsfo conıplfwiththe exposure Iinıits in the interim Aııstralian and New Zealand Standard 2772.l(Iııt): 1998wfiichhas now been withdrawn by Starıdards Australia.

The ACA standard is subsequently abbreviated as ACAS illthis publication. The nôn-occüpatiohal exposure limit specified in the ACAS, 6*-ptesSed in' terms 6fpöWeffü.ix density, is 2 W/n:$_{12}$ (equivalent to 200 µW/cm$_2$)fôr frequencies between 10 MH.ziafici 300 GHz, averaged over a 6 minute period. It should befiotecl that the exp6Surelinıits'!ıh the ACAS werif'developed bıı the basis of there beirtg a thresholcl. Sf 4iw/teğ>\vıı6İ~ body specific abs6rptiöll rate (S.AR)befôre aııy adverse heitlth··cdn§~qü~rit~ste likely to appear'. However, because the SAR (units W/kg) is difficult and often impractical to measure, the ACAS provides derived levels ôf electric (E} and 'magnetic'(H) field strengths, as well as the equivalent plane wave p6wef 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 rncoiie phone system (AMPS), VHF TV UHF TV, AM radio, FM radio and Paging.

4.2 Measurement Locatiensand Type ofthe Measurement Required

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 ofthe measurements required.

4.2.1 Fixed Site Environmental Measurements

Broadcastcommuniçation 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 ofeffeçtj:ve)rycypt~o°:frequently ~xtending t9 mally hundreds of kilometers from a single station transmitter. Furthermore, for such sources and considering their. necessary broadcast design reqtıit}'\mertts, we do not expect to encounter .sigıiificant or strong variations in signal stF~ngth in relatively open areas surrounding aimopile telephone base station. Given. the nature and emphasi~:.grc<>gı study we therefof(;)/a.d.9pted a .protoc91of mal<il1g a single set of sta.tic enyir9mp.(;)p;ta.ı measurementsfşr all,Rt;()adcast .s9llr9es otlıert~an fil{}bileJelephon(;) b<l.Se. statio11s.

Buildings or other likely objects may significantly attenuate or scatter the RF signal. Hence, where possible, measurements "l'eJ.Jt.ınade in locations that maintained direct line-of-sight with known RF sources, at. a heigµt of'l? metersabove ground, in open

areas in the near vicinity of the GSM base station of-interest. Measurement antennae were oriented to obtain maximum signal strength for the particular frequency band being· measured. The environmental RF EME signals were measured at a location within 500 meters ofthe 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, .FMradio 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 project. To measure the environmental RF EME levels the average RF EME levels over a six minute scanning period during the day was determined. Thetime taken to record all.the relevant sources ofenvironmental RF EME at each site was·approximately one· hour. A spectrum analyzer was used and some transient signal sources.

Such as paging services, mayhaveigone undetected if by chance.the relevant frequency band was notswept by the spectrum analyzer when the signalwas transmitted,

4.2.2 GSM Base\Sıatfün Activity Measurements

The primary aim of this study was tôidetermine the RF EME/levelresulting from all signaLfrequencies produced by the particular GSM base stations under survey. Mobile telephone <Communication signals are both transient and> partly random. in>their occurretıce.ı:ınddistribution. In this context, we were interested in determining-the RF EME·<levels a,t;.many locations· 'and .mere-particularlyj-we wanted to estimate-both maximumSatıd,minimumdevels and-also the ··long .term average value·for each location and to map suchtlevels in the area surroundingıthe.0base station, Because telephone communications are based oh humaneactivity.

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 cdaily 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 ofGSM base stations there is a possible minimum of' eight and a possible maximumcofnthirty-two.eime slots for any given sector:

Hence, .eight time slots will amount to <25% of the fota! activity possible frôm. the transmitting antenna of a single carrier GSM base Station.

The digitahGSM 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 .of0.6µsec with a repetitiollrate öf217 Hz. The temporal RF EME levels .ôf the transmitting antennae .at: GSM base-sstaıions- were analyzed identify contt81 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 frequencysrandomized to avoid bias. The system was optimized to gather as much data as possible by sampling more often when fewer frequencies were detected. Postlogging data analysis was performed to determine the average activity: over a six+rniniıte scanning period, yielding an activity .value.for every<six. minutes of the day.. {I'he analysis software included only the·signals.identified-as.belenging to the base<stati~nt\iri question- Where/more than one caa-ier.(Telstra, .Optuseor.Vodafone}ishated•lhe•saıne tower, the com.bined•activity··fromall carrierscwassdetermined... Aidiutnal .coı-:rection factor was derived from analysis ofthe 24-hour activity measurements for use in mobile measurements.

