NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Electrical and Electronic Engneering

GSM ARCHITECTURE AND CELL PLANNING

Graduation Project
EE- 400

Student: Umut Şahin Gül (970307)

Supervisor: Prof. Dr. Fakhreddin Mamedov

Lefkoşa - 2002

TABLE OF CONTENTS

ACKNOWLEDGMENTS

I want to thank Prof. Dr. Fakhreddin Mamedov to be my advisor. First, at the beginnig of this semester he gave me another subject for graduation project, which I want. Later, he changed my graduation project subject to this. But, I had not any knowledge about this subject and I really didn`t want it. Under his guidance, I like this subject and learn a lot about GSM. With this event, he showed the way of success to me. He helps me a lot in my study. He shared his knowledge and special documents with me to give some idea about my project.

I want to present my thanks all Professors, Doctors and education staff of Electrical and Electronic Engineering Department of Near East University. During my education along four years, they presents their knowledge without any boring and dread. Also, I will represent my professors, doctors and my university with these knowledge.

Special thanks to Cemal and Cem. With their kind help, I overcome many difficulties. I study with Cem`s computer for my project. Cemal helps me a lot with his experience.

I also want to thank my friends in Near East University and in Cyprus. Thanks to Erdem, Omran and Muhammed. They stand for me, when I need them and they support me all the time.Also thanks to my flatmates; Bülent, Sarp and Caner. Being with them is really funny.

And, I want to thank my family. I graduate with their endless support and love for me. My next purpose is relieving my mother`s life and brother`s life getting them to comfort. I wish they live happly and with presence. My father in the heaven be proud of me, in the end I am graduating and become an engineer as we want.

LIST OF ABBREVIATIONS

AGCH	Access Grant Channel
AM	Amplitude Modulation
AMPS	Advanced Mobile Phone System
ARQ	Automatic Request for retransmission
AuC	Authentication Center
BCCH	Broadcast Control Channel
BCH	Broadcast Channel
Bps	Bits per second
BS	Base Station
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver System
CC	Call Control
CCCH	Communication Control Channel
CCF	Call Control Function
CDMA	Code-Division Multiple Access
CEPT	Conference Europeenne des Postes et Telecommunications
CGI	Cell Global Identity Number
CM	Communication Management
dB	decibel
DCCH	Dedicated Control Channel
DECT	Digital Enhanced Cordless Telecommunication
DF	Data Frame
DRX	Discontinuous Receive
DTX	Discontinuous Transmission
EC	European Commission
EFR	Enhanced Full Rate
EIR	Equipment Identity Register
ETSI	European Telecommunications Standards Institute
FACCH	Fast Associated Control Channel
FCC	Federal Communications Commission
FCCH	Frequency Correction Channel

FDMA	Frequency-Division Multiple Access
FM	Frequency Modulation
GHz	Gigahertz
GIWU	GSM Interworking Unit
GMSC	Gateway Mobile Services Switching Center
GMSK	Gaussian Minimum Shift Keying
GP	Guard Period
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HLR	Home Location Register
Hz	Hertz
IEEE	Institute of Electrical and Electronic Engineers
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Station Identification
IMTS	Improved Mobile Telephone Service
IN	Intelligent Network
ISDN	Integrated-Service Digital Network
ITA	Interim Type Approval
ITU	International Telecom Union
kbps	kilo Bits Per Second
kHz	kilohertz
LA	Location Area
LAI	Location Area Identity
LSF	Line Supervision Frame
MHz	Megahertz
MIC	Mobile Internal Call
MM	Mobility Management
MoU	Memorandum of Understanding
MS	Mobile Station
MSC	Mobile Switching Center
MSISDN	Mobile Subscriber ISDN

MSN Mobile Service Node

MSRN Mobile Station Roaming Number

MT Mobile Termination

MTF Maintenance Test Frame

MTSO Mobile Phone Switching Office

MXE Message Center

NMT North Mobile Telephony

NSS Network Switching Subsystem

OAM Operation, Administration, Maintenance

OMC Operation Maintenance Centers

OSS Operational Subsystem

PCH Paging Channel

PCM Pulse Code Modulation

PCN Personal Communications Networks

PCS Personal Communications Services

PIN Personal Identification Network

PLMN Public Land Mobile Network

POTS Plain Old Telephone Service

PS Personal Station

PSTN Public Switching Telephone Network

RACH Random Access Channel

RCC Radio Common Carrier

RF radio frequency

RPE-LPC Regular Pulse Excited-Linear Predicture Coder

RPE-LTP Regular Pulse Excited-Long-Term Predictive

RR Radio Resources Management

RS Radio System

SACCH Slow Associated Control Channel

SCH Synchronization Channel

SDCCH Stand-alone Dedicated Contol Channel

SIM	Subscriber Identity Module
SMS	Short Message Service
SS	Switching System
SS7	Signaling System Number 7
TACS	Total Access Communications System
TCH	Traffic Channel
TCH/F	Traffic Channel/Full rate
TCH/H	Traffic Channel/Half rate
TDMA	Time-Division Multiple Access
TM	Telemetry Site
UMTS	Universal Mobile Telecommunications System
VAD	Voice Activity Detection
VLR	Visitor Location Register
WAP	Wireless Application Process

ABSTRACT

First European public cellular system is in the 900MHz range. In 1989 GSM responsibility transferred from CEPT to the ETSI, and in mid-1991 DCS 1800 was carried out in European counries. Then, in 1997 DCS 1800 was renamed GSM1800. North America made a delayed entry into the GSM with PCS 1900.

Operating high frequency gives virtually unlimited capacity. Phase 2 provides full duplex data traffic to any device fitted with GSM capability, such as a phone, fax, or pager, at a rate of 9600Kbps using the TDMA.

Interactions between GSM subsystems can be grouped in two main part: Operational; MS, BSS, NSS. Control; OSS. Operational part provides transmission paths and establishes them. Control part interacts with the traffic handling activity of the operational part by monitoring and modifying it to maintain or improve its functions.

GSM has four main functions: Transmission, Radio Resource Management, Mobility Management, Communication Management. The MS, BTS, BSC, among others, are deeply concerned with transmission. RRM controls the setup, maintanence and termination of radio and fixed channels, including handovers. MM manages the location updatingand registration procedures, as well as sequrity and authentication. CM handles generall call control and manages suplementary services.

Cellular mobile communicationis based on the concept of frequency reuseand cell splitting. The area a base station covers is called cell. The cells are grouped into cluster. The number of cells per cluster is intuitivelyrelated with system capacity as well as transmission quality. The cell size determination is usually based on the local traffic distribution and demand. Ther are following types of cells: macrocell, microcells, selective cell, umbrella cell.

Radio waves are typically generated as disturbances sent out by oscillating charges on a transmitting antenna. Since properties of UHF waves and frequency allocations liave made this the mobile telephony frequency band. Superimposing information is seldomly transmitted in the same frequncy range as it was generated. The modulation technique used in GSM is called Gaussian Minimum Shift Keying. This narrow band modulation technique is based on phase shifting.

Basic consideration of radio network survey is likely that the system operators has a number of alternative buildings, which may be used in the cellular network planning phase.

INTRODUCTION

During the early 1980s analog cellular telephone systems were experiencing rapid growth in Europe.

Today, GSM is a digital communication standard, which provides full duplex data traffic to any device fitted with GSM capability, such as a phone, fax or pager, at a rate of 9600Kbps using the TDMA communication scheme.

GSM is still growing up. There are new developments and technologies. Some of the operators have these features and more like phase 2+ features.

This thesis is aimed to examine architecture of GSM network, GSM subsystems and cell planning.

The thesis consists of the introduction, five chapters and conclusion.

The Chapter 1 introduces firstly history of GSM, continues with general overview of GSM and technology. Technology gives information about services and third generation. Then different GSM based networks are discussed. Finally there is some information about the GSM system architecture, which is related with the next chapter.

The Chapter 2 presents overview of architecture of GSM network. Then GSM subsystems are observed in details. Geographical areas of the GSM network and radio link aspects are the following topics. The GSM functions are described in the end. Finally, there is extra information about WAP and GPRS.

The Chapter 3 is concerned to the cellular concept and gives information about cells. Then basic wireless principles are studied related with cellular system. After general information, cellular phone, alternative techniques, cellular scheme, and certain cellular principles are considered. Finally two different GSM system, FDMA and narrow band TDMA systems discussed.

The Chapter 4 is devoted to nominal cell plan and examined the waves.

The Chapter 5 is concerned to radio network surveys with details. Finally radio measurements are examined.

Conclusion presents important results obtained by the author of the thesis.

1. INTRODUCTION TO GSM

1. 1. History of GSM

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. In the Nordic and Benelux countries the NMT 450 was developed, TACS in the UK and C-Netz in West Germany. The Radio com 2000 was in France and RTMI/RTMS in Italy. But each system was incompatible with everyone else's in equipment and operation and as business was becoming increasingly international, the cutting edge of the communications industry focused on exclusively local cellular solutions. These systems were fine if you wanted to call the office if you were in your own home, but not if you were with a client in another country. Also home market revenue simply wouldn't justify sustained programs of investment. As a solution in 1982 CEPT, the Conference des Administrations Europeans des Postes et Telecommunications comprised the telecom administrations of twenty-six European countries, established the Group Special Mobile (GSM). Its objective was to develop the specification for a pan-European mobile communications network capable of supporting the many millions of subscribers likely to turn to mobile communications in the years ahead. The home market revenue simply wouldn't justify sustained programs of investment so to further progress they lobbied for support from some political heavyweights. In 1985, the growing commitment to resolving the problem became evident when West Germany, France and Italy signed an agreement for the development of GSM. The United Kingdom added its name to the agreement the following year. By this time, CEPTs Group Special Mobile could argue persuasively that the standards they were developing held the key to a technically and economically viable solution as their standard was likely to employ digital rather than analogue technology and operate in the 900MHz frequency band. Digital technology offered an attractive combination of performance and spectral efficiency. In other words, it would provide high quality transmission and enable more callers simultaneously to use the limited radio band available. In addition, such a system would allow the development of advanced features like speech security and data communications. Handsets could be cheaper and smaller.

It would also make it possible to introduce the first hand-held terminals - even though in the early days in terms of size and weight these would be practically indistinguishable from a brick. Finally, the digital approach neatly complemented the Integrated Services Digital Network (ISDN), which was being developed by land-based telecommunications systems throughout the world. But the frequencies to be employed by the new standard were being snapped up by the analogue networks. Over-capacity crisis had started to sound alarm bells throughout the European Community. Demand was beginning to outstrip even the most optimistic projections. The Group Special Mobile's advocacy of digital cellular technology was on hand to offer light at the end of the tunnel. The Directive ensured that every Member State would reserve the 900MHz frequency blocks required for the rollout program. Although these were somewhat smaller than the amount advocated by the CEPT, the industry had finally achieved the political support it needed to advance its objectives. The logistical nightmare in the GSM, which followed soon left this achievement as a distant, dream so single, permanent organization at the helm. In 1986 the GSM Permanent Nucleus was formed and its head quarters established in Paris. It was all very well agreeing the technology and standards for this new product. But what about the creation of a market? It was essential to forge a commercial agreement between potential operators who would commit themselves to implementing the standard by a particular date. Without such an agreement there could be no network. Without the network there would be no terminals. Without network and terminals there would be no service. Stephen Temple of the UK's Department of Trade and Industry was charged with the task of drafting the first Memorandum of Understanding (MoU). In September 1987 network operators from thirteen countries signed a MoU in Copenhagen. One of the most important conclusions drawn from the early tests was that the new standard should employ Time Division Multiple Access (TDMA) technology. The strength of its technical performance ensured that narrowband TDMA had the support of major players like Nokia, Ericsson and Siemens. This promised the flexibility inherent in having access to a broad range of suppliers and the potential to get product faster into the marketplace. But as always as soon as one problem was solved other problems looming on the horizon. In 1989, the UK Department of Trade and Industry published a discussion document called "Phones on the Move". This advocated the introduction of mass-market mobile communications using new technology and operating in the 1800 MHz frequency band. The UK government licensed two operators to run what became known as Personal

Communications Networks (PCN). Operating at the higher frequency gave the PCN operators virtually unlimited capacity, where as 900MHz was limited. The next hurdle to over come was that of the deadline. If the 1 July 1991 launch date was not met there was a real danger that confidence in GSM technology would be fatally undermined but moral received a boost when in 1989 the responsibility for specification development passed from the GSM Permanent Nucleus to the newly created European Telecommunications Standards Institute (ETSI). In addition, the UK's PCN turned out to be more of an opportunity than a threat. The new operators decided to utilize the GSM specification - slightly modified because of the higher frequency - and the development of what became known as DCS 1800 was carried out by ETSI in parallel with GSM standardization. In fact, in 1997 DCS 1800 was renamed GSM 1800 (Global System for Mobile communication) to reflect the affinity between the two technologies. With so many manufacturers creating so many products in so many countries, it soon became apparent that it was critical that each type of terminal was subject to a rigorous approval regime. Rogue terminals could cause untold damage to the new networks. The solution was the introduction of Interim Type Approval (ITA). Essentially, this was a procedure in which only a subset of the approval parameters was tested to ensure that the terminal in question would not create any problems for the networks. In spite of considerable concern expressed by some operators, ITA terminals became widely available in the course of 1992. True hand held terminals hit the market at the end of that year and the GSM bandwagon had finally started to roll. From here the GSM became a success story. In 1987, the first of what was to become an annual event devoted to the worldwide promotion of GSM technology was staged by conference organizers IBC Technical Services. The Pan European Digital Cellular Conference. This year it celebrated its tenth anniversary in Cannes, attracting over 2,400 delegates. By the end of 1993, GSM had broken through the 1 million-subscriber barrier with the next million already on the horizon. By June 1995 Phase 2 of standardization came in to play and a demonstration of fax, video and data communication via GSM. When the GSM standard was being drawn up by the CEPT, six separate systems were all considered as the base. There were seven criteria deemed to be of importance when assessing which of the six would be used. Each country developed its own system, which was incompatible with everyone else's in equipment and operation. This was an undesirable situation, because not only was the mobile equipment limited to operation within national boundaries, which in a unified Europe were increasingly unimportant,

but there was also a very limited market for each type of equipment, so economies of scale and the subsequent savings could not be realized.

The Europeans realized this early on, and in 1982 the Conference of European Posts and Telegraphs (CEPT) formed a study group called the Group Special Mobile (GSM) to study and develop a pan-European public land mobile system. The proposed system had to meet certain criteria. In 1989, GSM responsibility was transferred to the European Telecommunication Standards Institute (ETSI), and phase-I of the GSM specifications were published in 1990. Commercial service was started in mid-1991, and by 1993 there were 36 GSM networks in 22 countries with 25 additional countries having already selected or considering GSM. This is not only a European standard - South Africa, Australia, and many Middle and Far East countries have chosen GSM. Although standardized in Europe, GSM is not only a European standard. Over 200 GSM networks (including DCS1800 and PCS1900) are operational in 110 countries around the world. In the beginning of 1994, there were 1.3 million subscribers worldwide, which had grown to more than 55 million by October 1997. With North America making a delayed entry into the GSM field with a derivative of GSM called PCS1900, GSM systems exist on every continent, and the acronym GSM now aptly stands for Global System for Mobile communications. The developers of GSM chose an unproven (at the time) digital system, as opposed to the then-standard analog cellular systems like AMPS in the United States and TACS in the United Kingdom. They had faith that advancements in compression algorithms and digital signal processors would allow the fulfillment of the original criteria and the continual improvement of the system in terms of quality and cost. The over 8000 pages of GSM recommendations try to allow flexibility and competitive innovation among suppliers, but provide enough standardization to guarantee proper inter-working 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 development of GSM started in 1982, when the Conference of European Posts and Telegraphs (CEPT) formed a study group called Group Special Mobile (the initial meaning of GSM). The group was to study and develop a pan-European public cellular system in the 900 MHz range, using spectrum that had been previously allocated. At that time, there were many incompatible analog cellular systems in various European countries. Some of the basic criteria for their proposed system were:

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

In 1989, the responsibility for GSM was transferred to the European Telecommunication Standards Institute (ETSI), and the Phase I recommendations were published in 1990. At that time, the United Kingdom requested a specification based on GSM but for higher user densities with low-power mobile stations, and operating at 1.8 GHz. The specifications for this system, called Digital Cellular System (DCS1800) were published 1991. Commercial operation of GSM networks started in mid-1991 in European countries. By the beginning of 1995, there were 60 countries with operational or planned GSM networks in Europe, the Middle East, the Far East, Australia, Africa, and South America, with a total of over 5.4 million subscribers. As it turned out, none of the six candidates was actually used! The information collected during the tests did enable the GSM (Group Special Mobile) to design the specifications of the current GSM network. The total change to a digital network was one of the fundamental factors of the success of GSM. Digital transmission is easier to decode than analogue due to the limited number of possible input values (0,1), and as ISDN was becoming de facto at the time, it was logical to avail of digital technology. This also ensured that GSM could evolve properly in an increasingly digital world, for example with the introduction of an 8kps speech coder. It is much easier to change channel characteristics digitally than analogously. Finally, the transmission method decided on for the network was TDMA, as opposed to FDMA and CDMA. In 1989, responsibility for the specification was passed from CEPT to the newly formed and now famous European Telecommunications Standards Institute (ETSI). By 1990, the specifications and explanatory notes on the system were documented extensively, producing 138 documents in total, some reaching sizes of several hundred pages in length services.

1. 2. Overview

GSM (Global System for Mobile Communications) is a European digital communications standard which provides full duplex data traffic to any device fitted with GSM capability, such as a phone, fax, or pager, at a rate of 9600 bps using the TDMA communications scheme. Since GSM is purely digital, it can easily interface with other digital communications systems, such as ISDN, and digital devices, such as Group 3 facsimile machines.

Unlike any other service, GSM products such as cellular phones require the use of a Subscriber Identity Module, or SIM card. These small electronic devices record all of the user information it. This includes data such as programmed telephone numbers and network security features, which identify the user. Without this module, the device will not function. This allows for greater security and also greater ease of use as this card may be transported from one phone to another, while maintaining the same information available to the user. GSM is also present outside of Europe but known by different names.

In North America it is known as PCS 1900 and elsewhere are DCS 1800 (also known as PCS). The only difference between these systems is the frequency at which operate. The number stands for the operating frequency in megahertz. While each system uses the GSM standard, they are not compatible with each other.

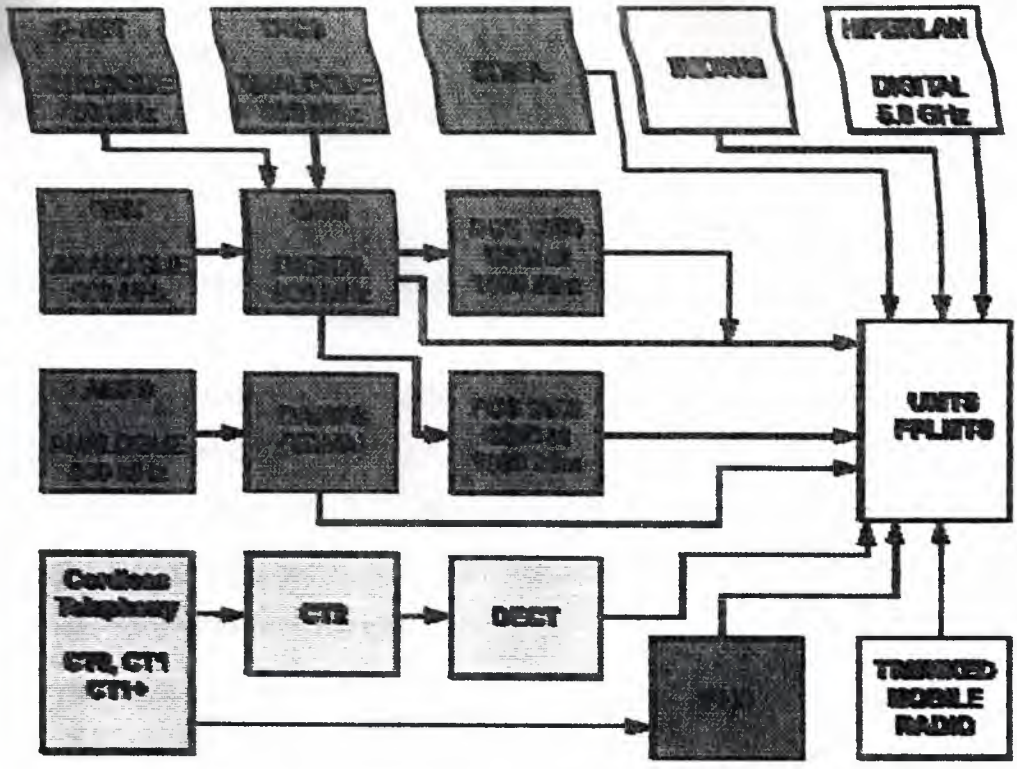


Figure 1.1 The Mobile Evolution

Before GSM networks there were public mobile radio networks (cellular). They normally used analog technologies, which varied from country to country and from manufacturer to another. These analog networks did not comply with any uniform standard. There was no way to use a single mobile phone from one country to another. The speech quality in most networks was not satisfactory.