4.2.3 Mobile GSM Base Station Area Measurements

A fixed antenna was roof mounted on.a car and automated n;ıobile measurements were made whilst driving around the streets near the GSM base station under survey. Both signal data and position.dnformation [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 :frequencywill have similar propagation characteristics to those·öf 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 EMEpver 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 ate presented in the individual reports for each survey site.

4.2.4 Equfpment

All RF EME measurements were recorded using a portable Tektronix Model 2712 Spectrum Analyzer. This instrument is essentially a radio receiver with the capacity to measure the power distribution of a received signal as a function of frequency. Signal amplitudewasusuallymeasuı:ed.indB relativeto a mill watt (dBm). Calculation of field strength requires knowledge of the rec¢iviıı.g antenna.properties and system losses.

Because the dBm measurements were all recorded in the far field of the transmitting antennae, the measurements results could be converted to equivalent electric field strength in dB relative to microvolt per meter (dBμV/m) using the following equation:

Field strength (dBμV/m) = dBm measurement+ 107 + receiving antenna factor +cable loss factor + spectrum analyzer calibration factor.

The field strength values (in dBμV/m) were subsequently converted to power flux density. Power flux density (S) is commonly expressed in units of microwatt per square centimeter (μW/cm2} and;<inthe far field ofa transmitting antenna, can be calculated from the plane wave relationship:

$$£_2 = Z*S \quad (5)$$

Where Eis the electric field strength (units Vim) and Z is the characteristic Inıpedance of free space (377ohms).

The spectrum analyzer was interfaced to and controlled, via a communication.ca1;4l,y a portable laptop computer based data logging system utilizing a portable QPS re9~iyer The receiver.was operated in differential mode.

GS:M and AMPS povyer,densitymeasurements were recorded from the signals radiated by the mobile telephone base stations. The signals measured by the spectrum analyzer, over the. frequency ranges specified. below, were received using a variety 9f antei;ıiiae. Each receiving antenna was calibrated at relevant frequencies, and the calibration factors were u.sedin tlıe calculations of the RF EME levels. The overall ups~μainty of the measurement resμlts is estilllatyd to be ±. 6dB.. The following .re9eiying a11tennae were used:

17 Low frequency signals (AM radio); 0.0 LMHz - 3Q MHz loqp antenna; EMCO model 6502 active. loop. This antenna was used fqr< the stationary enyirq#me:tj.tal measurements;

2-Yery High Freqμe11cies(FM.raqio,va:F 'fy,paging); 20 MHz - :320.MHz.bi-;.goı:ıfoal antenna; A.H. Systeins model SA§..gQ0/~41. This antenna.was used for the.stationary environmental measurements.

3-Ultra High Frequency (UHF TV, mobile telephone, paging); 300 MHz - 1000 MHz log periodic antenna; A.H. Systems model SAS 200/510. This antenna was used in the

environnıental and base station activity measurements; and Mobile phone frequencies; 870 MHz - 960 MHz magnetic base vehicle roof mount antenna; supplied·by·Telstra Shop. This antenna was used to determine 24-hour base station activity levels -and mobile area survey measurements.

4.3 Results for RF EME Exposure and Activity Levels from GSM Base Stations

Figure 4.1 illustrates the overall changes in activity at each measurement locality. The three symbols in the graph correspondto the minimum activity, average activity and maximum activity over the 24-hour period. The full names for the locality abbreviations given in Figure 4.1 are as follows: Bulleen (Bul), Bunbury (Bun), South Melbourne (SMe), Repatriation Hospital (Rep), Rapid Creek (Rap), Palmerston {Pal); Nerang (Ner), Launceston (Lau), Kenmore' (Keri), Jolimön:t (Jol), Hobart (Hob), Fulhartı {Ful) and Engadine (Eng). For graphs displaying the temporal variation in activity over the 24-hour period at each-indisidual-sirerefer-te'the specific report for that locality.

Across allGSM base stations the average·ofthe 24 hour variation in telephone activity was 32%<ofthetotal available capacity (a factor-of l.2Tccımpared with the minimum operational capacity of 25%), with the maximum base station activity averaging 48% of the total available. capacity.. The.ilargest<chariğe<possiblcis ati increase by a factor of four, which occurs when fourtransrrıitters are operatingiatfüU pcıwer. Bulleen;>f\ı'ic:\had the la:rgest.nıeasuredvariation in activity. For this site there was a'cha!ıigeinactivity<cıf 40% witherespect-to-the -totai-available capacity (a factor of 2.6 compared<witfüthe minimum operational.capacity of25%).

The smallest variation in activity was at Bunbury and Fulham, where no change in activity over the 24-hour period was recorded (i.e., it remained at 45% capacity).·

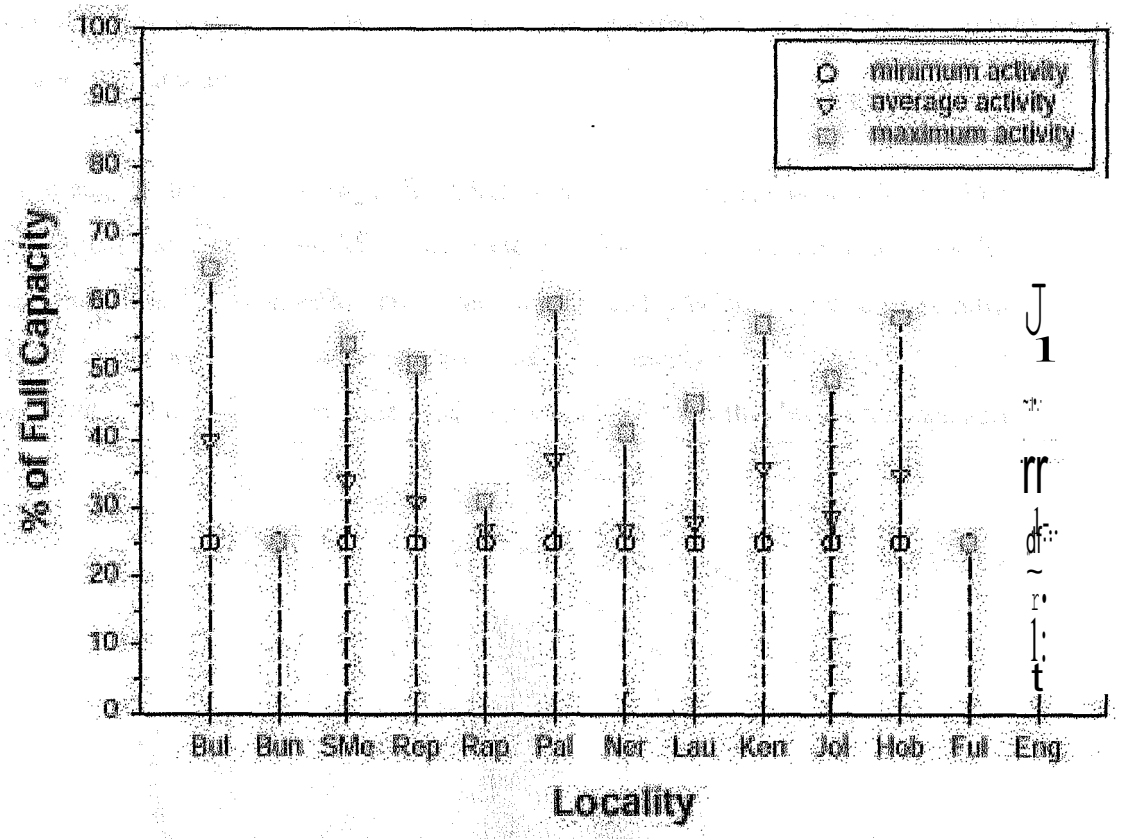


Figure4.1: Activity levels of GSM Base Station.

The changes in activity of GSM base stations over a 24-hour period are illustrated. The full names for the locality abbreviations are given in the text.