GSM became popular very quickly because it provided improved speech quality and, through a uniform international standard, made it possible to use a single telephone number and mobile unit around the world. The European Telecommunications Standardization Institute (ETSI) adopted the GSM standard in 1991, and GSM is now used in 135 countries

The benefits of GSM include:

- Support for international roaming
- Distinction between user and device identification
- Excellent speech quality

- Wide range of services
- Interworking (e.g. with ISDN, DECT)
- Extensive security features

GSM also stands out from other technologies with its wide range of services 1:

- Telephony
- Asynchronous and synchronous data services (2.4/4.8/9.6 kbit/s)
- Access to packet data network (X.25)
- Telematic services (SMS, fax, videotext, etc.)
- Many value-added features (call forwarding, caller ID, voice mailbox)
- E-mail and Internet connections

1. 3. Technology

1.3.1 Services Provided by GSM

From the beginning, the planners of GSM wanted ISDN compatibility in terms of the services offered and the control signaling used. However, radio transmission limitations, in terms of bandwidth and cost, do not allow the standard ISDN B-channel bit rate of 64 kbps to be practically achieved.

Using the ITU-T definitions, telecommunication services can be divided into bearer services, tele-services, and supplementary services. The digital nature of GSM allows data, both synchronous and asynchronous, to be transported as a bearer service to or from an ISDN terminal. Data can use either the transparent service, which has a fixed delay but no guarantee of data integrity, or a nontransparent service, which guarantees data integrity through an Automatic Repeat Request (ARQ) mechanism, but with a variable delay. The data rates supported by GSM are 300 bps, 600 bps, 1200 bps, 2400 bps, and 9600 bps.

The most basic tele-service supported by GSM is telephony. As with all other communications, speech is digitally encoded and transmitted through the GSM network

as a digital stream. There is also an emergency service, where the nearest emergency-service provider is notified by dialing three digits (similar to 911).

A variety of data services is offered. GSM users can send and receive data, at rates up to 9600 bps, to users on POTS (Plain Old Telephone Service), ISDN, Packet Switched Public Data Networks, and Circuit Switched Public Data Networks using a variety of access methods and protocols, such as X.25 or X.32. Since GSM is a digital network, a modem is not required between the user and GSM network, although an audio modem is required inside the GSM. Network to inter-work with POTS.

Other data services include Group 3 facsimile, as described in ITU-T recommendation T.30, which is supported by use of an appropriate fax adaptor. A unique feature of GSM, not found in older analog systems, is the Short Message Service (SMS). SMS is a bi directional service for short alphanumeric (up to 160 bytes) messages. Messages are transported in a store-and-forward fashion. For point-to-point SMS, a message can be sent to another subscriber to the service, and an acknowledgement of receipt is provided to the sender. SMS can also be used in a cell-broadcast mode, for sending messages such as traffic updates or news updates. Messages can also be stored in the SIM card for later retrieval.

Supplementary services are provided on top of tele-services or bearer services. In the current (Phase I) specifications, they include several forms of call forward (such as call forwarding when the mobile subscriber is unreachable by the network), and call barring of outgoing or incoming calls, for example when roaming in another country. Many additional supplementary services will be provided in the Phase 2 specifications, such as caller identification, call waiting, multi-party conversations.

GSM Phase 1 features

- Call Forwarding
- All Calls
- No Answer
- Engaged
- Unreachable
- Call Barring

- Outgoing - Bar certain outgoing calls (e.g. ISD)
- Incoming - Bar certain incoming calls (Useful if in another country)
- Global roaming - Visit any other country with GSM and a roaming agreement and use your phone and existing number

GSM Phase 2 features

- SMS - Short Message Service - Allows you to send text messages too and from phones
- Multi Party Calling - Talk to five other parties as well as yourself at the same time
- Call Holding - Place a call on Hold
- Call Waiting - Notifies you of another call whilst on a call
- Mobile Data Services - Allows handsets to communicate with computers
- Mobile Fax Service - Allows handsets to send, retrieve and receive faxes
- Calling Line Identity Service - This facility allows you to see the telephone number of the incoming caller on our handset before answering
- Advice of Charge - Allows you to keep track of call costs
- Cell Broadcast - Allows you to subscribe to local news channels
- Mobile Terminating Fax - Another number you are issued with that receives faxes that you can then download to the nearest fax machine.

GSM Phase 2+ features

- (Available by 1998)
- Upgrade and improvements to existing services
- Majority of the upgrade concerns data transmission, including bearer services and packet switched data at 64 kbps and above
- DECT access to GSM
- PMR/Public Access Mobile Radio (PAMR)-like capabilities
- GSM in the local loop
- Virtual Private Networks
- Packet Radio
- SIM enhancements
- Premium rate services (e.g. Stock prices sent to your phone)

1.3.2 Third Generation (3G)

The mobile communications industry has evolved in three stages:

Figure 1.2 Mobile Communications Industry Evolution

Three generations of mobile phones have emerged so far, each successive generation more reliable and flexible than the last:

Analog: You could only easily use analogue cellular to make voice calls, and typically only in any one country.

Digital mobile phone systems added fax, data and messaging capabilities as well as voice telephone service in many countries.

Multimedia services add high speed data transfer to mobile devices, allowing new video, audio and other applications through mobile phones- allowing music and television and the Internet to be accessed through a mobile terminal.

With each new generation of technology, the services which can de deployed on them becomes more and more wide ranging and truly limited only by imagination. We are reaching that stage with 3G.

During the first and second generations different regions of the world pursued different mobile phone standards, but are converging to a common standard for mobile multimedia called Third Generation (3G) that is based on CDMA technology. Europe pursued NMT and TACS for analog and GSM for digital, North America pursued AMPS for analog and a mix of TDMA, CDMA and GSM for digital. 3G will bring these incompatible standards together, and the aim of this paper is to discuss the optimal

migration path for mobile network operators to get from their existing 2G digital systems to the 3G world.

The Third Generation of mobile communications systems will soon by implemented. Following on the heals of analog and digital technology, the Third Generation will be digital mobile multimedia offering broadband mobile communications with voice, video, graphics, audio and other information. This transition is shown in Table 1.1 below:

Table 1.1 Source Mobile Lifestreams

Generation	Type	Time	Description
First	Analog	1980s	Voice centric, multiple standards (NMT, TACS etc.)
Second	Digital	1990s	Voice centric, multiple standards (GSM, CDMA, TDMA)
2.5	Higher Rate Data	Late 1990s	Introduction of new higher speed data services to bridge the gap between the second and Third Generation, including services such as General Packet Radio Service (GPRS) and Enhanced Data Rates for Global Evolution (EDGE)
Third	Digital Multimedia	2001+	Voice and data centric, single standard with multiple modes

a) 3G Features

Packet Everywhere:

With Third Generation (3G), the information is split into separate but related "packets" before being transmitted and reassembled at the receiving end. Packet switching is similar to a jigsaw puzzle- the image that the puzzle represents is divided into pieces at the manufacturing factory and put into a plastic bag. During transportation of the now boxed jigsaw from the factory to the end user, the pieces get jumbled up. When the recipient empties the bag with all the pieces, they are reassembled to form the original image. All the pieces are all related and fit together, but the way they are transported and assembled varies.

Packet switched data formats are much more common than their circuit switched counterparts. Other examples of packet-based data standards include TCP/IP, X.25, Frame Relay and Asynchronous Transfer Mode (ATM). As such, whilst packet switching is new to the GSM world, it is well established elsewhere. In the mobile world, CDPD (Cellular Digital Packet Data), PDCP (Personal Digital Cellular Packet), General Packet Radio Service (GPRS) and wireless X.25 technologies have been in operation for several years. X.25 is the international public access packet radio data network standard.

Internet Everywhere:

The World Wide Web is becoming the primary communications interface- people access the Internet for entertainment and information collection, the intranet for accessing company information and connecting with colleagues and the extranet for accessing customers and suppliers. These are all derivatives of the World Wide Web aimed at connecting different communities of interest. There is a trend away from storing information locally in specific software packages on PCs to remotely on the Internet. When you want to check your schedule or contacts, instead of using a software package such as "Act!", you go onto the Internet site such as a portal. Hence, web browsing is a very important application for packet data.

High Speed:

Speeds of up to 2 Megabits per second (Mbps) are achievable with Third Generation (3G). The data transmission rates will depend upon the environment the call is being made in- it is only indoors and in stationary environments that these types of data rates will be available. For high mobility, data rates of 144 kbps are expected to be available- this is only about three times the speed of today's fixed telecoms modems.

New Applications, Better Applications:

Third Generation (3G) facilitates several new applications that have not previously been readily available over mobile networks due to the limitations in data transmission speeds. These applications range from Web Browsing to file transfer to Home Automation- the ability to remotely access and control in-house appliances and machines. Because of the bandwidth increase, these applications will be even more easily available with 3G than they were previously with interim technologies such as GPRS.

Service Access:

To use Third Generation (3G), users specifically need:

- A mobile phone or terminal that supports Third Generation (3G)
- A subscription to a mobile telephone network that supports Third Generation (3G)
- Use of Third Generation (3G) must be enabled for that user. Automatic access to the 3G may be allowed by some mobile network operators, others will charge a monthly subscription and require a specific opt-in to use the service as they do with other nonvoice mobile services
- Knowledge of how to send and/ or receive Third Generation (3G) information using their specific model of mobile phone, including software and hardware configuration (this creates a customer service requirement)
- A destination to send or receive information through Third Generation (3G). From day one, Third Generation (3G) users can access any web page or other Internet applications- providing an immediate critical mass of users.

These user requirements are not expected to change much for the meaningful use of 3G.

b) 3G Talking Points

The telecommunications world is changing as the trends of media convergence, industry consolidation, Internet and IP technologies and mobile communications collide into one. Significant change will be bought about by this rapid evolution in technology, with Third Generation mobile Internet technology a radical departure from that that came before in the first and even the second generations of mobile technology. Some of the changes include:

People will look at their mobile phone as much as they hold it to their ear. As such, 3G will be less safe than previous generations- because television and other multimedia services tend to attract attention to themselves- instead of hands-free kits, we will need eyes-free kits!

Data ("non-voice") uses of 3G will be as important as and very different from the traditional voice business.

Mobile communications will be similar in its capability to fixed communications, such that many people will only have a mobile phone. The mobile phone will be used as an integral part of the majority of people's lives- it will not be an added accessory but a core part of how they conduct their daily lives. The mobile phone will become akin to a remote control or magic wand that lets people do what they want when they want.

As with all new technology standards, there is uncertainty and the fear of displacement. Third Generation (3G) mobile is topical and contentious for several reasons:

Because the nature and form of mobile communications is so radically changed, many people don't understand how to make money in the nonvoice world, and do not understand their role in it.

3G licenses have started being awarded around the world, necessitating that existing mobile communications companies in the 2G world think about and justify their continued existence.

3G is based on a different technology platform- Code Division Multiple Access (CDMA)- that is unlike the Time Division Multiple Access (TDMA) technology that is widely used in the 2G world. GSM (Global System for Mobile Communications) was based on TDMA technology.

The US, Japanese and European mobile players all have different technology competences and are now unified in this single standard- the separate wireless evolution paths and European wireless leadership are thereby challenged.

Japanese network operators will be the first to implement 3G networks in the year 2001, and Japanese terminal manufacturers, who have not had much market share outside their home market, will be first with 3G terminals.

Many industry analysts and other pundits have questioned the return on an investment in 3G technology- questioning whether network operators will be able to earn an adequate return on the capital deployed in acquiring and rolling out a 3G network.

Many media and Internet companies have expressed an interest in bidding for and using 3G technology as a new channel to distribute their content, opening the opportunity for new entrants and new partnerships and value chains.

1. 4. The Different GSM-Based Networks

Different frequency bands are used for GSM 900, GSM1800 and GSM 1900 (Table 1.2). In some countries, an operator applies for the available frequencies. In other countries, e.g. United States, an operator purchases available frequency bands at auctions.

Table 1.2 Frequency bands for the different GSM-based networks

Network type	Frequency band UL / DL	Implementations
GSM 900	890-915 / 935-960 MHz	GSM 900
GSM1800	1710–1785 / 1805 -1880 MHz	GSM 1800
GSM1900	1850-1910 / 1930-1990 MHz	GSM1900

1.4.1 Where are the GSM Frequencies Used?

GSM networks presently operate in three different frequency ranges. These are:

a) GSM 900

(Also called GSM) operates in the 900 MHz frequency range and is the most common in Europe and the world.

b) GSM 1800

(Also called PCN (Personal Communication Network), and DCS 1800) - operates in the 1800 MHz frequency range and is found in a rapidly-increasing number of countries including France, Germany, Switzerland, the UK, and Russia. A European Commission mandate requires European Union members to license at least one DCS 1800 operator before 1998.

c) GSM 1900

(Also called PCS (Personal Communication Services), PCS 1900, and DCS 1900) The only frequency used in the United States and Canada for GSM. Note that the terms PCS is commonly used to refer to any digital cellular network operating in the1900 MHz frequency range, not just GSM.

1. 5. GSM System Architecture

The increasing demand for data services leads to the Internet growing and the World Wide Web has grown from 130 mostly educational sites in mid-1993 to 650,000 largely

commercial sites at the beginning of 1997. There are now estimated to be well in excess of 50 million individual subscribers with Internet access. This development can be divided into two periods. First generation wireless networks evolve from specialized proprietary protocols or national standards. Wireless voice and data networks operate independently or, at best, are loosely coupled. Over the last decade a second generation fully digital mobile communication network, now called the Global System for Mobil communications (GSM), with integrated voice and data capabilities has been created and deployed. GSM has three spectral variants: GSM 900, DCS1800 and PCS 1900 operating respectively in the 900MHz, 1.8 GHz and 1.9 GHz bands. GSM has matured to be adopted by around 200 operators in 100 countries. The success of GSM has produced a market led evolution. The GSM system was originally deployed in phase 1 as a basic voice and circuit data service and then additional supplementary services were added in the pre-planned phase 2. GSM is now in "phase 2+", which allows for the ongoing introduction of new services and which should eventually migrate to a third generation system known as the Universal Mobile Telecommunications System (UMTS). A rich collection of new data services is currently being defined under phase 2+. These services when combined with existing data services will provide greater choices and improved bandwidth.

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

- The BSS provides and manages radio transmission paths between the mobile stations and the Mobile Switching Center (MSC). It also manages the radio interface. Each BSS consists of many Base Station Controllers (BSCs) which connect the MS to the NSS via the MSCs.
- The NSS manages the switching functions of the system and allows the MSCs to communicate with other networks such as the PSTN and ISDN.
- The OSS supports the operation and maintenance of GSM and allows system engineers to monitor, diagnose, and troubleshoot all aspects of the GSM system.

This subsystem interacts with the other GSM subsystems, and is provided solely for the staff of the GSM operating company, which provides service facilities for the network.

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

The following figure shows the block diagram of the GSM system architecture. The Mobile Stations (MS) communicate with the Base Station Subsystem (BSS) over the radio air interface. The BSS consists of many BSCs, which connect to a single MSC, and each BSC typically controls up to several hundred Base Transceiver Stations (BTSs).

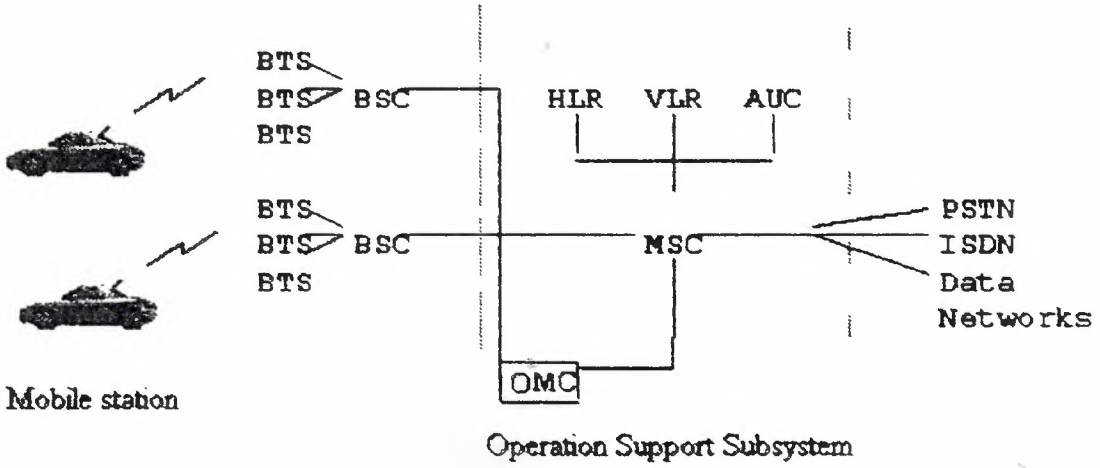


Figure 1.3 GSM System Architecture

The NSS handles the switching of GSM calls between external networks and the BSCs in the radio subsystem and is also responsible for managing and providing external access to several customer databases. The MSC is the central unit in the NSS and controls the traffic among all of the BSCs. In the NSS, there are three different

databases called the Home Location Register (HLR), Visitor Location Register (VLR), and the Authentication Center (AUC). The HLR is a database, which contains subscriber information and location information for each user who resides in the same city as the MSC. Each subscriber in a particular GSM market is assigned a unique International Mobil Subscriber Identity (IMSI), and this number is used to identify each home user. The VLR is a database, which temporarily stores the IMSI and customer information for each roaming subscriber who is visiting the coverage area of a particular MSC. The Authentication Center is a strongly protected database which handles the authentication and encryption keys for every single subscriber in the HLR and VLR. The OSS supports one or several Operation Maintenance Centers (OMC) which are used to monitor and maintain the performance of each MS, BS, BSC, and MSC within a GSM system.

2. ARCHITECTURE OF GSM NETWORK

2. 1. Overview

The GSM technical specifications define the different entities that form the GSM network by defining their functions and interface requirements. The GSM network can be divided into four main parts:

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

The architecture of the GSM network is presented in figure 2.1

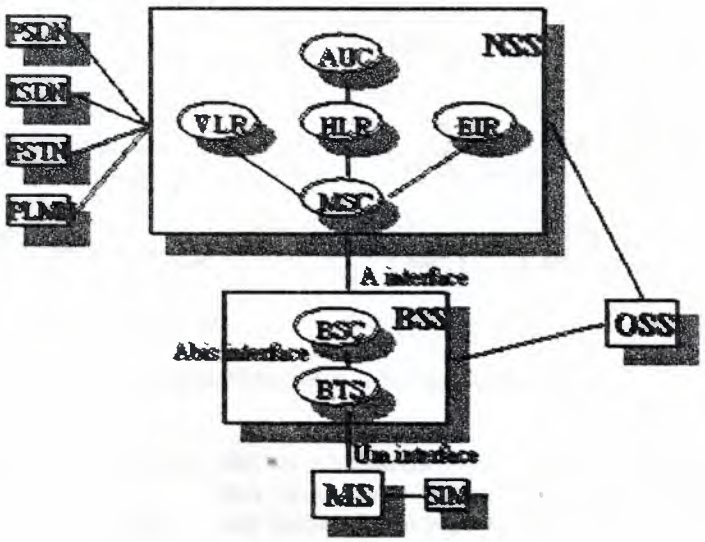


Figure 2.1 Architecture of the GSM network

A GSM network is composed of several functional entities, whose functions and interfaces are specified. Figure 2.1 shows the layout of a generic GSM network. The GSM network can be divided into three broad parts. The subscriber carries the Mobile Station. The Base Station Subsystem controls the radio link with the Mobile Station. The Network Subsystem, the main part of which is the Mobile Services Switching

Center (MSC), performs the switching of calls between the mobile users, and between mobile and fixed network users. The MSC also handles the mobility management operations. Not shown is the Operations and Maintenance Center, which oversees the proper operation and setup of the network. The Mobile Station and the Base Station Subsystem communicate across the U_m interface, also known as the air interface or radio link. The Base Station Subsystem communicates with the Mobile Services Switching Center across the A interface. GSM provides recommendations, not requirements. The GSM specifications define the functions and interface requirements.
In detail but do not address the hardware. The reason for this is to limit the designers as little as possible but still to make it possible for the operators to buy equipment from different suppliers. The GSM network is divided into three major systems: the switching system (SS), the base station system (BSS), and the operation and support system (OSS). The basic GSM network elements are shown in Figure 2.2 and Figure 2.3.

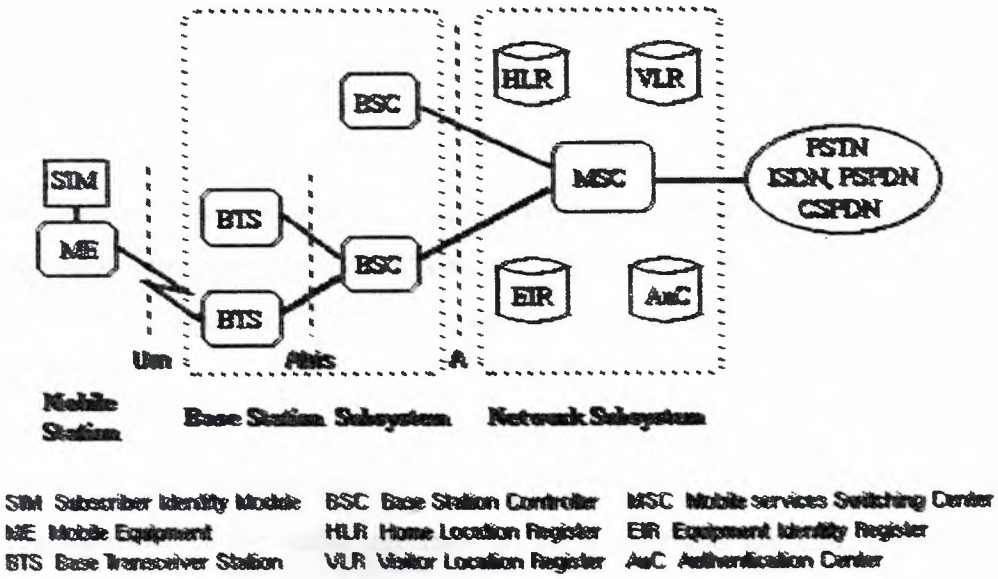


Figure 2.2 General architecture of a GSM network

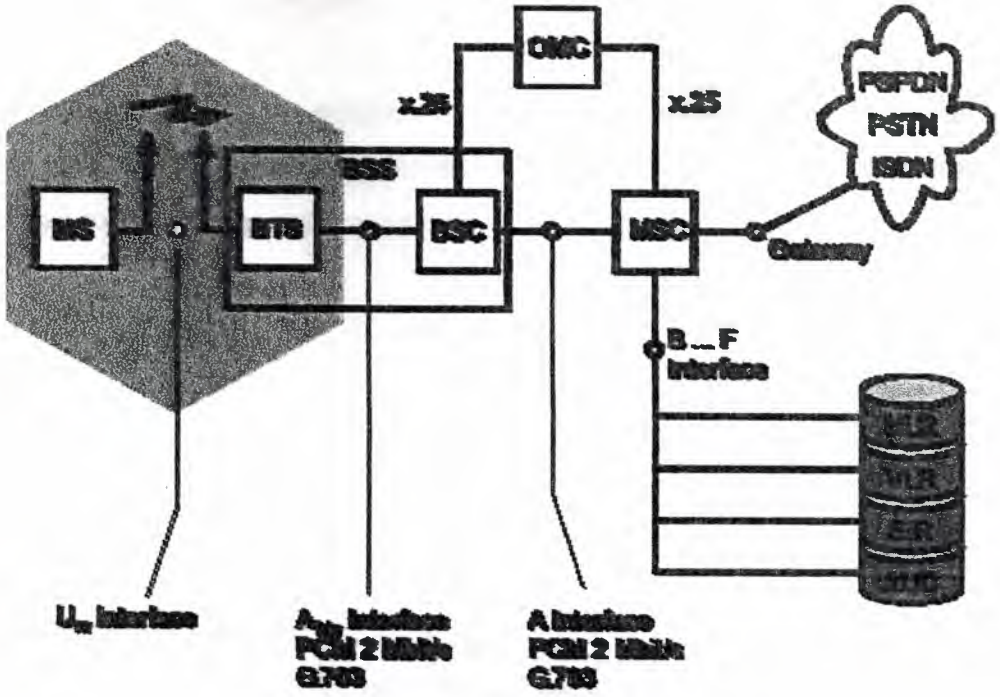


Figure 2.3 GSM network

2. 2. GSM Subsystems

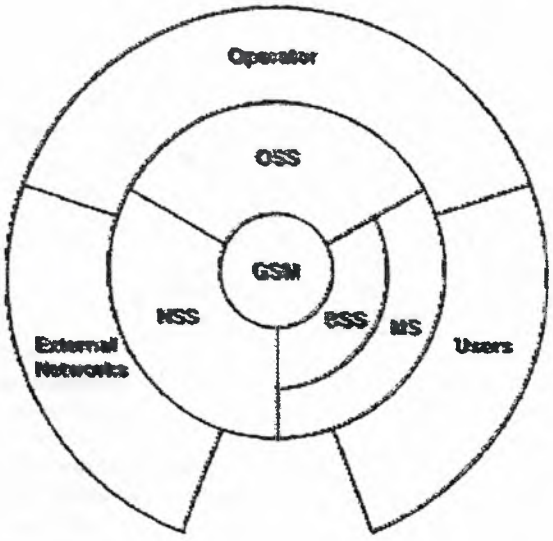
A series of functions are required to support the services and facilities in the GSM PLMN. The basic subsystems of the GSM architecture are (Figure 2.4) the Base Station Subsystem (BSS), Network and Switching Subsystem (NSS), and Operational Subsystem (OSS).

The BSS provides and manages transmission paths between the MSs and the NSS. This includes management of the radio interface between MSs and the rest of the GSM system. The NSS has the responsibility of managing communications and connecting MSs to the relevant networks or other MSs. The NSS is not in direct contact with the MSs. Neither is the BSS in direct contact with external networks. The MS, BSS, and NSS form the operational part of the GSM system. The OSS provides means for a service provider to control and manage the GSM system. In the GSM, interaction between the subsystems can be grouped in two main parts:

Operational: External networks to/from NSS to/from BSS to/from MS to/from subscriber

Control: OSS to/from service provider

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



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

Figure 2.4 GSM Subsystems

2.2.1 Mobile Station

The MS consists of the physical equipment used by the subscriber to access a PLMN for offered telecommunication services. Functionally, the MS includes a Mobile Termination (MT) and, depending on the services it can support, various Terminal Equipment (TE), and combinations of TE and Terminal Adaptor (TA) functions (the TA acts as a gateway between the TE and the MT) (see Figure 2.6). Various types of MS, such as the vehicle-mounted station, portable station, or handheld station, are used.

The MSs come in five power classes which define the maximum RF power level that the unit can transmit. Tables 2.1 and 2.2 provide the details of maximum RF power for

various classes in GSM and DCS-1800. Vehicular and portable units can be either class I or class II, whereas handheld units can be class III, IV, and V. The typical classes are II and V. Table 2.3 provides the details of maximum RF power for GSM and DCS-1800 micro-BSs.

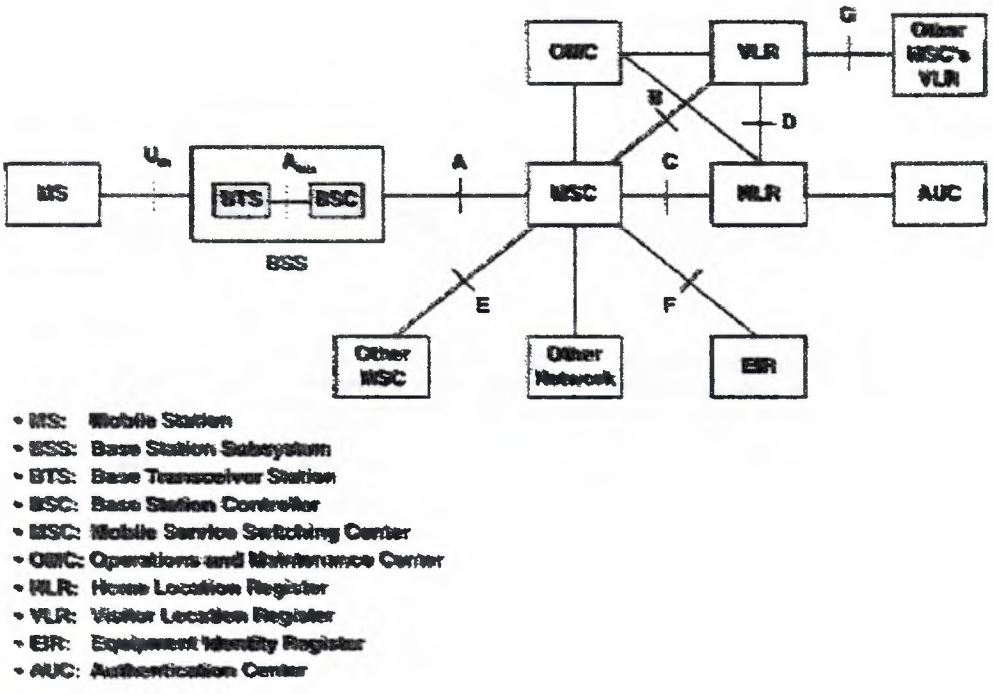


Figure 2.5 GSM Reference Model

Table 2.1 Maximum RF Power for MS in GSM

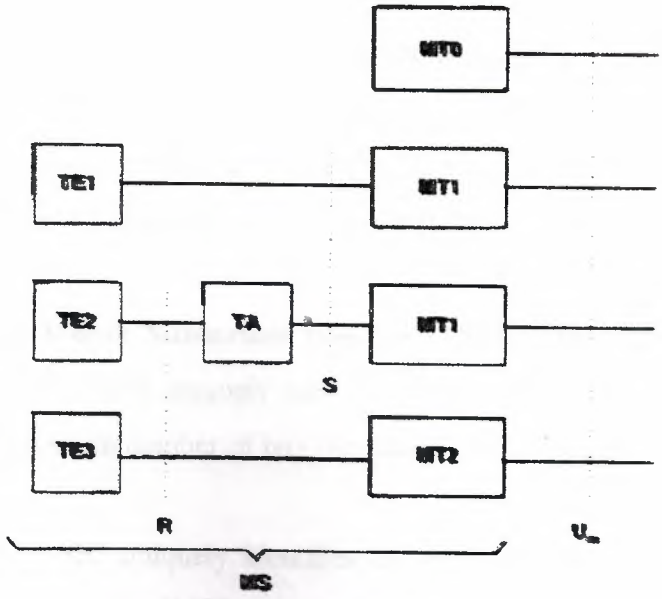
Class	MS Max. RF Power (watts)
I	20 (not currently implemented)
II	8
III	5
IV	2
V	0.8

Table 2.2 Power Level in DCS-1800

Power Class	Max. MS RF Power watts (dBm)	Max. BS RF Power watts (dBm)
1	1 (30)	20 (43)
2	0.25 (24)	10 (40)
3		5 (37)
4		2.5 (34)

Table 2.3 Power Levels for Micro-BS in GSM and DCS-1800

Power Class	Max. RF Power of GSM Micro-BS, watts (dBm)	Max. RF Power of DCS-1800 Micro-BS, watts (dBm)
M1	0.25 (24)	1.6 (32)
M2	0.08 (19)	0.5 (27)
M3	0.03 (14)	0.16 (22)



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

Figure 2.6 Types of MSs

Basically, an MS can be divided into two parts. The first part contains the hardware and software to support radio and human interface functions. The second part contains terminal/user-specific data in the form of a smart card, which can effectively be considered a sort of logical terminal. The SIM card plugs into the first part of the MS and remains in for the duration of use. Without the SIM card, the MS is not associated with any user and cannot make or receive calls (except possibly an emergency call if the network allows). The SIM card is issued by the mobile service provider after subscription, while the first part of the MS would be available at retail shops to buy or rent. This type of SIM card mobility is analogous to terminal mobility, but provides a personal-mobility-like service within the GSM mobile network.

An MS has a number of identities including the International Mobile Equipment Identity (IMEI), the International Mobile Subscriber Identity (IMSI), and the ISDN number. The IMSI is stored in the SIM. The SIM card contains all the subscriber-related information stored on the user's side of the radio interface.

IMSI: The IMSI is assigned to an MS at subscription time. It uniquely identifies a given MS. The IMSI will be transmitted over the radio interface only if necessary. The IMSI contains 15 digits and includes

- Mobile Country Code (MCC)—3 digits (home country)
- Mobile Network Code (MNC)—2 digits (home GSM PLMN)
- Mobile Subscriber Identification (MSIN)
- National Mobile Subscriber Identity (NMSI)

Temporary Mobile Subscriber Identity (TMSI): The TMSI is assigned to an MS by the VLR. The TMSI uniquely identifies an MS within the area controlled by a given VLR. The maximum number of bits that can be used for the TMSI is 32.

IMEI: The IMEI uniquely identifies the MS equipment. It is assigned by the equipment manufacturer. The IMEI contains 15 digits and carries

- The Type Approval Code (TAC)—6 digits
- The Final Assembly Code (FAC)—2 digits
- The serial number (SN)— 6 digits

- A Spare (SP)—1 digit

SIM: The SIM carries the following information:

- IMSI
- Authentication Key (K i)
- Subscriber information
- Access control class
- Cipher Key (K c) * (updated by the network)
- TMSI *
- Additional GSM services *
- Location Area Identity (LAI) *
- Forbidden PLMN

In some of the newer applications (data communications in particular), an MS can also be a terminal that acts as a GSM interface, e.g. for a laptop computer. In this new application the MS does not look like a normal GSM telephone. The seemingly low price of a mobile phone can give the (false) impression that the product is not of high quality. Besides providing a transceiver (TRX) for transmission and reception of voice and data, the mobile also performs a number of very demanding tasks such as authentication, handover, encoding and channel encoding.

The Authentification Center (AuC) is the network sub-system register which contains all the password numbers in the customer's SIM card, which is used for authentification and securuty over the network.

One of the main reasons why cell-phones can be so small and still have enough power to remain on standby for so long is that they use a receiving method known as Discontinuous Receive (DRX). This allows the mobile to only listen to paging signals when they are emitted by a known paging cycle of the network. The phones are not continuously checking for signals and use one tenth of the power requirements they would need therefore.

The mobile station is the formal name for what represents, for most people, their actual cell-phone and a smart card called the Subscriber Identity Module (SIM). Other examples of mobile stations are car-phones and transportable units. The SIM card can be regarded as separate from the actual terminal as a user can insert the card into another terminal, receive calls from there, and reap the full access of other subscribed services. The SIM card provides for greater security and renders theft futile as it may contain a user password or personal identity number. The terminal itself is uniquely identified by the International Mobile Equipment Identity (IMEI), which is similar in idea as the unique number a printer, say, has as a part of a computer network.
A Mobile Station consists of two main elements:

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

a) The Terminal

There are different types of terminals distinguished principally by their power and application: The `fixed' terminals are the ones installed in cars. Their maximum allowed output power is 20 W. The GSM portable terminals can also be installed in vehicles. Their maximum allowed output power is 8W.

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

b) The SIM

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

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

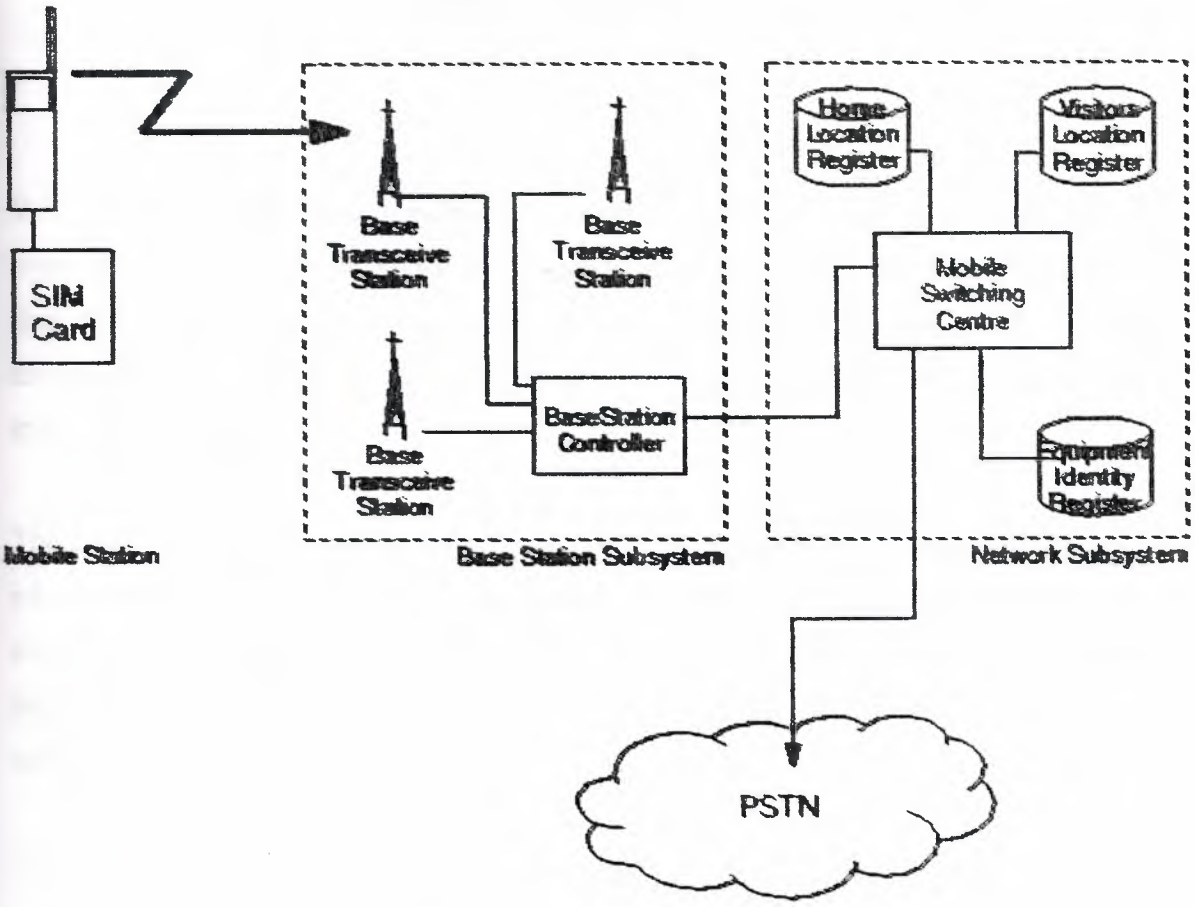


Figure 2.7 Overview of a GSM Mobile Network

2.2.2 Base Station Subsystem

All radio-related functions are performed in the BSS, which consists of base station controllers (BSCs) and the base transceiver stations (BTSs).

a) The Base Transceiver Station

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

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

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

GSM uses a series of radio transmitters called BTSs to connect the mobiles to a cellular network. Their tasks include channel coding/decoding and encryption/decryption. ABTS is comprised of radio transmitters and receivers, antennas, the interface to the PCM facility, etc. The BTS may contain one or more transceivers to provide the required call handling capacity. A cell site may be omnidirectional or split into typically three directional cells.

The BTS contains the Transcoder Rate Adapter Unit (TRAU). In TRAU, the GSM-specific speech encoding and decoding is carried out, as well as the rate adaptation function for data. In certain situations the TRAU is located at the MSC to gain an advantage of more compressed transmission between the BTS and the MSC.

b) The Base Station Controller

The primary function of the BSC is call maintenance. The mobile stations normally send a report of their received signal strength to the BSC every 480 ms. With this information the BSC decides to initiate handovers to other cells, change the BTS transmitter power, etc.

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

The BSC provides all the control functions and physical links between the MSC and BTS. It is a high-capacity switch that provides functions such as handover, cell configuration data, and control of radio frequency (RF) power levels in base transceiver stations. A number of BSCs are served by an MSC. Once the mobile has been successfully connected to a BTS, the BSC will set up a bi-directional signaling channel specifically for itself and it will connect it on to the MSC.

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

c) RBS200

The RBS 200 Base Station family was the first base station developed in the early 1990's. It exists only in the GSM 900/1800 product line. The RBS 200/204 is the GSM 900 BTS, and the RBS 205 is the BTS supporting GSM 1800.

d) RBS 2000

The RBS 2000 Base Station family is the second generation of base stations and can be used for GSM 900/1800 and GSM 1900.
There are six different models in the series:

- RBS 2101 with 2 Transceiver Units (TRUs)
- RBS 2102 and 2202 with 6 TRUs
- RBS 2103 (GSM 900 only) with 6 TRUs and smaller footprint
- RBS 2301 is the micro-base station
- RBS 2302 is the micro-base station supporting Maxite™
- RBS 2401 is the first dedicated indoor radio base station
- All models are outdoor versions except RBS 2202 and RBS 2401.

2.2.3 Network and Switching Subsystem

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

The MSC performs the necessary switching functions required for the MSs located in an associated geographical area, called an MSC area (see Figure 2.9).

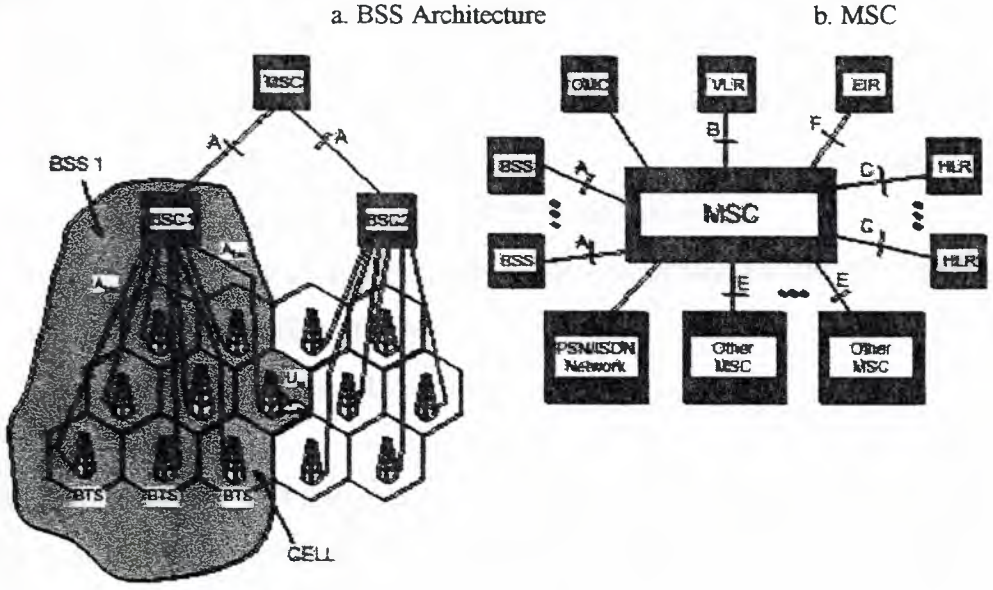


Figure 2.9 MSC Area in GSM

The MSC monitors the mobility of its subscribers and manages necessary resources required to handle and update the location registration procedures and to carry out the handover functions. The MSC is involved in the interworking functions to communicate with other networks such as PSTN and ISDN. The interworking functions of the MSC depend upon the type of the network to which it is connected and the type of service to be performed. The call routing and control and echo control functions are also performed by the MSC.