Figure 4.2 displays •graphically tlıe BŞNI.R.F' Elv1E İe'\fels for the different activity levels at the 13 locations of measurell)ifi:~!ttr~~Cii;,1;1gure 4:2 the 'area a~' RF EME levels was considerably less than the <highest average' RF EME levels at most sites. The largest of the 'highest average' RF El\1E··ıevels was at Kenmore(():052 µW/cm~..... th~Jimit.sp'rcifj~ij in th~t~CAS is at le~.stJ,()J!)Oti~~s great~fth~n tlıişJeVel), as was the largest of the 'area average} RF EME levels (0.0051 µW/cm^2 - the limit specified in th¢.•.A€;.AStis·atileast 30~0ô0ttimes(greater than this Jevel):•At•· ma,dmtlın activity the largest .R.FEME·&ecurr¢d atI<.eitmtirei(0.082·µW/cm~. ...;(/tp.¢r1imit :Specified in' the ACAS is atleast 2,000 times greater than this level), whilst.at TOO% ·activity the largest RF EME Wfl.~ at Nerangr(Q.178 µW/cm2 - the limit specified in the ACAS is 1,000 times greater than thiş level). The mean of the 'highest average' RF EME levels

over all sites was 0.020 µW/cm² (the limit specified in the ACAS is 10,000 times grcaterthanthis level).

The mean of the 'area average' RF :EME levels over a.U sites.was 0.0016 µW/cm² (the limit specified in the ACAS is at.Jeaşt 100,000 times greater tharı this level). For maximum and 1000/o activity the· meanş were 0.031.JıW/cm² (the liinit. specified in the ACAS is at least 6,000 times greater than this level) and 0.062 µW/cm² (the limit specified in the ACAS is at least 3,000 times greater than this level) respectively.

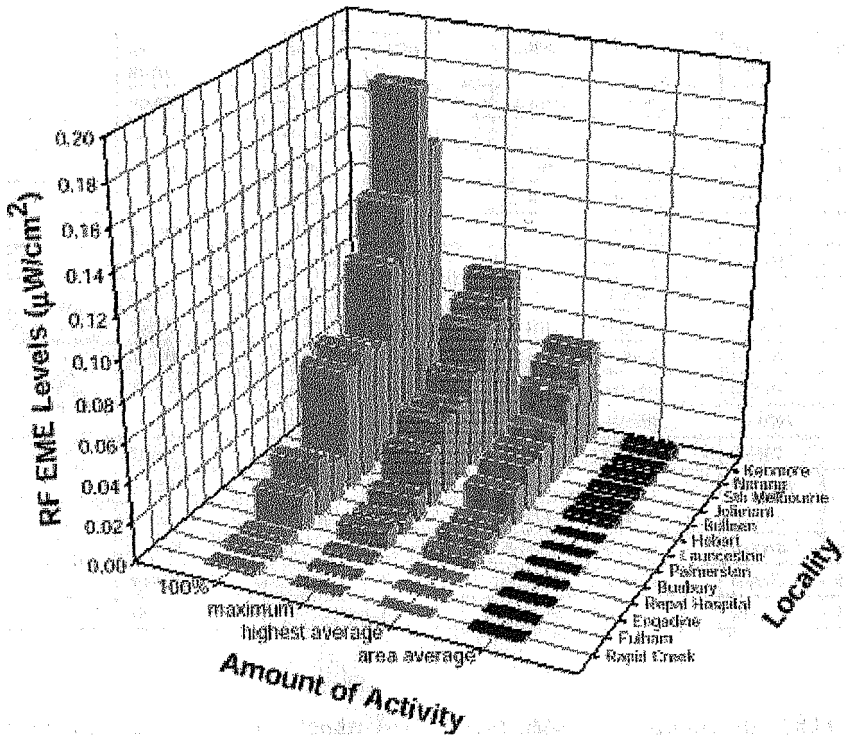


Figure 4.2: RF Power Flux Density Levels (µW/cm²) fot GSM Base Station

The above .3D plot is of the GSM base stations RF EME power flux density levels for the 13 different locations, at different activity levels. For explanations of the different activity levels see the text.

4.4 Fixed Site Environmental RF EME Levels from Various Signal Sources

Table 4.1 lists the average fixed site environmental RF EME power flux density levels over a six-minute scanning period for the.different signal sources at the 14 base stations'. In this project the reference to RF EME levels always implies power flux density levels μW/cm2.