The HLR is the functional unit used for management of mobile subscribers. The number of HLRs in a PLMN varies with the characteristics of the PLMN. Two types of information are stored in the HLR: subscriber information and part of the mobile information to allow incoming calls to be routed to the MSC for the particular MS. Any administrative action by the service provider on subscriber data is performed in the HLR. The HLR stores IMSI, MS ISDN number, VLR address, and subscriber data (e.g., supplementary services).

The VLR is linked to one or more MSCs. The VLR is the functional unit that dynamically stores subscriber information when the subscriber is located in the area covered by the VLR. When a roaming MS enters an MSC area, the MSC informs the associated VLR about the MS; the MS goes through a registration procedure. The registration procedure for the MS includes these activities:

- The VLR recognizes that the MS is from another PLMN.
- If roaming is allowed, the VLR finds the MS's HLR in its home PLMN.
- The VLR constructs a Global Title (GT) from the IMSI to allow signaling from the VLR to the MS's HLR via the PSTN/ISDN networks.
- The VLR generates a Mobile Subscriber Roaming Number (MSRN) that is used to route incoming calls to the MS.
- The MSRN is sent to the MS's HLR.

The information in the VLR includes MSRN, TMSI, the location area in which the MS has been registered, data related to supplementary service, MS ISDN number, IMSI, HLR address or GT, and local MS identity, if used.

The NSS contains more than MSCs, HLRs, and VLRs. In order to deliver an incoming call to a GSM user, the call is first routed to a gateway switch, referred to as the Gateway Mobile Service Switching Center (GMSC). The GMSC is responsible for collecting the location information and routing the call to the MSC through which the subscriber can obtain service at that instant (i.e., the visited MSC). The GMSC first finds the right HLR from the directory number of the GSM subscriber and interrogates it. The GMSC has an interface with external networks for which it provides gateway

function, as well as with the SS7 signaling network for interworking with other NSS entities.

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

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

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

The other two registers are used for authentication and security purposes. The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where its International Mobile Equipment Identity (IMEI) identifies each mobile station. An IMEI is marked as invalid if it has been reported

stolen or is not type approved. The Authentication Center (AUC) is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and encryption over the radio channel.

The OSS supports one or several Operation Maintenance Centers (OMC), which are used to monitor and maintain the performance of each MS, BS, BSC, and MSC within a GSM system. The switching system (SS) is responsible for performing call processing and subscriber-related functions.

The Home Location Register (HLR) and the Visitor Location Register (VLR) handle call routing and roaming. Its main role is to manage the communications between the mobile users and other users, such as mobile users, ISDN users, fixed telephony users, etc. It also includes data bases needed in order to store information about the subscribers and to manage their mobility. The different components of the NSS are described below.

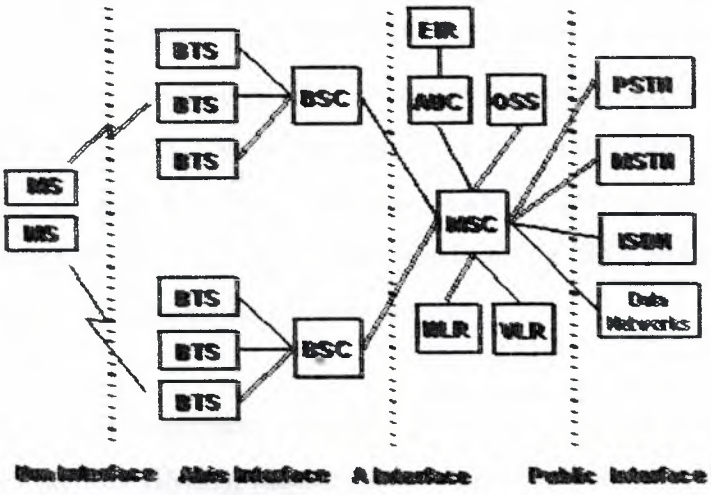


Figure 2.10 Components of the NSS

a) The Switching System

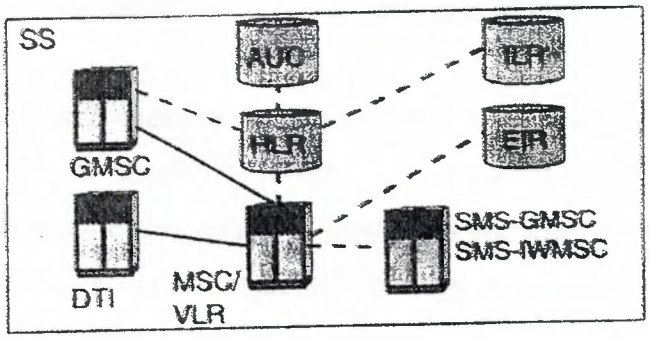


Figure 2.11 Switching System

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

The HLR is a database used for storage and management of subscriptions. The HLR is considered the most important database, as it stores permanent data about subscribers, including a subscriber's service profile, location information, and activity status. When an individual buys a subscription from one of the PCS operators, he or she is registered in the HLR of that operator. The HLR is considered as a very important database that stores information of the subscribers belonging to the covering area of a MSC. It also stores the current location of these subscribers and the services to which they have access. The location of the subscriber corresponds to the SS7 address of the Visitor Location Register (VLR) associated to the terminal.

A database used for management of mobile subscribers. It stores the international mobile subscriber identity (IMSI), mobile station ISDN number (MSISDN) and current visitor location register (VLR) address. The main information stored there concerns the location of each mobile station in order to be able to route calls to the mobile subscribers managed by each HLR. The HLR also maintains the services associated with each MS. One HLR can serve several MSCs.

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

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

The MSC acts like a standard exchange in a fixed network and additionally provides all the functionality needed to handle a mobile subscriber. The main functions are registration, authentication, location updating, handovers and call routing to a roaming subscriber. The signaling between functional entities (registers) in the network subsystem uses Signaling System 7 (SS7). If the MSC also has a gateway function for communicating with other networks, it is called Gateway MSC (GMSC).

- **Visitor Location Register (VLR):**

Contains the current location of the MS and 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. A VLR is connected to one MSC and is normally integrated into the MSC's hardware.

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

- **The Authentication Center (AUC):**

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

The Authentication Center is the network subsystem register, which contains all the password numbers in the customer's SIM card, which is used for authentication and security over the network.

Authentication verifies a mobile customer with a complex challenge and reply routine. The network sends a randomly generated number to the mobile. The mobile then performs a calculation against it with a number it has stored in its SIM and sends the result back. Only if the switch gets the number it expects does the call proceed. The AC stores all data needed to authenticate a call and to then encrypt both voice traffic and signaling messages.

One of the main reasons why cell-phones can be so small and still have enough power to remain on standby for so long is that they use a receiving method known as Discontinuous Receive (DRX). This allows the mobile to only listen to paging signals when they are emitted by a known paging cycle of the network. The phones are not continuously checking for signals and use one tenth of the power requirements they would need therefore.

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

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

The EIR is also used for security purposes. It is a register containing information about the mobile equipments. More particularly, it contains a list of all valid terminals. Its International Mobile Equipment Identity (IMEI) identifies a terminal. The EIR allows then to forbid calls from stolen or unauthorized terminals (e.g., a terminal which does not respect the specifications concerning the output RF power).

The EIR has three databases:

1-White list: for all known, good IMEIs

2-Black list: for bad or stolen handsets

3-Grey list: for handsets/IMEIs that are uncertain

- **Interworking Location Register (ILR):**

Around the world there are market demands for roaming capabilities with GSM. The ILR is the node that forwards roaming information between cellular networks using different operating standards. This currently exists only in the GSM 1900 network.

b) Additional Functional Elements

- **Message Center (MXE):**

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

- **Mobile Service Node (MSN):**

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

- **The Gateway Mobile services Switching Center (GMSC):**

A gateway is a node interconnecting two networks. The GMSC is the interface between the mobile cellular network and the PSTN. It is in charge of routing calls from the fixed network towards a GSM user. The GMSC is often implemented in the same machines as the MSC.

- **Short Message Service - Gateway MSC (SMS-GMSC):**

A Short Message Service Gateway MSC (SMS-GMSC) is capable of receiving a short message from a Service Center (SC), interrogating an HLR for routing information and message waiting data, and delivering the short message to the MSC of the recipient MS. The SMS-GMSC functionality is normally integrated in an MSC/VLR node.

- **Short Message Service - InterWorking MSC (SMS-IWMSC):**

A Short Message Service InterWorking MSC (SMS-IWMSC) is capable of receiving a mobile originated short message from the MSC or an ALERT message from the HLR and submitting the message to the recipient SC. The SMS-IWMSC functionality is normally integrated in the MSC/VLR node.

- **Data Transmission Interface (DTI):**

DTI - consisting of both hardware and software - provides an interface to various networks for data communication. Through DTI, users can alternate between speech and data during the same call. Its main functions include a modem and fax adapter pool and the ability to perform rale adaptation. It was earlier implemented as the OSM InterWorking Unit (GIWU).

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

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

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

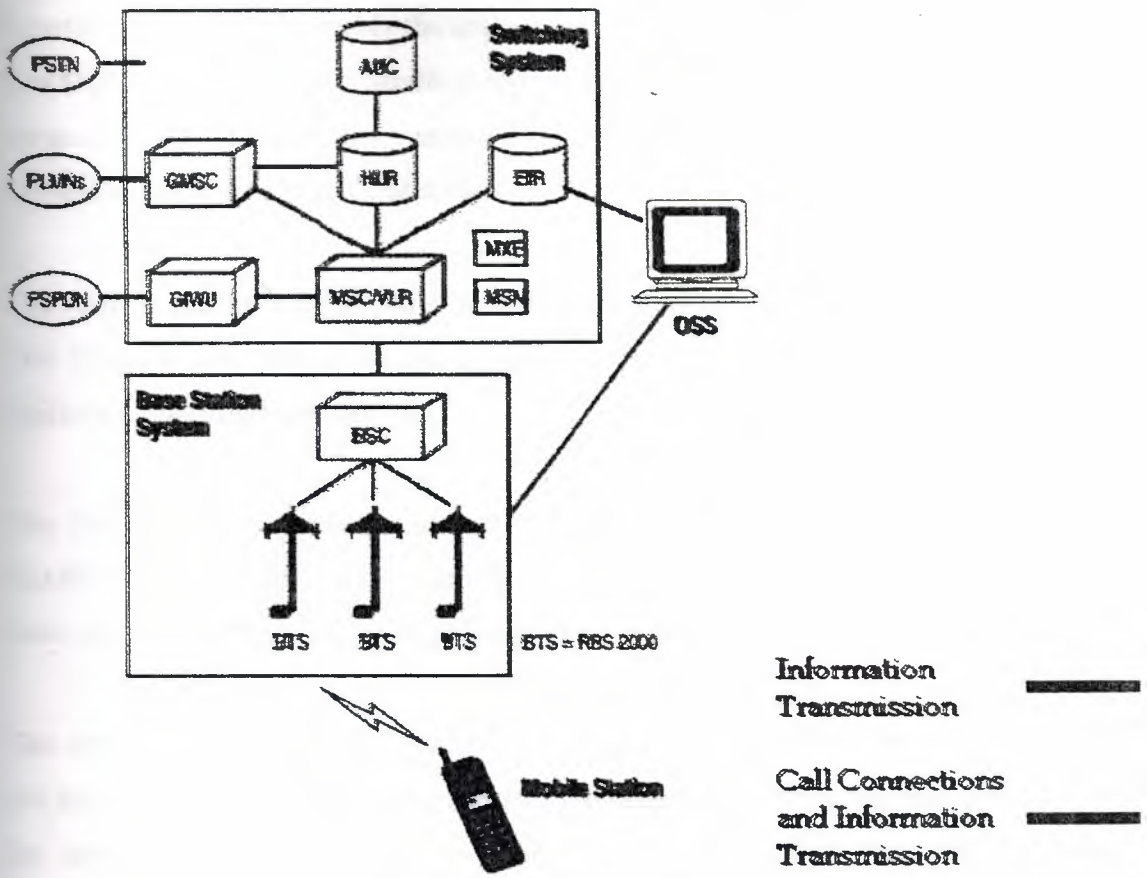


Figure 2.12 GSM Network Elements

2.2.4 Operation and Support Subsystem (OSS)

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

has provoked that some of the maintenance tasks are transferred to the BTS. This transfer decreases considerably the costs of the maintenance of the system.
The OSS is responsible for handling system security based on validation of identities of various telecommunications entities. These functions are performed in the Authentication Center (AUC) and EIR.

The AUC is accessed by the HLR to determine whether an MS will be granted service. The EIR provides MS information used by the MSC. The EIR maintains a list of legitimate, fraudulent, or faulty MSs.

The OMSS is also in charge of remote operation and maintenance functions of the PLMN. These functions are monitored and controlled in the OMSS. The OMSS may have one or more Network Management Centers (NMCs) to centralize PLMN control.

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

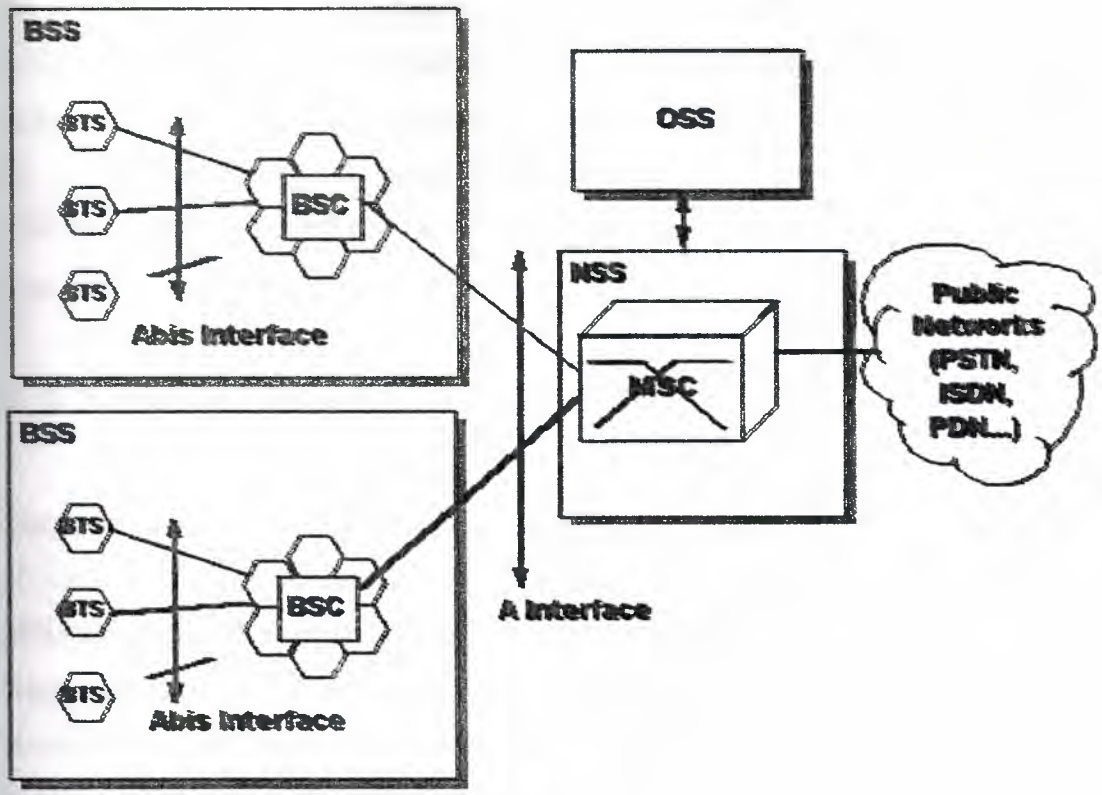


Figure 2.13 Major GSM Components

2. 3. The Geographical Areas of the GSM Network

The Figure 2.14 presents the different areas that form a GSM network.

Figure 2.14 GSM Network Areas

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

2. 4. Radio Link Aspects

The International Telecommunication Union (ITU), which manages the international allocation of radio spectrum (among many other functions), allocated the bands 890-915 MHz for the uplink (mobile station to base station) and 935-960 MHz for the downlink (base station to mobile station) for mobile networks in Europe. Since this range was already being used in the early 1980s by the analog systems of the day, the CEPT had the foresight to reserve the top 10 MHz of each band for the GSM network that was still being developed. Eventually, GSM will be allocated the entire 2x25 MHz bandwidth.

2.4.1 Multiple Access and Channel Structure

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

Channels are defined by the number and position of their corresponding burst periods. All these definitions are cyclic, and the entire pattern repeats approximately every 3

hours. Channels can be divided into "dedicated channels", which are allocated to a mobile station, and "common channels", which are used by mobile stations in idle mode.

a) Traffic Channels

A traffic channel (TCH) is used to carry speech and data traffic. Traffic channels are defined using a 26-frame multiframe, or group of 26 TDMA frames. The length of a 26-frame multiframe is 120 ms, which is how the length of a burst period is defined (120 ms divided by 26 frames divided by 8 burst periods per frame). Out of the 26 frames, 24 are used for traffic, 1 is used for the Slow Associated Control Channel (SACCH) and 1 is currently unused (see Figure 2.15). TCHs for the uplink and downlink are separated in time by 3 burst periods, so that the mobile station does not have to transmit and receive simultaneously, thus simplifying the electronics.

In addition to these full-rate TCHs, there are also half-rate TCHs defined, although they are not yet implemented. Half-rate TCHs will effectively double the capacity of a system once half-rate speech coders are specified (i.e., speech coding at around 7 kbps, instead of 13 kbps). Eighth-rate TCHs are also specified, and are used for signalling. In the recommendations, they are called Stand-alone Dedicated Control Channels (SDCCH).

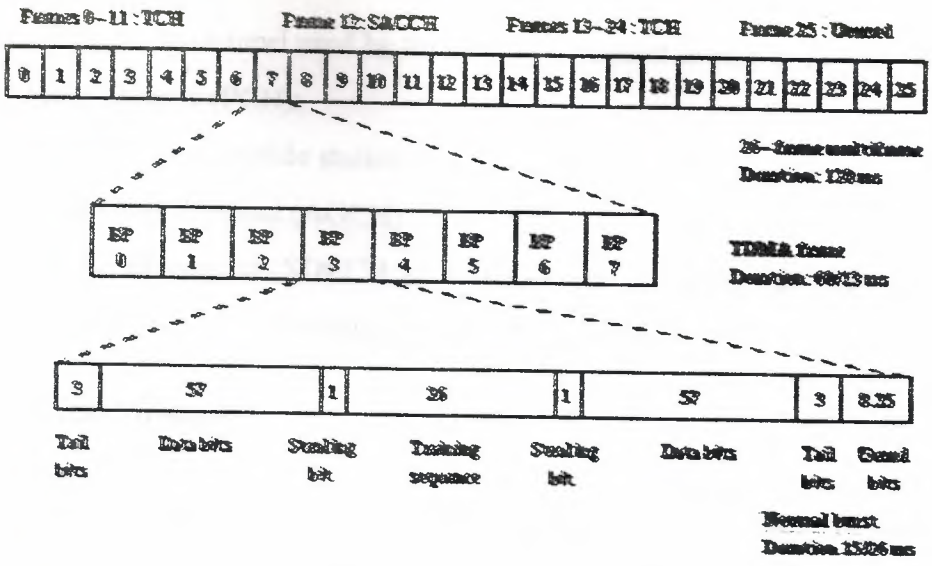


Figure 2.15 Organization of bursts, TDMA frames, and multiframes for speech and data

b) Control Channels

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

- Broadcast Control Channel (BCCH):
  Continually broadcasts, on the downlink, information including base station identity, frequency allocations, and frequency-hopping sequences.
- Frequency Correction Channel (FCCH) and Synchronisation Channel (SCH):
  Used to synchronise the mobile to the time slot structure of a cell by defining the boundaries of burst periods, and the time slot numbering. Every cell in a GSM network broadcasts exactly one FCCH and one SCH, which are by definition on time slot number 0 (within a TDMA frame).
- Random Access Channel (RACH):

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

- Paging Channel (PCH):

  Used to alert the mobile station of an incoming call.

- Access Grant Channel (AGCH):

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

c) Burst Structure

There are four different types of bursts used for transmission in GSM. The normal burst is used to carry data and most signalling. It has a total length of 156.25 bits, made up of two 57 bit information bits, a 26 bit training sequence used for equalization, 1 stealing bit for each information block (used for FACCH), 3 tail bits at each end, and an 8.25 bit guard sequence, as shown in Figure 2. The 156.25 bits are transmitted in 0.577 ms, giving a gross bit rate of 270.833 kbps.

The F burst, used on the FCCH, and the S burst, used on the SCH, have the same length as a normal burst, but a different internal structure, which differentiates them from normal bursts (thus allowing synchronization). The access burst is shorter than the normal burst, and is used only on the RACH.

2.4.2 Speech Coding

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

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

2.4.3 Channel Coding and Modulation

Because of natural and man-made electromagnetic interference, the encoded speech or data signal transmitted over the radio interface must be protected from errors. GSM uses convolutional encoding and block interleaving to achieve this protection. The exact algorithms used differ for speech and for different data rates. The method used for speech blocks will be described below.

Recall that the speech codec produces a 260 bit block for every 20 ms speech sample. From subjective testing, it was found that some bits of this block were more important for perceived speech quality than others. The bits are thus divided into three classes:

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

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

To further protect against the burst errors common to the radio interface, each sample is interleaved. The 456 bits output by the convolutional encoder are divided into 8 blocks of 57 bits, and these blocks are transmitted in eight consecutive time-slot bursts. Since each time-slot burst can carry two 57 bit blocks, each burst carries traffic from two different speech samples.

Recall that each time-slot burst is transmitted at a gross bit rate of 270.833 kbps. This digital signal is modulated onto the analog carrier frequency using Gaussian-filtered Minimum Shift Keying (GMSK). GMSK was selected over other modulation schemes as a compromise between spectral efficiency, complexity of the transmitter, and limited spurious emissions. The complexity of the transmitter is related to power consumption, which should be minimized for the mobile station. The spurious radio emissions, outside of the allotted bandwidth, must be strictly controlled so as to limit adjacent channel interference, and allow for the co-existence of GSM and the older analog systems (at least for the time being).

2.4.4 Multipath Equalization

At the 900 MHz range, radio waves bounce off everything - buildings, hills, cars, airplanes, etc. Thus many reflected signals, each with a different phase, can reach an antenna. Equalization is used to extract the desired signal from the unwanted reflections. It works by finding out how a known transmitted signal is modified by multipath fading, and constructing an inverse filter to extract the rest of the desired signal. This known signal is the 26-bit training sequence transmitted in the middle of every time-slot burst. The actual implementation of the equalizer is not specified in the GSM specifications.

2.4.5 Frequency Hopping

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

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

2.4.6 Discontinuous Transmission

Minimizing co-channel interference is a goal in any cellular system, since it allows better service for a given cell size, or the use of smaller cells, thus increasing the overall capacity of the system. Discontinuous transmission (DTX) is a method that takes advantage of the fact that a person speaks less that 40 percent of the time in normal conversation, by turning the transmitter off during silence periods. An added benefit of DTX is that power is conserved at the mobile unit.

The most important component of DTX is, of course, Voice Activity Detection. It must distinguish between voice and noise inputs, a task that is not as trivial as it appears, considering background noise. If a voice signal is misinterpreted as noise, the transmitter is turned off and a very annoying effect called clipping is heard at the receiving end. If, on the other hand, noise is misinterpreted as a voice signal too often, the efficiency of DTX is dramatically decreased. Another factor to consider is that when the transmitter is turned off, there is total silence heard at the receiving end, due to the digital nature of GSM. To assure the receiver that the connection is not dead, comfort noise is created at the receiving end by trying to match the characteristics of the transmitting end's background noise.

2.4.7 Discontinuous Reception

Another method used to conserve power at the mobile station is discontinuous reception. The paging channel, used by the base station to signal an incoming call, is structured into sub-channels. Each mobile station needs to listen only to its own sub-channel. In the time between successive paging sub-channels, the mobile can go into sleep mode, when almost no power is used.

2.4.8 Power Control

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

The mobile station measures the signal strength or signal quality (based on the Bit Error Ratio), and passes the information to the Base Station Controller, which ultimately decides if and when the power level should be changed. Power control should be handled carefully, since there is the possibility of instability. This arises from having mobiles in co-channel cells alternatingly increase their power in response to increased co-channel interference caused by the other mobile increasing its power. This in unlikely to occur in practice but it is (or was as of 1991) under study.

2. 5. The GSM Functions

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

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

Ensuring the transmission of voice or data of a given quality over the radio link is only part of the function of a cellular mobile network. A GSM mobile can seamlessly roam nationally and internationally, which requires that registration, authentication, call routing and location updating functions exist and are standardized in GSM networks. In addition, the fact that the geographical area covered by the network is divided into cells

necessitates the implementation of a handover mechanism. These functions are performed by the Network Subsystem, mainly using the Mobile Application Part (MAP) built on top of the Signalling System No. 7 (SS7) protocol.

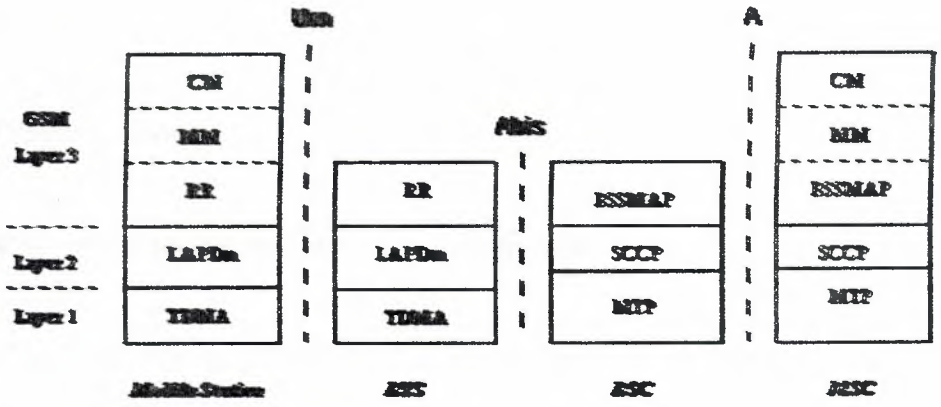


Figure 2.16 Signalling protocol structure in GSM

The signalling protocol in GSM is structured into three general layers, depending on the interface, as shown in Figure 2.16. Layer 1 is the physical layer, which uses the channel structures discussed above over the air interface. Layer 2 is the data link layer. Across the Um interface, the data link layer is a modified version of the LAPD protocol used in ISDN, called LAPDm. Across the A interface, the Message Transfer Part layer 2 of Signalling System Number 7 is used. Layer 3 of the GSM signalling protocol is itself divided into 3 sublayers.

- Radio Resources Management

  Controls the setup, maintenance, and termination of radio and fixed channels, including handovers.
- Mobility Management

  Manages the location updating and registration procedures, as well as security and authentication.
- Communication Management

  Handles general call control, and manages Supplementary Services and the Short Message Service.

Signalling between the different entities in the fixed part of the network, such as between the HLR and VLR, is accomplished throught the Mobile Application Part (MAP). MAP is built on top of the Transaction Capabilities Application Part (TCAP, the top layer of Signalling System Number 7. The specification of the MAP is quite complex, and at over 500 pages, it is one of the longest documents in the GSM recommendations.

2.5.1 Transmission

The transmission function includes two sub-functions:

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

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

2.5.2 Radio Resources Management

The radio resources management (RR) layer oversees the establishment of a link, both radio and fixed, between the mobile station and the MSC. The main functional components involved are the mobile station, and the Base Station Subsystem, as well as the MSC. The RR layer is concerned with the management of an RR-session, which is the time that a mobile is in dedicated mode, as well as the configuration of radio channels including the allocation of dedicated channels.

An RR-session is always initiated by a mobile station through the access procedure, either for an outgoing call, or in response to a paging message. The details of the access and paging procedures, such as when a dedicated channel is actually assigned to the

mobile, and the paging sub-channel structure, are handled in the RR layer. In addition, it handles the management of radio features such as power control, discontinuous transmission and reception, and timing advance.

a)Handover

In a cellular network, the radio and fixed links required are not permanently allocated for the duration of a call. Handover, or handoff as it is called in North America, is the switching of an on-going call to a different channel or cell. The execution and measurements required for handover form one of basic functions of the RR layer.

There are four different types of handover in the GSM system, which involve transferring a call between:

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

The first two types of handover, called internal handovers, involve only one Base Station Controller (BSC). To save signalling bandwidth, they are managed by the BSC without involving the Mobile services Switching Center (MSC), except to notify it at the completion of the handover. The last two types of handover, called external handovers, are handled by the MSCs involved. An important aspect of GSM is that the original MSC, the anchor MSC, remains responsible for most call-related functions, with the exception of subsequent inter-BSC handovers under the control of the new MSC, called the relay MSC.

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

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

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

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

2.5.3 Mobility Management

The Mobility Management layer (MM) is built on top of the RR layer, and handles the functions that arise from the mobility of the subscriber, as well as the authentication and security aspects. Location management is concerned with the procedures that enable the system to know the current location of a powered-on mobile station so that incoming call routing can be completed.

a) Location Updating

A powered-on mobile is informed of an incoming call by a paging message sent over the PAGCH channel of a cell. One extreme would be to page every cell in the network for each call, which is obviously a waste of radio bandwidth. The other extreme would be for the mobile to notify the system, via location updating messages, of its current location at the individual cell level. This would require paging messages to be sent to

exactly one cell, but would be very wasteful due to the large number of location updating messages. A compromise solution used in GSM is to group cells into location areas. Updating messages are required when moving between location areas, and mobile stations are paged in the cells of their current location area.

The location updating procedures, and subsequent call routing, use the MSC and two location registers: the Home Location Register (HLR) and the Visitor Location Register (VLR). When a mobile station is switched on in a new location area, or it moves to a new location area or different operator's PLMN, it must register with the network to indicate its current location. In the normal case, a location update message is sent to the new MSC/VLR, which records the location area information, and then sends the location information to the subscriber's HLR. The information sent to the HLR is normally the SS7 address of the new VLR, although it may be a routing number. The reason a routing number is not normally assigned, even though it would reduce signalling, is that there is only a limited number of routing numbers available in the new MSC/VLR and they are allocated on demand for incoming calls. If the subscriber is entitled to service, the HLR sends a subset of the subscriber information, needed for call control, to the new MSC/VLR, and sends a message to the old MSC/VLR to cancel the old registration.

For reliability reasons, GSM also has a periodic location updating procedure. If an HLR or MSC/VLR fails, to have each mobile register simultaneously to bring the database up to date would cause overloading. Therefore, the database is updated as location updating events occur. The enabling of periodic updating, and the time period between periodic updates, is controlled by the operator, and is a trade-off between signalling traffic and speed of recovery. If a mobile does not register after the updating time period, it is deregistered.

A procedure related to location updating is the IMSI attach and detach. A detach lets the network know that the mobile station is unreachable, and avoids having to needlessly allocate channels and send paging messages. An attach is similar to a location update, and informs the system that the mobile is reachable again. The activation of IMSI attach/detach is up to the operator on an individual cell basis.

b)Authentication and Security

Since the radio medium can be accessed by anyone, authentication of users to prove that they are who they claim to be, is a very important element of a mobile network. Authentication involves two functional entities, the SIM card in the mobile, and the Authentication Center (AUC). Each subscriber is given a secret key, one copy of which is stored in the SIM card and the other in the AUC. During authentication, the AUC generates a random number that it sends to the mobile. Both the mobile and the AUC then use the random number, in conjuction with the subscriber's secret key and a ciphering algorithm called A3, to generate a signed response (SRES) that is sent back to the AUC. If the number sent by the mobile is the same as the one calculated by the AUC, the subscriber is authenticated.

The same initial random number and subscriber key are also used to compute the ciphering key using an algorithm called A8. This ciphering key, together with the TDMA frame number, use the A5 algorithm to create a 114 bit sequence that is XORed with the 114 bits of a burst (the two 57 bit blocks). Enciphering is an option for the fairly paranoid, since the signal is already coded, interleaved, and transmitted in a TDMA manner, thus providing protection from all but the most persistent and dedicated eavesdroppers.

Another level of security is performed on the mobile equipment itself, as opposed to the mobile subscriber. As mentioned earlier, each GSM terminal is identified by a unique International Mobile Equipment Identity (IMEI) number. A list of IMEIs in the network is stored in the Equipment Identity Register (EIR). The status returned in response to an IMEI query to the EIR is one of the following:

- White-listed

  The terminal is allowed to connect to the network.
- Grey-listed

  The terminal is under observation from the network for possible problems.
- Black-listed

  The terminal has either been reported stolen, or is not type approved (the correct type of terminal for a GSM network). The terminal is not allowed to connect to the network.

2.5.4 Communication Management

The Communication Management layer (CM) is responsible for Call Control (CC), supplementary service management, and short message service management. Each of these may be considered as a separate sublayer within the CM layer. Call control attempts to follow the ISDN procedures specified in Q.931, although routing to a roaming mobile subscriber is obviously unique to GSM. Other functions of the CC sublayer include call establishment, selection of the type of service (including alternating between services during a call), and call release.

The CM function is responsible for:

- Call Routing.
- Supplementary Services Management.
- Short Message Services Management.

a) Call Routing

Unlike routing in the fixed network, where a terminal is semi-permanently wired to a central office, a GSM user can roam nationally and even internationally. The directory number dialed to reach a mobile subscriber is called the Mobile Subscriber ISDN (MSISDN), which is defined by the E.164 numbering plan. This number includes a country code and a National Destination Code, which identifies the subscriber's operator. The first few digits of the remaining subscriber number may identify the subscriber's HLR within the home PLMN.

An incoming mobile terminating call is directed to the Gateway MSC (GMSC) function. The GMSC is basically a switch, which is able to interrogate the subscriber's HLR to obtain routing information, and thus contains a table linking MSISDNs to their corresponding HLR. A simplification is to have a GSMC handle one specific PLMN. It should be noted that the GMSC function is distinct from the MSC function, but is usually implemented in an MSC.

The routing information that is returned to the GMSC is the Mobile Station Roaming Number (MSRN), which is also defined by the E.164 numbering plan. MSRNs are

related to the geographical numbering plan, and not assigned to subscribers, nor are they visible to subscribers.

The most general routing procedure begins with the GMSC querying the called subscriber's HLR for an MSRN. The HLR typically stores only the SS7 address of the subscriber's current VLR, and does not have the MSRN. The HLR must therefore query the subscriber's current VLR, which will temporarily allocate an MSRN from its pool for the call. This MSRN is returned to the HLR and back to the GMSC, which can then route the call to the new MSC. At the new MSC, the IMSI corresponding to the MSRN is looked up, and the mobile is paged in its current location area (see Figure 2.17).

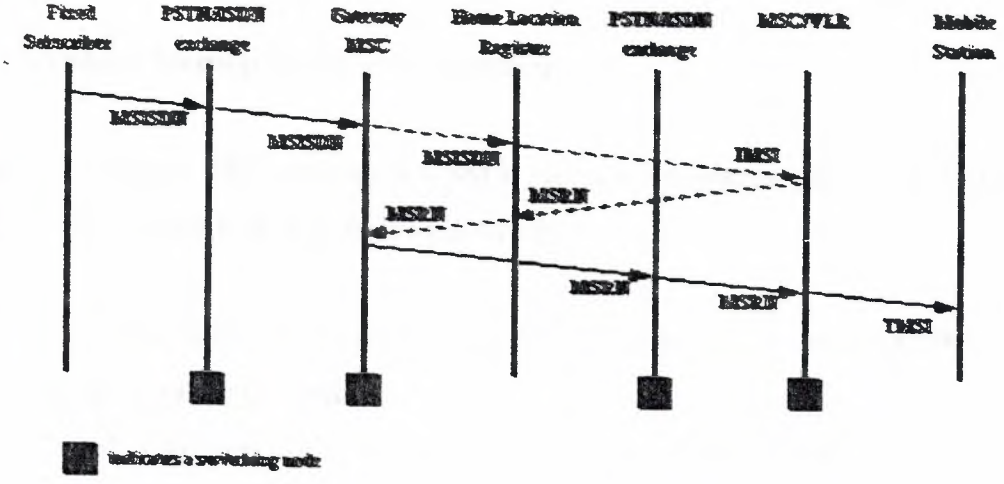


Figure 2.17 Call routing for a mobile terminating call

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

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

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

b) Supplementary Services Management

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

c) Short Message Services Management

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

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

2. 6. Wireless Application Protocol (WAP)

There are three major parts of any WAP-enabled system, namely the WAP Gateway, the HTTP Web Server, and the WAP Device itself, which is interacting with the WAP Gateway, as Figure 2.18 illustrates below. The WAP Gateway sends WML- formatted content to the WAP device, whilst the WAP gateway must communicate with the Web server using the Web's primary protocol, HTTP.

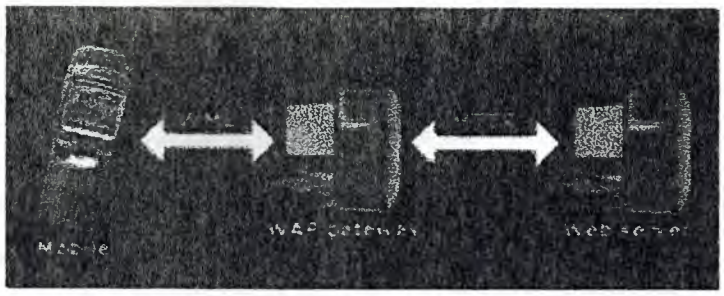


Figure 2.18 WAP-enabled System

All Web servers can communicate with a variety of information sources, using a number of different integration tools and protocols, for example a Web server can serve pages of information that are generated by tools such as Active Server Pages (ASP), ColdFusion, or PHP. Database integration is achieved using protocols such as CGI (the Common Gateway Interface) or, more likely,ODBC, as Figure 2.19 illustrates.

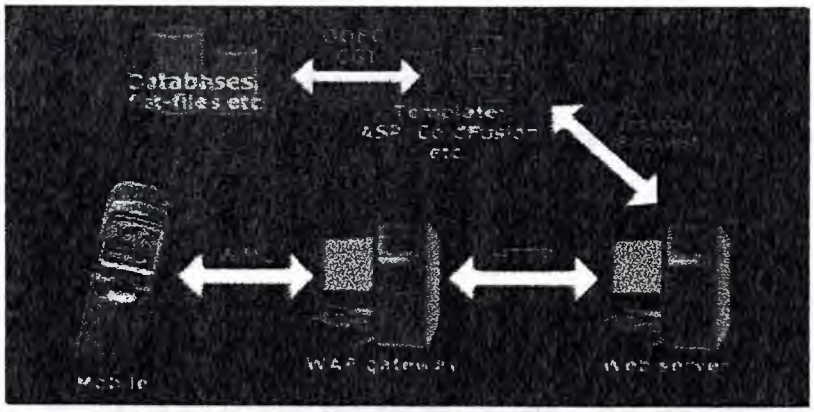


Figure 2.19 Database Integration

The Wireless Application Protocol (WAP) is a hot topic that has been widely hyped in the mobile industry and outside of it. WAP is simply a protocol- a standardized way that a mobile phone talks to a server installed in the mobile phone network. It is amazing how in just six months, it has become imperative for all Information Technology companies in Nordic countries and beyond to have a WAP division. Many many advertising agencies and "dot.coms" have announced WAP services.

WAP is hot for several reasons:

- It provides a standardized way of linking the Internet to mobile phones, thereby linking two of the hottest industries anywhere.
- Its founder members include the major wireless vendors of Nokia, Ericsson and Motorola, plus a newcomer Phone.com.
- By April 2000, the WAP Forum had over 350 member companies.
- Mobile information services, a key application for WAP, have not been as successful as many network operators expected. WAP is seen as a way to rectify this situation.

WAP also has its detractors and controversies:

- It is very difficult to configure WAP phones for new WAP services, with 20 or so different parameters needing to be entered to gain access to a WAP service.
- Compared with the installed base of Short Message Service (SMS) compliant phones, the relative number of handsets supporting WAP is tiny.
- WAP is a protocol that runs on top of an underlying bearer. None of the existing GSM bearers for WAP- the Short Message Service (SMS), Unstructured Supplementary Services Data (USSD) and Circuit Switched Data (CSD) are optimized for WAP.

The WAP standard is incomplete, with key elements such as Push (proactive sending of information to mobile devices) and wireless telephony (updating address reports and the like) included in the WAP 1.2, standardized in late 1999 and first expected to be implemented in the Spring of 2000.

There are many WAP Gateway vendors out there competing against each other with largely the same standardized product. This has led to consolidation such as the pending acquisition of APiON by Phone.com.

Other protocols such as SIM Application Toolkit and Mobile Station Application Execution Environment (MexE) are respectively already widely supported or designed to supercede WAP.

WAP services are expected to be expensive to use since the tendency is to be on-line for a long Circuit Switched Data (CSD) call as features such as interactivity and selection of more information are used by the end user. Without specific tariff initiatives, there are likely to be some surprised WAP users when they see their mobile phone bill for the first time after starting using WAP.