Table 4.1 Environmental RF EME Power Flux Density.

Location	FM Radio	AM Radio	GSM	AMPS	UHF TV	VHF TV	Paging	Total RF
Bulleen	<0.0001	Ô.2282	Ö.0001	<0.0001	<0.0001	<0.0001		0.22~4
Bunbury	<0.0001	0;0010	<0.0001				<0.0001	0.0010
SthMelboume	<0.0001	0,0662	0.0023	0.0004	UHF+VHF=	0.0002	0.0002	0.0693
Repathospital		0.0822	0.0012	0.0001	<0.0001	·<0.0001		0.0835
	0.0010		0.0002		<0.0001	<0.0001		0.0069
					0.0018	<0.0001	<0.ÖÖOl,	0.0280
					0.0001			0.0010
				0.0011	0.0047	0.0032	0.0001	0.0837
					0.0003	0.0001		0.0661
					<0.oooı	0.0002	<0.0001	0.0023
					<0:0001			0.0612
Hobart				<0.0001	@001			0.0058
Fulham								0.0643
Engadinc				0.0001				0.0043
Mean	0.0024			0.0003				0.0504
SD	0,0011			0;0004	0.0014	0.0010	0.0001	0.0611
N	13			6	12	11	7	14

At therb9ttom of Tabte 4.1 the me.arı/levelsand standard deviation (SJ;.>) :are'given, as well aS/the number of sites (N) where signals were detected. It is emphasized tfüitthe envitonın.enfal.'RÆME levels are only given as·a guide. Except.fbr G;SM;the/ciistances from the signal •·sourcesof the: RF EME power. flux density measıtrements \¥@re .:tıôt known or. considered. iHen<ı:e,Jif\thɛnv orcR.adio broadcasting transmitter was very distant then this may underestim4te the typicai population exposure to those RF sources. Likewise, *if* the .broadcastingtransmitters w~re-very.close,su~hias the FM transnıittet at Palmerston, then this may overestimate the typi¢~k populatiô1:1./e:iq?psuretothose RF sources. Generally, transmitter TV and radio towers te;nd.tobe much:lıigh~rand further away from population areas than base stations. Also, with these other RF sources the

wavelength of the RF EME radiation is longer and.there is a more uniform.distributi011 of the signal.'Figure 4.3 is a presentation of the environmental RF EME levelsofalltlıe signal'sources, atthe 14 locations of measurements.

As is illustrated in Figure 4.3, AM radio signals were the dominant signal sourceıover all the other signal sources combined in 1 I. of the 14 sites of measurement, and in seven ofthese localities AM radio contributed ::„95% of the total.Rf EME (Le., at.l;lulleen, Bunbury, Fulham, Jolimont, Launceston,.Repatriation Hospital, South Melbourne).

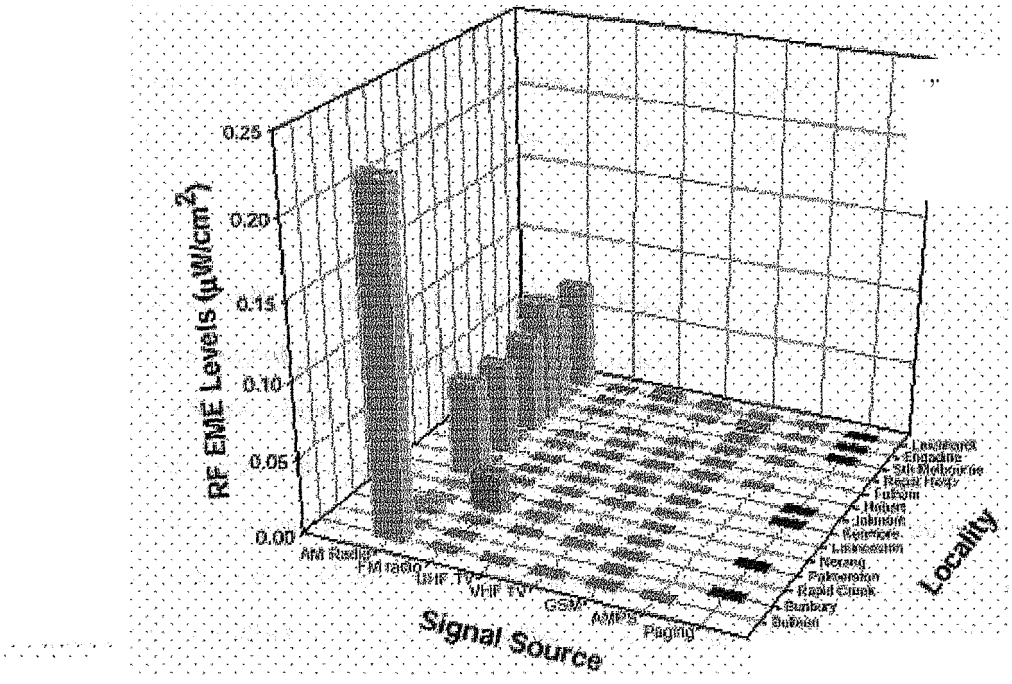


Figure 4.3: Environmental RF EME Powel'Fluk beıısity Levels µW!tirı2

The above 3D plot is of the fixed site environmental RF EME power flux density levels from the 14 different locations. All significant signal sources are plotted, including AM Radio, FM Radio, UHF TV, VHF TV, GSM, AMPS and Paging.

The largest fixed site environmental RF EME levels were at: Bulleen for AM radio (0.2282 µW/cm2 - the limit specified in the ACASis at least 8,000 times greater than this level), Palmerston for FM radio (0.0259 µW/cm^2 - the limit specified in the ACAS

is at least 7,000 times greater thanthis.level),.Eıiigadirıeiför GSM (O.Ö0'.27\µW/cln2 ---th.e limit specified in the ACAS is at.least 70,000 tilnes greater than this level), Leichhardt for AMPS (0.0011 µW/cm2 - the linıitspecifıedinthe ACAS is at least 100,000 times greater than this 'level); Leichhardt for tJHF 'I'V (0:()()4'7 µW/cm ^{2} ~· the limit specified in the ACAS is atleast 40,00Ötimes greater tha:titl:ıi.$:feifel),Leichhardt for VHF TV (0.0032 µW/cm2 -the limit .specifıedinthe ACAS/is at1east 60,000 times greater than this level), and South Melbourne.{or Paging (0.()002 µW/cm ^{2} - the limit specified in the ACAS is 1,000,000 timesgrɕatet than this level).

The top pie chart fixed site environmental RF EME power flux density ,ı;ır.mi,-signal sources. The bottom pie chart illustrates .,~5ıaı" have been weighted for frequency.

When all the me flux density levels from the Seven different "'+"~"'"'; Jögɕther the RF radiation from the base stations (AMPS and GSM vvıuuın "..u, of the totalmean RF El\ıIB, with the GSM base stations proportion being 1.4%. FM and AM radio contributed 4.7% and 91% of the total mean RF EME levels, respectively. However, a more meaningful comparison is obtained when-the signals-have beenweightedfot·frequency.<When this is done the RF radiation from the base stations (AMPS and GSM combined) contributed 11% of the total mean RF EME, with'the GSM base stations proportion being 7.7%. FM and AM radio contributed 26% and 51%ofthe total mean RF EME levels, respectively. A pie chart comparison of the ratio (in percentage) ofthe mean RF EME levels between the significant fixed site environmental signal sources is shown in Figure 4.4.