2. 7. General Packet Radio Service (GPRS)

Wireless communications lets people live and work in ways never before possible. With over two hundred million cellular subscribers worldwide, users have overwhelmingly embraced the concept of having a telephone that is always with them. And now business users also want a data connection with the office wherever they go, so that they can have access to e-mail, the Internet, their files, faxes and other data wherever and whenever it is needed, giving them a competitive advantage and more flexible lifestyles. A number of wireless data services are available today, but none are as exciting as a forthcoming data service for GSM networks called General Packet Radio Service (GPRS).

GPRS refers to a high-speed packet data technology, which is expected to be deployed in the next two years. It is expected to profoundly alter and improve the end-user experience of mobile data computing, by making it possible and cost-effective to remain constantly connected, as well as to send and receive data at much higher speeds than today. Its main innovations are that it is packet based, that it will increase data transmission speeds from the current 9.6 Kbps to over 100 Kbps, and that it will extend the Internet connection all the way to the mobile PC – the user will no longer need to dial up a separate ISP. GPRS will complement rather than replace the current data services available through today's GSM digital cellular networks, such as circuit-switched data and Short Message Service. It will also provide the type of data capabilities planned for "third generation" cellular networks, but years ahead of them.

2.7.1 Why is GPRS Important?

The most important aspects of GPRS are that it allows data transmission speeds to over 100 Kbps, that it is packet based, and that it supports the world's leading Internet communications protocols, Internet Protocol (IP) and X. 25.

The fact that GPRS will operate at much higher speeds than current networks should provide a huge advantage from a software perspective. Today, wireless middleware is often required to allow slow speed mobile clients to work with fast networks for applications such as e-mail, databases, groupware or Internet access. With GPRS, wireless middleware will often be unnecessary, and thus it should be easier to deploy wireless solutions than ever before.

Whereas today's wireless applications tend to be text oriented, the high throughput offered by GPRS will finally make multimedia content, including graphics, voice and video practical. Imagine participating in a video conference while waiting for your flight at the airport, something completely out of the question with today's data networks.

Why is packet data technology important? Because packet provides a seamless and immediate connection from a mobile PC to the Internet or corporate intranet allowing all existing Internet applications such as e-mail and Web browsing to operate smoothly without even needing to dial into an Internet service provider. The advantage of a packet-based approach is that GPRS only uses the medium, in this case the precious radio link, for the duration of time that data is being sent or received. This means that multiple users can share the same radio channel very efficiently. In contrast, with current circuit-switched connections, users have dedicated connections during their entire call, whether or not they are sending data. Many applications have idle periods during a session. With packet data, users will only pay for the amount of data they actually communicate, and not the idle time. In fact, with GPRS, users could be "virtually" connected for hours at a time and only incur modest connect charges. For detailed information about how GPRS works, see "For Network Managers" below.

While packet-based communications works well with all types of communications applications, it is especially well suited for frequent transmission of small amounts of data, what some call short and bursty, such as "real time" e-mail and dispatch. But packet is equally well suited for large batch operations, and other applications involving large file transfers.

GPRS will support the widely used Internet Protocol (IP) as well as the X.25 protocol. IP support is becoming increasingly important as companies are now looking to the Internet as a way for their remote workers to access corporate intranets. For further discussion about remote access, see "GPRS and Remote Access" below.

The IP protocol is ubiquitous and familiar, but what is X.25, and why is support for it important? X.25 defines a set of communications protocols that prior to the Internet constituted the basis of the world's largest packet data networks. These X.25 networks are still widely used, especially in Europe, and so wireless access to these networks will benefit many organizations. But what does this really mean? Quite simply it means that any existing IP or X.25 application will now be able to operate over a GSM cellular connection. You can think of cellular networks with GPRS service as wireless extensions of the Internet and existing X.25 networks, as shown in figure one.

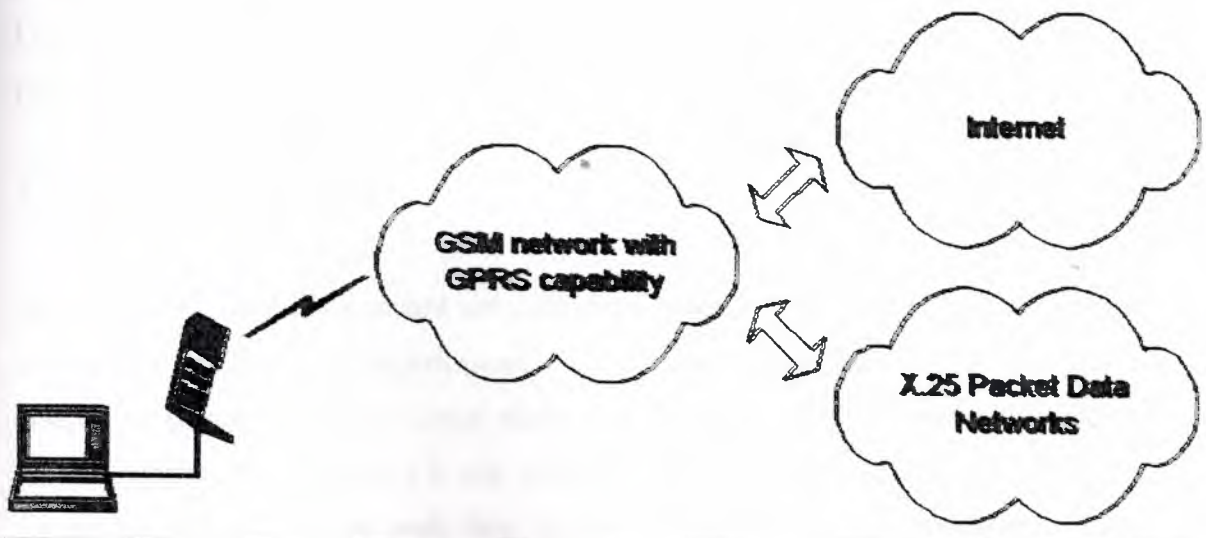


Figure 2.20 GPRS as an extension of other packet networks.

2.7.2 The User Experience

We now look more closely at how the user takes advantage of GPRS. We have already emphasized the packet nature of GPRS, which makes a GPRS connection similar in many ways to a local area network (LAN) connection. Just as with a LAN connection, once a GPRS mobile station registers with the network, it is ready to send and receive packets. A user with a laptop computer could be working on a document without even thinking about being connected, and then automatically receive new e-mail. The user could decide to continue working on their document, then half an hour later read the e-mail message and reply to it. All this time the user has had a network connection and not once had to dial in, as he or she must today with circuit-switched connections. Furthermore, GPRS allows for simultaneous voice and data communication, so the user can still receive incoming calls or make outgoing calls while in the midst of a data session.

Since there is almost no delay before sending data, GPRS is ideally suited for applications such as extended communications sessions, e-mail communications, database queries, dispatch, and stock updates to name just a few. In addition, the high throughput of GPRS will remove many of the obstacles from the use of multimedia, graphical web-based applications. For example, mobile users will be able to easily use graphically intensive web-based map application to get directions while traveling. Furthermore, with almost no transmission delay and high throughout, it will be more practical to use enterprise applications such as SAP* wirelessly and remotely.

2.7.3 Platforms and GPRS

Because GPRS supports standard networking protocols, configuring computers to work with GPRS will be very straightforward. In the case of IP communications, you will be able to use existing TCP/IP protocol stacks, such as the stack that comes with Windows 95 or Windows 98, Windows CE and Windows NT. TCP/IP stacks are readily available for most other platforms as well. With all the developments in the handheld computer area, you can expect a multitude of hardware platforms to take advantage of GPRS.

- Laptops or handheld computers connected to GPRS-capable cellphones or external modems
- Laptops or handhelds with GPRS-capable PC Card modems
- Smart phones that have full screen capability (e.g. Nokia* 9000)
- Cellphones employing microbrowsers using the Wireless Application Protocol
- Dedicated equipment with integrated GPRS capability, e.g. mobile credit-card swipers

GPRS coincides with another important technology development: the replacement of a cable connection to a cellphone by a short radio link. Intel, Ericsson, Nokia, IBM, Toshiba and others are already working on such wireless connections in an initiative called "Bluetooth".

As we discuss next, GPRS is also complementary with an important industry trend associated with remote access: the transition from dial-up remote access to Internet-based remote access.

2.7.4 GPRS and Remote Access

Traditionally companies have provided remote access for their workers using dial-up modem connections into corporate modem pools. But as companies have established high speed connections to the Internet, and as remote workers have an increasing number of options for connecting to the Internet, companies are now looking to the Internet as a way for their remote workers to access corporate intranets. This is especially effective because most communications applications today work over IP networks -- including many originally designed for modem dial-up connections. It can be highly cost effective to use the Internet instead of making long distance phone calls, and in the case of international connections, much more reliable. But this Internet-based technique does raise an issue of privacy from hackers. A new technology is emerging which addresses privacy and authentication concerns, referred to as a virtual private network (VPN).

A VPN is a method of having private communications across public networks. It adds additional software at each end of the connection -- in our case the mobile computer and the corporate network. This software establishes what are called "tunnels". Within this

tunnel, information is encrypted and additional information is added to each packet to prevent tampering. Various standards are available or being finalized to define interoperability between VPN products, including the Point to Point Tunneling Protocol (PPTP), Layer Two Tunneling Protocol (L2TP), SOCKS and IPsec (Secure IP). A wide range of companies already offer VPN solutions today, including router vendors, network software providers, firewall suppliers and companies specializing in this area. Since most VPN solutions are quite flexible in their feature set, corporate IT can choose the level and type of protection desired, such as 56 bit encryption or 128 bit encryption.

Almost all VPN technologies operate independently of the communications link, meaning the same VPN technology will work with a dial-up modem connection, Ethernet connections, ISDN connections and most importantly for us, wireless connections. See figure two.

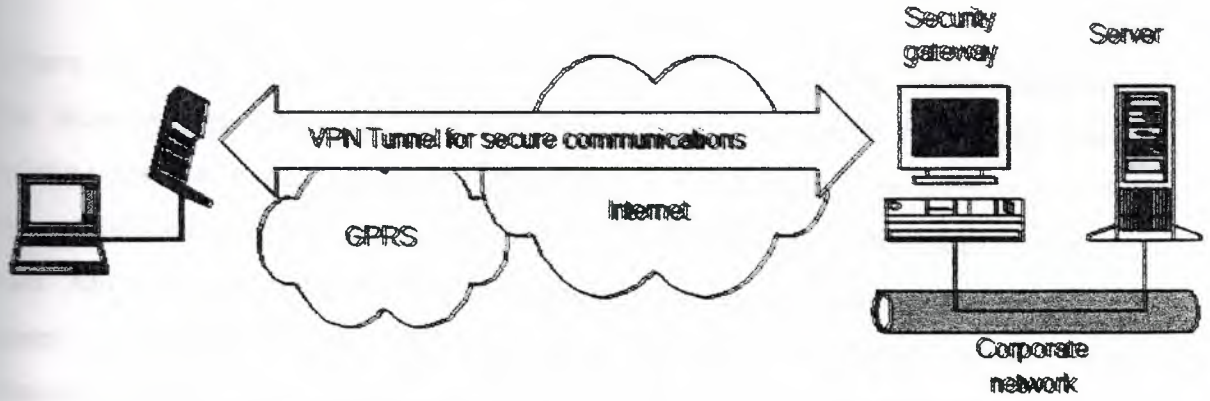


Figure 2.21 Tunneling with VPN technology

Companies using VPNs will be able to smoothly migrate from existing wireless technologies to GPRS. Today their users can make circuit-switched connections to an Internet service provider, and then establish a VPN connection. Once GPRS becomes available, the Internet connection will extend to the mobile computer and the user will no longer need to dial a separate ISP. The net result is wireless connectivity that works hand in hand with VPN technologies to let remote workers easily access corporate resources and to stay in touch with their work teams.

2.7.5 The Road Map

According to Kevin Holley, the chair for the GSM SMG4 committee, which develops GPRS standards, the first version of the GPRS standard is complete, while a next version of the standard that adds advanced features such as point-to-multipoint communications is in development. Most GSM vendors such as Alcatel, Ericsson, Lucent, Motorola, Nokia, Nortel, and Siemens have been active in the standards process and many are developing the necessary infrastructure elements. Field trials are expected in 1999 and deployment will begin in the year 2000. Though the GPRS standard specifies support for both X.25 and IP, it is likely that vendors and operators will emphasize IP service. It is also likely that GPRS will first roll out in European countries. As of late 1998, no operators have announced when they will deploy GPRS service, but it is very likely that many will do so, especially since the infrastructure cost of deploying the service is relatively modest. At this time no cellphones or modems that support GPRS have been announced but it is possible that eventually all new GSM phones will support GPRS.

Where does GPRS fit in with other GSM data developments, as well as data capabilities for other wireless networks? The first improvement with GSM data is increasing existing circuit-switched data speeds from 9600 bps to 14.4 kbps. The addition of V.42 bis compression over the airlink will further increase throughput by about a factor of two. After that, and before GPRS is available, some carriers will begin offering high speed circuit-switched data (HSCSD) which like GPRS combines multiple voice channels to offer higher data rates. SingTel in Singapore announced in May of 1998 that using HSCSD technology it will soon be offering data rates of up to 38.4 kbps.

Another development is referred to by some as "direct IP access". The user makes a circuit-switched data call, but rather than switching the call into the public switched telephone network, the carrier terminates it at a router that is connected to the Internet. From the user perspective, the carrier appears like an Internet service provider offering dial-up service. This hybrid circuit/packet type of service is a good stepping-stone to GPRS and will also work with HSCSD.

And GSM standards bodies are already defining data networking technologies that will build upon GPRS. One such technology is called Enhanced Data rate for GSM Evolution (EDGE) which will offer a maximum theoretical rate of 384 kbps, though normal operating speeds will be about half this rate. Beyond EDGE, third generation cellular systems will eventually offer data rates to 2 Mbps. The table below summarizes all these developments.

Table 2.4 Road Map of Data Services for GSM

	Timeframe	Capabilities	Notes
9.6 kbps service	Available today	Circuit-switched data and fax	Service available from most GSM operators today.
14.4 kbps service	Available over next 12 months	Higher speed circuit-switched data and fax	Should work identically to 9.6 kbps service only at higher speed. V.42 bis compression will further increase throughput by about 200%.
Direct IP Access	Available from some carriers today	Circuit-switched connection directly to Internet	Reduces call set-up time and provides a stepping stone to packet data. Will also be available for high-speed circuit-switched data services.
High-speed circuit-switched data service (HSCSD)	Available within 12 months	High speed rates to 56 kbps	A software-only upgrade for carriers not requiring expensive infrastructure. Operators will need to decide whether to offer this service or GPRS or both.
GPRS	Available within two years	High speed packet data with transmission speeds over 100 Kbps, with most user devices offering about 56 kbps	Extremely capable and flexible mobile communications.
EDGE	Available within three years	High speed packet data which will triple the rates available with GPRS	Final high-speed data technology for existing GSM networks. Will also be used with IS-136 TDMA networks.
Third generation cellular	Available within three to five years	High speed packet data to 2 Mbps	Completely new airlink.

Data services similar to those for GSM are also being developed for IS-136 TDMA and CDMA networks. But as a more mature digital technology, GSM has a strong head start. When GPRS is deployed, no other wireless data technology will be able to match its capabilities. But it is also important to remember that GSM already offers excellent data and fax capabilities that provide more than sufficient capability for many types of applications. As technologies like GPRS become available, the scope of data applications that are practical for wireless connectivity will only increase.

2.7.6 GPRS Details

To better understand GPRS, we take a quick tour beginning with the mobile PC and traversing through the network. First, we have a notebook computer connected to a GPRS-capable cellphone or modem, either through a serial cable or other type of connection such as Universal Serial Bus (USB) or local wireless link. Or perhaps the connection device is in the form of a PC Card. The GPRS phone or modem communicates with GSM base stations, but unlike circuit-switched data calls which are connected to voice networks by the mobile switching center, GPRS packets are sent from the base station to what is called a Serving GPRS Support Node (SGSN). The SGSN is the node within the GSM infrastructure that sends and receives data to and from the mobile stations. It also keeps track of the mobiles within its service area. The SGSN communicates with what is called the Gateway GPRS Support Node (GGSN), a system that maintains connections with other networks such as the Internet, X.25 networks or private networks. See figure two. A GPRS network can use multiple serving nodes, but requires only one gateway node for connecting to an external network such as the Internet.

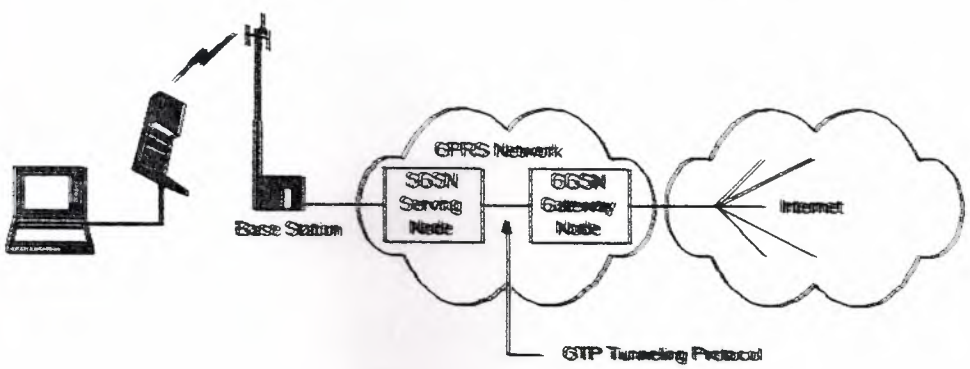


Figure 2.22 GPRS system.

When the mobile station sends packets of data, it is via the SGSN to the GGSN, which converts them for transmission over the desired network, which could be the Internet, X.25 networks or private networks. IP packets from the Internet addressed for the mobile station are received by the GGSN, forwarded to the SGSN and then transmitted to the mobile station.

To forward IP or X.25 packets between each other, the SGSN and GGSN encapsulate these packets using a specialized protocol called the GPRS tunnel protocol (GTP) which operates over the top of standard TCP/IP protocols. But the details of the SGSN and GGSN are both invisible and irrelevant to the user who simply experiences a straightforward IP or X.25 connection that just happens to be wireless.

An interesting aspect of GPRS is how it achieves its high speeds to over 100 kbps when circuit-switched data today is limited to 9600 or 14.4 kbps. GPRS uses the same radio channel as voice calls, a channel that is 200 kHz wide. This radio channel carries a raw digital radio stream of 271 kbps which for voice calls is divided into 8 separate data streams, each carrying about 34 kbps. After protocol and error correction overhead, 13 kbps is left for each voice connection or about 14 kbps for data. Circuit-switched data today uses one voice channel. GPRS can combine up to 8 of these channels, and since each of these can deliver up to 14 kbps of data throughput, the net result is that users will be able to enjoy rates over 100 Kbps. But not all eight-voice channels have to be used. In fact, the most economical phones will be ones that are limited to 56 kbps. The GPRS standard defines a mechanism by which a mobile station can request the amount of bandwidth it desires at the time it establishes a data session.

3. THE ARCHITECTURE OF THE CELLULAR MOBILE SYSTEM

3. 1. What is a Cellular Phone System?

No strict definition of a cellular phone system is generally accepted by industry professionals, but most experts would agree that it usually entails the following specific characteristics:

1. Division of heavily populated areas into small regions called cells. In this way, concentrated areas of population can have more transmitting stations;
2. Reducing coverage area yields to reduce the power of transmission and reuse the same frequencies in the different base stations;
3. Special design features that allow transmitters and receivers to operate in a controlled-interference environment;
4. Computer-controlled capabilities to set up automatic hand-offs from base station to base station when the signal-to-noise ratio or transmission distance can be improved to a more acceptable value.

3. 2. The Cellular Concept

Cellular mobile communication is based on the concept of frequency reuse. That is, the limited spectrum allocated to the service is partitioned into, for example, N non-overlapping channel sets, which are then assigned in a regular repeated pattern to a hexagonal cell grid. The hexagon is just a convenient idealization that approximates the shape of a circle (the constant signal level contour from an omnidirectional antenna placed at the center) but forms a grid with no gaps or overlaps. The choice of N is dependent on many trade-offs involving the local propagation environment, traffic distribution, and costs. The propagation environment determines the interference received from neighboring co-channel cells which in turn governs the reuse distance, that is, the distance allowed between co-channel cells (cells using the same set of frequency channels).

The cell size determination is usually based on the local traffic distribution and demand. The more the concentration of traffic demand in the area, the smaller the cell has to be

sized in order to avail the frequency set to a smaller number of roaming subscribers and thus limit the call blocking probability within the cell. On the other hand, the smaller the cell is sized, the more equipment will be needed in the system as each cell requires the necessary transceiver and switching equipment, known as the base station subsystem (BSS), through which the mobile users access the network over radio links. The degree to which the allocated frequency spectrum is reused over the cellular service area, however, determines the spectrum efficiency in cellular systems. That means the smaller the cell size, and the smaller the number of cells in the reuse geometry, the higher will be the spectrum usage efficiency. Since digital modulation systems can operate with a smaller signal to noise (i.e., signal to interference) ratio for the same service quality, they, in one respect, would allow smaller reuse distance and thus provide higher spectrum efficiency. This is one advantage the digital cellular provides over the older analogue cellular radio communication systems.