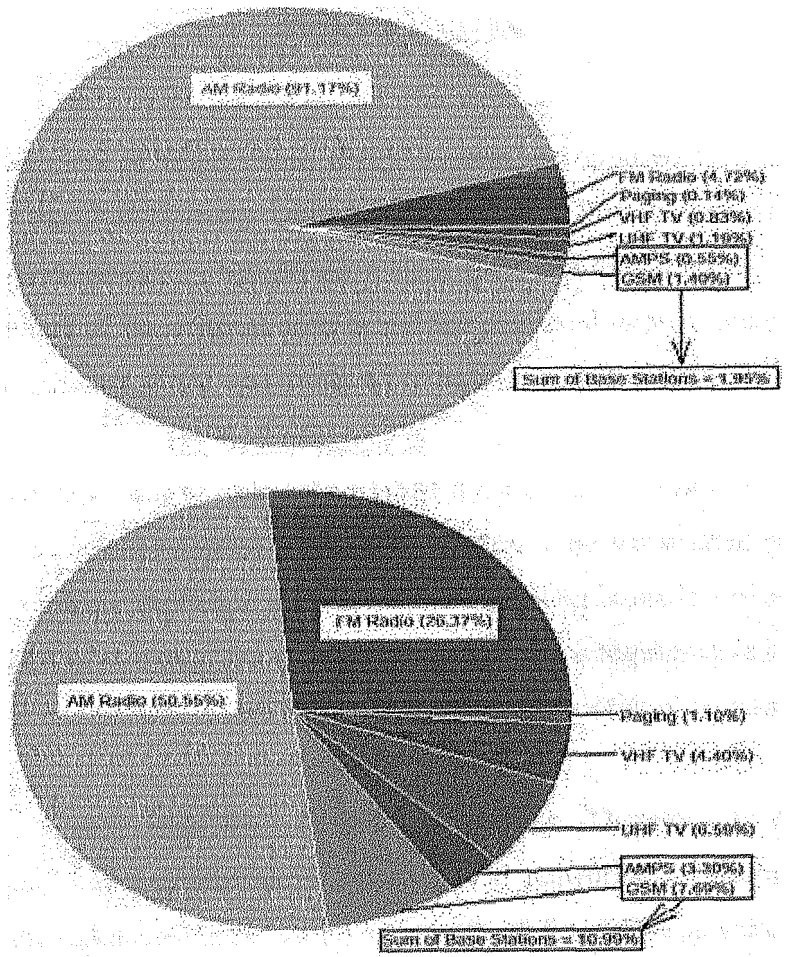


Figure 4.4: Ratio of Mean Environmental RF1?o-wer Flux D¢nsity Level.

CONCLUSION

The developers of GSM chose digital system, as opposed to cellular systems like AMPS in the United States and TACS in the United .L'-'"~'"'"-'"'· had faith that advancements in compression algorit4ms and digital allow the fulfillment of the original criteria and the continual improvement of the '"'"'~'"'·' terms of quality and cost. GSM was designed to be compatible with ISDN services.

Protection has been introduced in GSM by means of transmission ciphering. The ciphering method does not depend on the type of data to be transmitted (speech, user data or signaling) but is only applied to normal bursts; Ciphering is ıısed to protect signaling and user data. The BIR is also used for security purposes. It is a register containing information about the mobile equipments. More particularly, it contains a list öf all valid terminals.

One of the main objectives of GSM is roaming. Therefore, in order to obtain a complete compatibility between mobile stations and networks of different manufacturers and operators, the radiq interface must be completely defined. The specification of the.radio interface has then an important influence on the spectrum efficiency. Not all the countries can use the whole GSM frequency bands. This is due principally to :militaryreasons and to the existence of previous analog systems using part of the two 25 MHz frequency bands.

AJ.l inforrnationii:ıu.stbe.ptövided on the levels of RF tadiation from RF transmitter towers (base stations) to which members of the public may be exposed. Reviews on the potenti~Vh~~lthrisks of RF .radiadon are available els.e-w-here.

RAFERENCES

[1] Fakhreddin Mamedov, Telecommunication, Nicosia, Near East University, 2000.

[2] Rhee Man Young. Cellular Mobile Communications and Network Security .Prentice Hall International Editions, 1989.

[3] Warren Hioki.Telecommunication. Second Edition. Prentice Hall International Editions, 1995.

[4]Mallinder B"An Overview of the GSM system", Proceedings of the third Nordic Seminar on Digital Land Mobile Communication.Copenhagen,September, 1988.

[5] Emelyano\T.G.A., Shwarzman VO. Digital Communication Systems. Radio and communication Edition, •MOSCOW, 1982.

[6] Jean Warland.Communication Networks.Mc Graw Hill International Editions, 1998.

[7] Jack Quin. Digital data Communications, Prentice Hall International Editions, 1995.

[BjHaıg T."The,<a-SMProgram a Pan-European effort" Proceeding of the Mobile Radio Conference.Nice, November1991.

[9] Frediflalsall.~~ta.~qı;nmunications, Computer Network and Open systems

[lOJGame,F.Bryah.Telecommunieations. Primer: Data, Voice and Video Coınmutıicatiôns. International Editions, 1999.

[11] Calhoun G.Digital Cellular R.adio.ArtechHouse,1988.