It is worth mentioning that the digital systems have commonly used sectored cells with 120-degree or smaller directional antennas to further lower the effective reuse distance. This allows a smaller number of cells in the reuse pattern and makes a larger fraction of the total frequency spectrum available within each cell. Currently, research is being done on implementing other enhancements such as the use of dynamic channel assignment strategies for raising the spectrum efficiency in certain cases, such as high uneven traffic distribution over cells.

3. 3. Cellular Coverage

The major problems with radio distribution arise from electromagnetic wave propagation. As mentioned in the power of radio waves decreases with the inverse of the squared distance (d^{-2}); however, it must be remembered that this applies only in empty space. As a consequence, propagation at ground level in an urban environment with different obstacles is more difficult. A second problem is spectrum scarcity: the number of simultaneous radio communications supported by a base station is therefore limited. Cellular coverage allows a high traffic density in a wide area despite both problems at the expense of infrastructure cost and of complexity. Because of the limited transmission range of the terminals, cellular system is based on a large number of

receptions and transmission devices on the infrastructure side (the base stations), which are scattered over the area to cover a small geographical zone called a cell.

3.3.1 Cluster

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

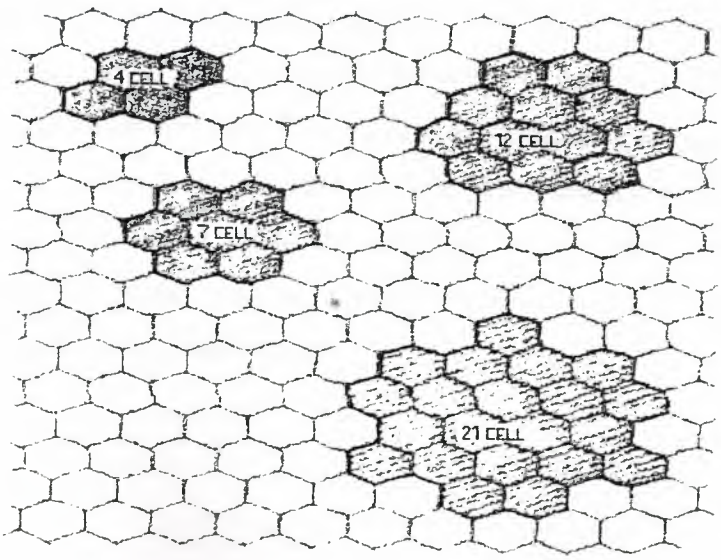


Figure 3.1 Typical clusters

- **Macrocells**

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

- **Microcells**

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

- **Selective cells**

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

- **Umbrella cells**

A freeway crossing of very small cells produces an important number of handovers among the different small neighbouring cells. In order to solve this problem, the concept of umbrella cells is introduced. An umbrella cell covers several microcells. The power level inside an umbrella cell is increased comparing to the power levels used in the microcells that form the umbrella cell. When the speed of the mobile is too high, the mobile is handed off to the umbrella cell. The mobile will then stay longer in the same cell (in this case the umbrella cells). This will reduce the number of handovers and the work of the network.

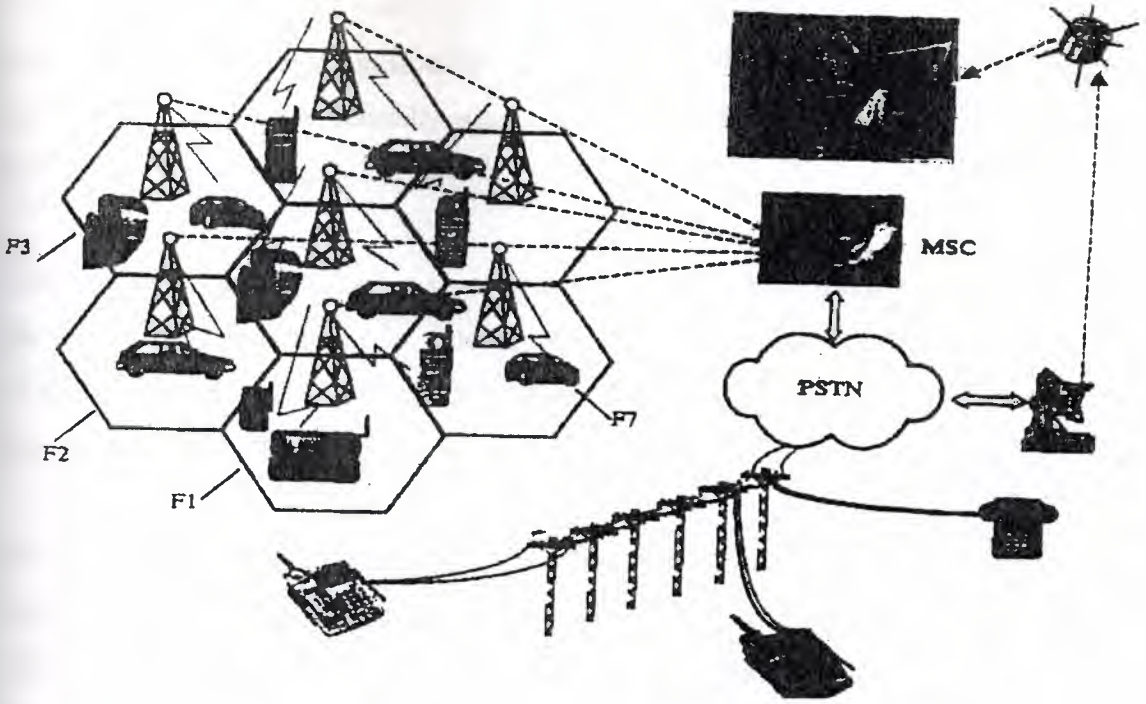


Figure 3.2 The cellular setup

The cells are often represented by hexagons, in order to model the system by paving the plane with a single geometrical figure. Hexagons nicely pave the plane without overlapping and are commonly used for calculating theoretical frequency reuse in cellular system.

At the centre of each hexagonal cell is a base station consisting primarily of a power source, computer-processing devices, and a base antenna. Each of the seven base stations in the Figure 3.2 operates on a different frequency, denoted by Fl, F2,...,F7. In the Global System for Mobile Communication (GSM), the design was aimed at the beginning at medium-sized cells, of a diameter expressed in kilometers or tens of kilometers. Yet, the lower boundary is difficult to determine: cells of more than one kilometer radius should be no problem. Whereas the system may not be fully suitable to cells with a radius below, say 300 meters. One source of limitation is more economics than due to physical laws. The efficiency of the system decreases when cell size is reduced and then the ratio between the expenditure and the traffic increases, and eventually reaches a point where economical considerations call for a halt. Another important point is the capacity of the system to move communication from one cell to another rapidly, and GSM requires longer a time to prepare such a transfer to cope with

fast moving users in very small cells. The cell size upper bound is more obvious: The first, non-absolute, limitation in GSM is a range of 35 kilometers. Cells of bigger sizes are possible but require specially designed cell-site equipment and incur some loss in terms of maximum capacity.

The number of sites to cover a given area with a given high traffic density, and hence the cost of the infrastructure, is determined directly by the reuse factor and the number of traffic channels that can be extracted from the available spectrum. These two factors are compounded in what is called the spectral efficiency of system.

Seven cell configurations are used in industry, but so are 3 cell configurations, 4 cell configurations, 12 cell configurations, and even 21 cell configurations. Moreover even when a seven-cell configuration is employed, the signals from the individuals base stations do not span neat and clean hexagonal cells. Neat and clean coverage zones do not exist in the real world because, houses, buildings, and natural barriers together with unavoidable sources of RF interference create coverage regions that are shaped more like amoebas than circles or hexagonal cells. The cellular setup is shown in Figure 3.2.

The mobile units consist of a control unit, a transceiver, and appropriate antennas. The transceiver contains circuits that can tune to any of the 666 FM channels in the 800 MHz range assigned to the cellular system. Each cell site has at least one set up channel dedicated for signalling between the cell and its mobile units. The remaining channels are used for conversation. Each mobile unit is assigned a 10 digit number, identical inform to any other phone number. Callers to the mobile unit will dial the local or long distance number for desired mobile unit. The mobile user will dial 7 or 10 digits with a zero or a one prefix, where applicable, in case of calling from a fixed phone.

Whenever a mobile unit is turn on but not in use, the mobile control unit monitors the data being transmitted on a set up channel selected from among the several standards set up frequencies on the bases of signal strength. If signal strength becomes marginal as the mobile unit approaches a cell boundary, the mobile control finds a setup channel with a stronger signal.

3.3.2 Setting Up a Cellular Phone Call

When a phone call comes into the cellular system, from the conventional Public Switching Telephone Network (PSTN) or from another cellular phone, the computer-based Mobile Switching Centre (MSC) follows the three steps depicted in setting up the proper connection. In step one, an appropriate paging message is directed by MSC to all the Base Stations (BS) [Figure 3.3 (a)]. In the step two, appropriate cellular telephone acknowledges the page by sending digital pulse-train, back to the base station from which a signal came [Figure 3.3 (b)]. In step three, the base station automatically selects and activates a duplex voice channel to handle the call, then signals appropriate cellular phone for transmission and reception [Figure 3.3 (c)].

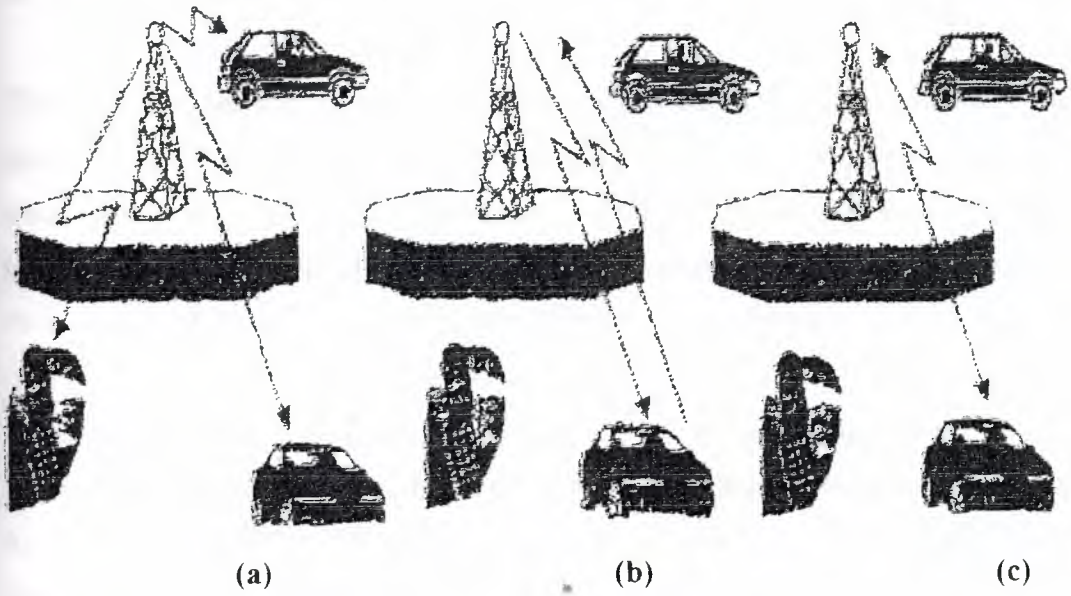


Figure 3.3 Setting up a cellular phone call

3.3.3 Roamers

The system is designed to make handling of roamers automatic. This is the principal goal of the cellular approach. Locating and hand-off are the concept that comes directly from the use of small cells. "Locating" in this sense is not the determination of precise geographic location-although that is obviously a factor. It is the process of determining

whether a moving active user should continue to be served by his current channel and transmitter, or "handed off" to either another channel, cell, or both. The decision is made automatically by a computer, based on signal quality and potential interference, and involves sampling the signal from the mobile unit.

The Mobile Switching Centre (MSC) computer continuously analyses signal quality and makes the appropriate changes without any interruption in service.

With the cellular system, a subscriber could make a call from his car while driving in the countryside toward a city, continue through the city's downtown, and not hang up until well beyond the city on the other side. More importantly, the switching of transmitters and frequencies during the conversation would be entirely automatic, with no interruptions and no action required by the user or an operator.

The base stations are connected to the computer-based MSC a specifically designed computer telecommunications facility that sets up the proper connections, keeps the track of billing charges, and automatically handles any necessary hand-offs. Hand-offs to a new base station are attempted whenever the signal quality degrades as users travel through the cellular phone coverage area from one cell to another.

Trunk lines connect the cellular switch to the PSTN, and from the mobile cellular phone system can originate from or be directed toward ordinary phones or cellular phones located in completely different parts of the country. Because of their extensive frequency reuse in a small local area, cellular phone systems can handle a multitude of users. In most urban areas government regulators maintain the proper competitive environment by licensing two separate cellular phone companies, thus giving customers a choice between competitors.

Wherever there is a system to serve it, a roaming unit will be able to obtain a complete automatic service; however a call from a land phone to a mobile unit, which has roamed, to another metropolitan area presents additional problems. It would be technically possible for the system to determine automatically where the mobile unit is, and to connect it automatically to the land party. There are two reasons for not doing so. First, the caller will expect to pay only a local charge if a local number is dialed.

Second, the mobile user may not want to he identified to be at a particular location automatically by the system without an approval. Therefore the system will complete the connection only if the extra charge is agreed to, and when possible to do so without unauthorised disclosure of the service area to which the mobile unit has roamed.

3.3.4 Unique Features

There are two essential elements of the cellular concept, which are unique: frequency reuse and cell splitting.

Frequency reuse means using the same frequency or channel simultaneously for different phone conversations, in the same general geographic area. The idea of having more than one transmission on a given frequency is not new; it is done in virtually all radio services. What are unique to cellular systems-the closeness of the users; two users of the same frequency maybe only a few dozen miles apart, rather than hundreds of miles. This is achieved using relatively low-power transmitters on multiple sites, rather than single high-power transmitter that do this. Each transmitter covers only its own cell, and cells sufficiently far a part can also use the same frequency.

Cell splitting is based on the notion that cell sizes are not fixed and may vary in the same area or over time. The principle of the cell splitting, initially all the cells in an area may be relatively large. When the average number of users in some cells becomes too large to be handled with proper service quality, the overloaded cells are split into smaller cells by adding more transmitters. The same MSC can continue to serve all of the cell sites, but expansion of its computer and switching facilities probably will be required.

Multiple frequency reuse is possible because of the lower transmitter power radiated in each cell, and by not using the same frequency in adjacent cells. The cellular system can be expanded because cell splitting may occur as demand increases.

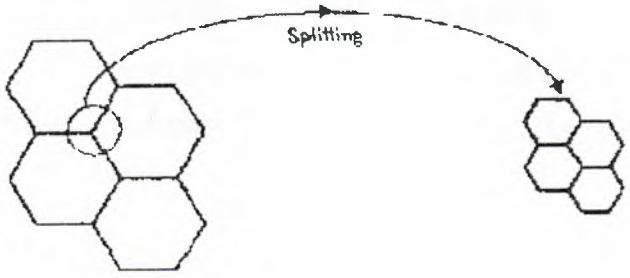


Figure 3.4 Splitting

The spectrum scarcity is circumvented by the reuse of radio resources. Frequencies used in a given cell are reused few cells away, at a distance sufficient enough so that the unavoidable interference created by the close use of the same spectrum which has fallen to an acceptable level. This depends in particular on the transmission method. This concept of frequency reuse is the key capacity. As an example, if the same frequency may be reused in very ninth cell, a spectrum allocation of N frequencies allows N/9 carriers to be used simultaneously in any given cell. The total system throughput can, therefore, be increased by reducing the cell size.

The world's most popular cellular phone system was Advanced Mobile Phone System (AMPS) developed in the United States, and Total Access Cellular System (TACS), developed to serve various European countries.

The American AMPS is an 800 MHz system with 30-kHz channel separations. Each cell handles 832 frequency modulation (FM) channels with digital frequency shift keying for the control-channel modulations. AMPS is presently being used in 37 different countries.

The TACS system operates at 900 MHz with 920 channels separated by 25 kHz. Like the AMPS system. TACS uses FM analog voice-channel modulations with digital frequency shift keying for the control channels.

3.3.5 Cell-site controller

Each cell contains one cell-site controller that operates under the direction of the

switching centre. The cell-site controller manages each of the radio channels at the site, supervises calls, turns the radio transmitter and receiver on and off, injects data onto the control and user channels, and performs diagnostic tests on the cell-site equipment.

3. 4. Basic Wireless Principles

3.4.1 Cellular Defined

Four key components make up most cellular radio systems: the cellular layout itself, a carefully engineered network of radio base stations and antennas, base station controllers which manage several base stations at a time, and a mobile switch, which gathers traffic from dozens of cells and passes it on to the public switched telephone network.

All analog and digital mobiles use a network of base stations and antennas to cover a large area. The area a base station covers is called a cell, the spot where the base station and antennas are located is called a cell site. Viewed on a figure, the small territory covered by each base station appears like a cell in a honeycomb, hence the name cellular. Cell sizes range from sixth tenths of a mile to thirty miles in radius for cellular (1km to 50km). GSM and PCS use much smaller cells, no more than 6 miles (10km) across. A large carrier may use hundreds of cells.

Each cell site's radio base station uses a computerized 800 or 1900 megahertz transceiver with an antenna to provide coverage. Each base station uses carefully chosen frequencies to reduce interference with neighboring cells. Narrowly directed sites cover tunnels, subways and specific roadways. The area served depends on topography, population, and traffic. In some PCS and GSM systems, a base station hierarchy exists, with pico cells covering building interiors, microcells covering selected outdoor areas, and macrocells providing more extensive coverage to wider areas. See Figure 3.5 below.

The macro cell controls the cells overlaid beneath it. A macro cell often built first to provide coverage and smaller cells built to provide capacity.

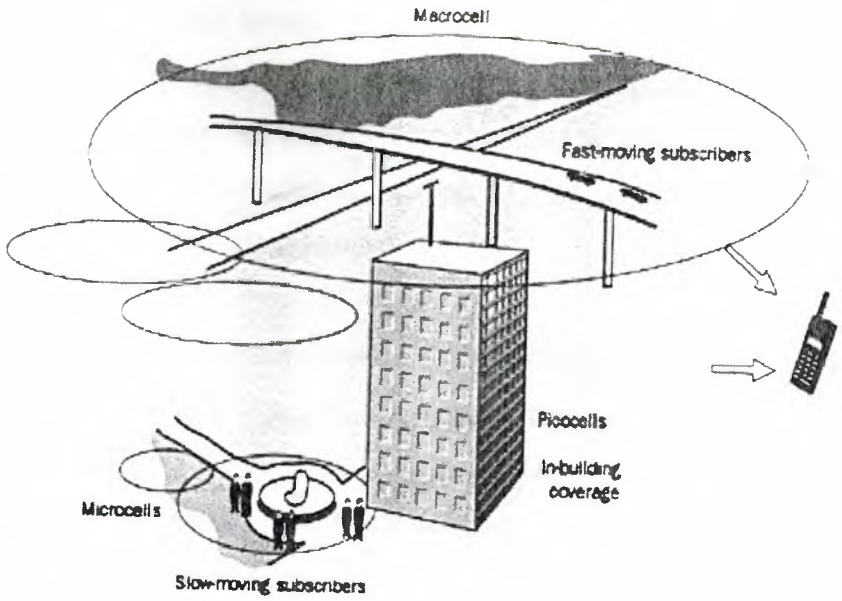


Figure 3.5 Pico cell, Microcell, Macrocell

Figure describes a business park or college campus as a typical situation. In those cases a macrocell provides overall coverage, especially to fast moving mobiles like those in cars. A microcell might provide coverage to slow moving people between large buildings and a piconet might cover an individual lobby or the floor of a convention center.

Typically microcells are employed along the sides of busy highways or on street corners.

Base station equipment by itself is nothing without a means to manage it. In GSM and PCS 1900 that's done by a base station controller or BSC. As Nokia puts it, a base station controller "is a high-capacity switch which provides total overview and control of radio functions, such as handover, management of radio network resources and handling of cell configuration data. It also controls radio frequency power levels in the RBSs, and in the mobile phones. Base station controllers also set transceiver configurations and frequencies for each cell." Depending on the complexity and capacity of a carrier's system, there may be several base station controllers.

These BSCs react and coordinate with a mobile telecommunication switching office or MTSO, sometimes called, too, a MSC or mobile switching center. With AMPS or D-

AMPs, however, the mobile switch controls the entire network. In either case, the mobile switch interacts with distant databases and the public switched telephone network or PSTN. It checks that a customer has a valid account before letting a call go through, delivers subscriber services like Caller ID, and pages the mobile when a call comes in. Among many other administrative duties.

How does this work out in the real world? Consider Omnipoint's PCS network for the greater city area. To cover the 63,000-square-mile service area, Ericsson says Omnipoint installed over 500 cell sites, with their attendant base stations and antennas, three mobile switching centers, one home location register, and one service control point. (The latter two are network resources.) The entire system cost $680 million dollars, although they didn't say if that included Omnipoint's discounted operating license. What makes up a cellular network, let's discuss the idea that makes that makes those networks possible: frequency reuse.

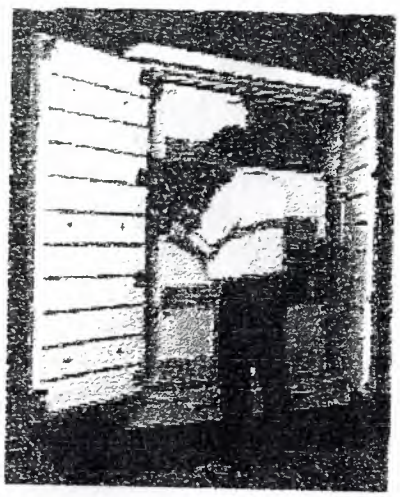


Figure 3.6 Dual band IS-136 Ericsson RBS 884 base station

3.4.2 Frequency reuse

The heart and soul, the inner core, the sine qua non of cellular radio is frequency reuse. The same frequency sets are used and reused systematically throughout a carrier's coverage area. If you have frequency reuse you have cellular. Frequency reuse

distinguishes cellular from conventional mobile telephone service, where only a few frequencies are used over a large area, with many customer's competing to use the same channels. Much like a taxi dispatch operation, older style radio telephone service depended on a high powered, centrally located transmitter which paged or called mobiles on just a few frequencies.

Cellular instead relies on a distributed network of cells, each cell site with its own antenna and radio equipment, using low power to communicate with the mobile. In each cell the same frequency sets are used as in other cells. But the cells with those same frequencies are spaced many miles apart to reduce interference. Thus, in a 21 cell system a single frequency may be used several times. The lone, important exception to this are CDMA systems. In those, the same frequencies are used by every cell.

Each base station, in addition, controls a mobile's power output, keeping it low enough to complete a circuit while not high enough to skip over to another cell.

Figure 3.7 Cells with different set of channels

The frequency reuse concept. Each honeycomb represents a cell. Each number represents a different set of channels or paired frequencies. A cellular system separates each cell that shares the same channel set. This minimizes interference while letting the same frequencies be used in another part of the system. This is frequency reuse. Note, though, that CDMA based systems can use, in theory, all frequencies in all cells, substantially increasing capacity . For review, a channel is a pair of frequencies, one for transmitting on and one for receiving. Frequencies are described by their place in the radio spectrum, such as 900mHZ, whereas channels are described by numbers, such as channels 334 through 666.

3.4.3 Adding Cells and Cell Sectorizing

Adding cells and sectoring cells allows cellular expansion. Don't have enough circuits in a crowded cell? Too many customers? Then add to that cell by providing smaller cells like micro and pico cells, underneath and controlled by the existing and larger macro cell.By placing these short-range microcells along busy highways or at busy street corners, you effectively reduce the strain on the primary macrosites by a substantial margin.

Splitting a single cell does not mean that it is broken into smaller cells, like a dividing amoebae, but rather into sectors. A previously omnidirectional base station antenna, radiating equally in all directions, is replaced by several directional antennas on the same tower. This "sectorizing" thus divides the previously homogeneous cell into 3 or 6 distinct areas (120 and 60 degrees around the site respectively). Each sector gets its own frequencies to operate on.

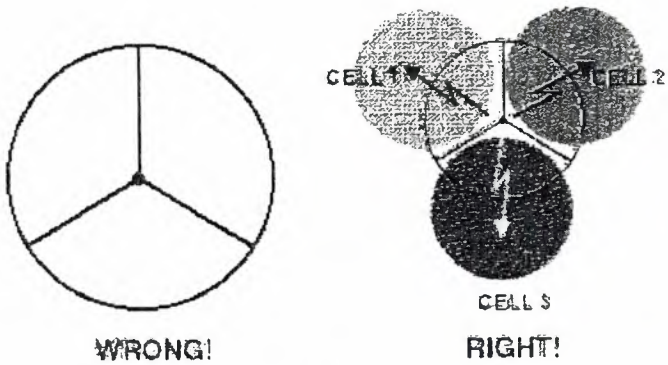


Figure 3.8 A cell site does not lie at the center of a cell, rather it lies at the edge of several cells. The pipe shared pieces represents sectors, cell areas covered by directional antennas at the cell site, using different frequencies than the other sectors and cells.

We sector cells to reduce interference between similar cells in adjacent clusters. Cell splitting is done to increase traffic capacity.

According to Telephony Magazine, AT&T began splitting their macrocell based New York City network in 1994. (They use IS-136 at both 800 and 1900 MHz.) Starting in Midtown Manhattan, the $30 million-plus project added 55 microcells to the three square mile area by 1997, with 10 more on the way. Lower Manhattan got a "few dozen." Microcells in lower Manhattan sought to increase signal quality, while Midtown improvements tried to increase system capacity. An AT&T engineer said "a macrocell costs $500,000 to $1 million to build, a microcell one-third as much and you don't have to build a room around it." AT&T used Ericsson base stations, with plans to use Ericsson 884 base stations as pictured above in the future. Camouflaged antennas got placed on buildings between 25 and 50 feet above street level.

3. 5. Cellular Phone

Cellular phone, or the advanced mobile phone service (AMPS), is a circuit-switched system. It is a means of providing mobile phone service using radio frequency transmission. In a traditional mobile phone system, a radio tower is placed at the centre of a city, and serves mobile vehicles within a radius of 25 to 75 miles. In most areas the number of channels available is around 40, making it possible to serve only a limited number of customers.

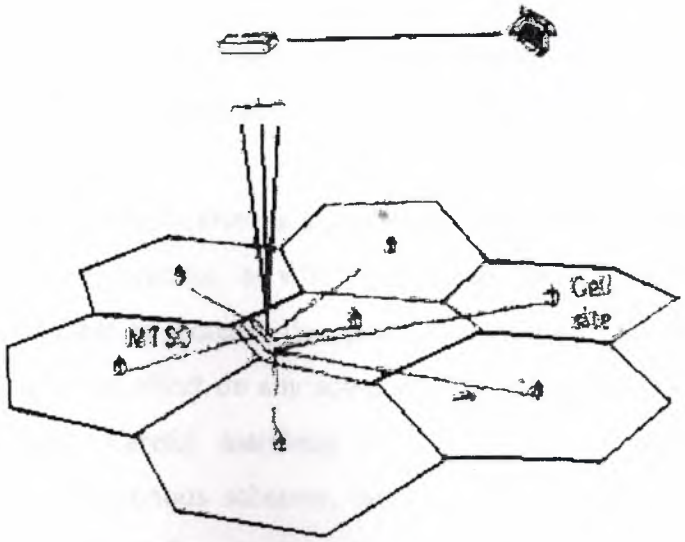


Figure 3.9 The AMPS system with cell sites located at the center each cell

Moreover, the strong signal emitted from the radio tower prevents the use of the same frequencies by radio towers in nearly cities from interference. In the cellular phone system, the total area covered by the system is divided into cells. Each cell has the shape of a hexagon, or a circle, and is served by a cell site. The cell site is an interface between the car phone and the terrestrial public phone network.

A large central controller called the mobile phone switching office (MTSO) controls all cell sites. All cell sites are wires connected to the MTSO.

Radio communications between the mobile vehicle and the cell site employs frequency modulation (FM). The capture effect of FM causes, when two separate transmissions on the same frequency arrive at a receiver, the receiver to suppress the weaker (that is the interfering) signal and detect the stronger signal without significant quality degradation. The AMPS utilises this FM capture effect to increase the efficiency in the use of the radio spectrum by repeating the use of channel frequencies in different cell sites. If two cell sites simultaneously transmit on the same radio channel, a FM receiver tuned to that channel will lock onto the transmitter with the stronger are quite different. However, in an AM system, changes in either the modulation or in the signal level affect the same parameter, amplitude. Therefore under conditions when the mobile receiver is subjected to signal components from more than one transmitter, modulation will be additive in the AM case whereas the situation with receivers is much more complex. Quasi-synchronous, W1 schemes have been found to operate most successfully when the frequency of sets between the transmitters are a few Hz.

The AGC system in an AM receiver is designed to compensate only for variations in the mean signal level and in practice, as will be seen later, these occur relatively slowly. It is considered undesirable to increase the speed of response of the AGC system, as this would have a detrimental effect on any sub-audio signalling systems such as those used for selective calling. Careful matching of the transmitter modulation indices is employed in quasi-synchronous schemes, but the accuracy of matching is not highly critical. Deterioration of performance occurs gradually with mismatch in AM schemes and this significantly eases the task of installatton. In addition, with AM schemes, it is relatively simple to employ "fill-in" base stations to improve coverage in areas where reception would otherwise be very poor. In an area where the receiver is subject to weak

signals. The effect of quasi-synchronous operation is to pause a periodic increase in the background noise level at a rate equal to the offset frequency. This has only a minor detrimental effect on speech transmissions, but is potentially more serious when high-speed data is being transmitted over the link.

Quasi-synchronous FM (also known as Simulcast) schemes were initially set up with carrier frequency offsets of a few tens of Hz, which in the early days represented the performance limitation of quartz crystal oscillators. It was assumed that, due to the capture effect inherent in FM receivers.

The mobile would respond only to the strongest signal present and that period of apparently equal signal strength, when capture would not occur. Would be infrequent and would produce few problems. In practice, it was difficult to obtain good performance unless the modulation matching was very carefully undertaken with respect to both amplitude and phase. In addition, steps needed to be taken to avoid even approximately equal strength signals in areas where intelligible communication was required. The difficulties in establishing a successful quasi-synchronous FM scheme were considerable. It was marginally easier at UHF than at VHF, and the overall quality of reception was improved significantly if the frequency offsets were reduced from the few tens of Hz of the early schemes down to a few Hz as in the schemes most recently installed. The careful and accurate modulation matching that was necessary in FM schemes was much more easily achieved when the various transmitters were controlled by radio links rather than by land lines. Generally speaking, dedicated lines are not available, and it is relatively straightforward to match the modulation delay and modulation index over a radio link with adjustment needed only on rare occasions.

3. 6. Alternative Techniques

All base station transmitter use the same channel but are operated sequentially rather than simultaneously. However this apparently simple technique has several disadvantages, since the system operator will not be aware of the location of the mobiles, and a simple vehicle location scheme must therefore be incorporated into the system. This requires selective calling facilities which have been described earlier, and a

return path receiver "voting system", to be incorporated. When the operator in a system if this type wishes to initiate a call, each base station in turn transmits the appropriate selective call sequence for the required mobile. On receipt of its call sequence the mobile automatically re-transmits its own sequence (identity) and alerts the driver to the fact that a call is imminent. Each base station receiver that is within range of that particular mobile will then inform the central control point of the system of the strength or quality of the signal that has been received from the mobile, so that the optimum base station site can be selected for that particular mobile phone the receivers "vote" as to which is the best base station site. For calls initiated by the mobile. The driver will normally transmit his selective call sign before initiating a message, and the system will select the optimum base station site in the same manner as before.

This technique which is in common use by message handling organisations that need a selective calling system anyway, provides satisfactory performance in almost all circumstances. In several terms, complexity is its major disadvantage, and its success relies very largely on the skill of the fixed-station operators.

Finally, in UHF (Upper High Frequency:300-3000 MHz, 10Mbps) schemes it is possible to extend the range of coverage, or to fill in areas within the overall coverage area where reception is poor, by the use of "on-frequency" repeaters. These are essentially high-gain amplifiers which receive the signal on one antenna and then retransmit it in a different direction on another antenna. Clearly there are problems. Since any feedback around the system caused by pick-up between one antenna and the other are likely to cause oscillation, and an isolation of about 90 dB is commonly required. This can he achieved at UHF but is not possible at lower frequencies. Generally speaking, on-frequency repeaters are not favoured where other tecniques can be used.

3. 7. Cellular Schemes

The most sophisticated technique in current use for area coverage a cellular scheme. At this point we will merely identify the principle of frequency re-use by which a large area is covered. If a fixed number of radio channels are available for use in a given radio

phone system, they can be divided into a number of sets, each set being allocated for use in a given small area (a cell) served by a single base station. It is apparent that the greater the number or channels available in any cell, the more simultaneous phone calls that can he handled. But the smaller the total number of cells in a cluster that uses all the channels. For example, if the total number of channels is 56 than these can be split into 4 groups of 14 or 7 groups of 8, after which the frequencies have to be re-used. Some of the ways in which a fixed number of channels can be grouped to cover a given area are illustrated. Frequency re-use is a fundamental concept in cellular radio systems, but such systems need careful planning to avoid degradation by co-channel interference, i.e. interference with calls in one cell caused by a transmitter in another cell that uses the same set of frequencies.

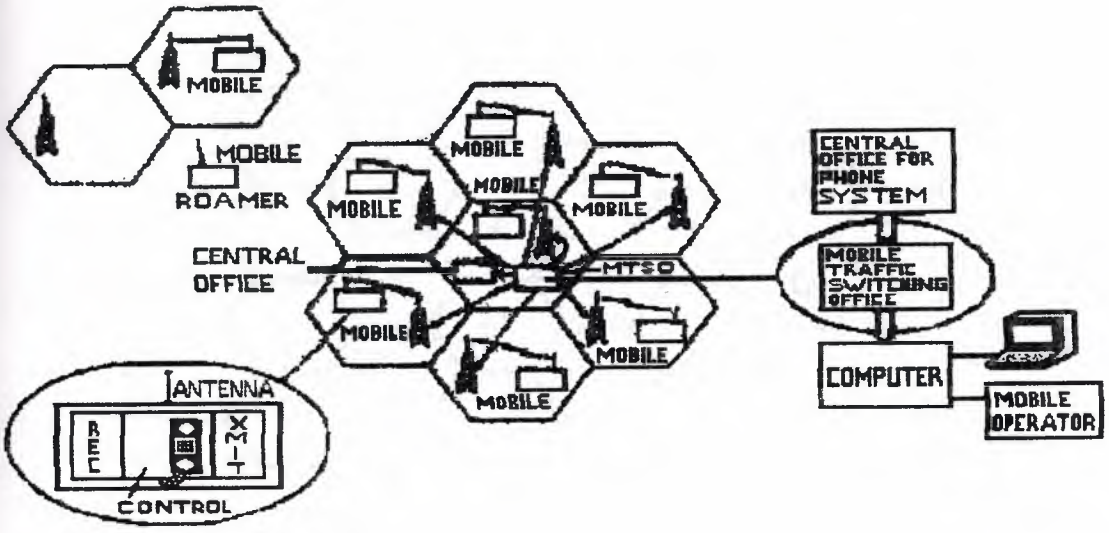


Figure 3.10 Typical cellular schemes

3. 8. Cellular Principles

The basic idea of the cellular concept is frequency reuse in which the same set of channels can be reused in different geographical locations sufficiently apart from each other so that channel interference be within tolerable limits. The set of channels available in the system is assigned to a group of cells constituting the cluster. Cells are assumed to have a regular hexagonal shape and the number of cells per cluster

determines the repeat pattern. Because of the hexagonal geometry only certain repeat patterns can tessellate. The number N of cells per cluster is given by: where i and j are integers. We note that the clusters can accommodate only certain numbers of cells such as 1, 3, 4, 7, 9, 12, 13, 16, 9, 21, . . , the most common being 4 and 7, The number of cells per cluster is intuitively related with system capacity as well as with transmission quality. The fewer cells per cluster, the larger the number of channels per cell (higher traffic carrying capacity) and the closer the cocells (potentially more cochannel interference). An important parameter of a cellular layout relating these entities is the D/R ratio, where D is the distance between cocells and R is the cell radius.

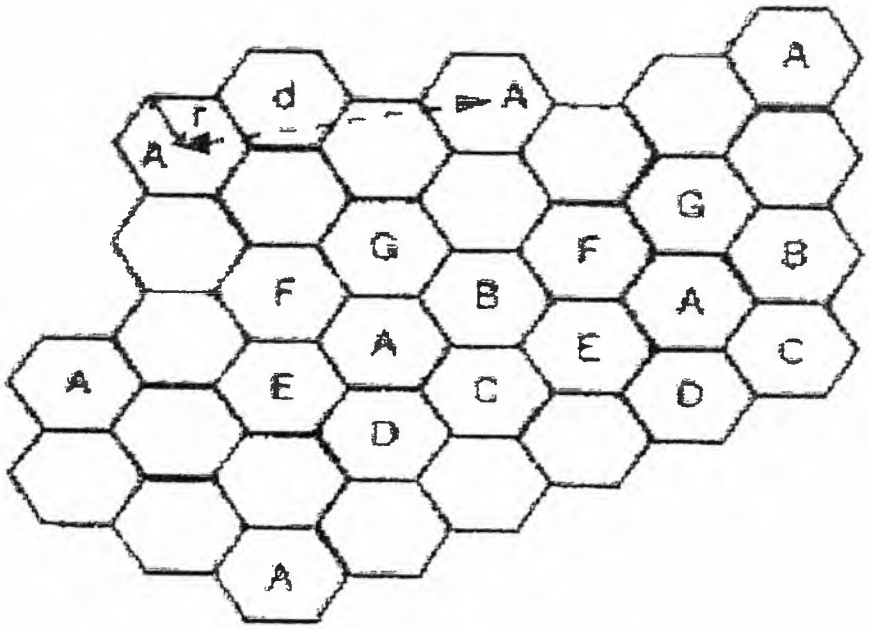


Figure 3.11 Frequency reuse pattern among cells

3.9 FDMA Cellular System

A frequency-division multiple access system can be used to provide high-quality mobile radiophone service. Known as AMPS (Advance Mobile Phone Service), the overall control of the system resides in a large central controller in each metropolitan service area.

This Mobile Telephone Switching Office (MTSO) in an electronic switching system programmed to provide call-processing and system fault detection and diagnostics.

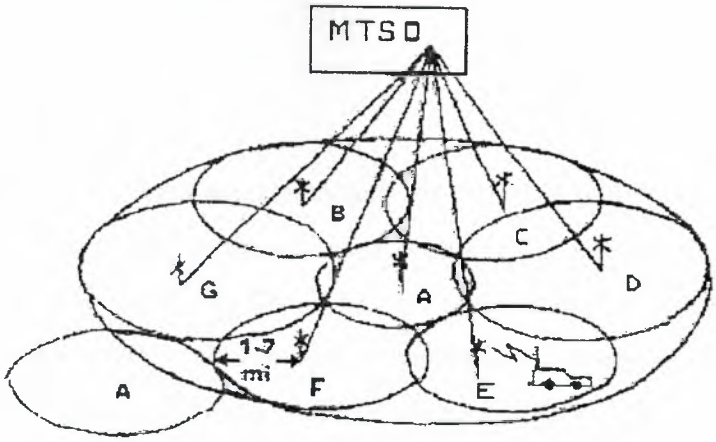


Figure 3.12 Mobile telephone switching office

3.9.1 Introduction

Designing a cellular network is a challenging task that invites engineers to exercise all of their knowledge in telecommunications. Although it may not be necessary to work as an expert in all of the fields, the interrelationship among the areas involved impels the designer to naturally search for a deeper understanding of the main phenomena.

In other words, the time for segregation, when radio engineers and traffic engineers would not talk to each other, at least through a common vocabulary, is probably gone. A great many aspects must be considered in a cellular network planning. The main ones include the following.

- Radio Propagation: Here the topography and the morphology of the terrain, the urbanisation factor and the clutter factor of the city, and some other aspects of the target geographical region under investigation will constitute the input data for the radio coverage design.

• Frequency Regulation and Planning: In most countries there is a centralist organisation, usually performed by a government entity, regulating the assignment and use of the radio spectrum. The frequency planning within the assigned spectrum should then be made so that interferences are minimised and the traffic demand is satisfied.

3.9.2 Modulation

As far as analog systems are concerned, the narrow band FM is widely used due to its remarkable performance in the presence of fading. The North American Digital Cellular Standard IS-54 proposes the n/4 differential quadrature phase-shift keying (n/4 DQPSK) modulation, whereas the Global System for Mobile Communications (GSM) establishes the use of the Gaussian Minimum-Shift Keying (GMSK).

3.9.3 Antenna Design

To cover targe areas and for low-traffic applications omnidirectional antennas are recommended. Some systems at their inception may have these characteristics, and the utilisation of omnidirectional antennas certainly keeps the initial investment low. As the traffic demand increases, the use of some sort of capacity enhancement technique to meet the demand, such as replacing the omnidirectional by directional antennas is mandatory.

3.9.4 Transmission Planning

The structure of the channels, both for signalling and voice, is one of the aspects to be considered in this topic. Other aspects include the performance of the transmission components (power capacity, noise, bandwidth, stability etc.) and the design or specification of transmitter and receivers.

3.9.5 Switching Exchange

In most cases this consists of adapting the existing switching network for mobile radio communication purposes.

3.9.6 Telegraphic

For a given grade of service and number of channels available, how many subscribers can be accommodated into the system? What is the proportion of voice and signalling channels?

3.9.7 Software Design

With the use of microprocessors throughout the system there are software applications in the mobile unit, in the base station, and in the switching exchange. Other aspects, such as human factors, economics, etc., will also in since the design. This chapter outlines the aspects involving the basic design steps in cellular network planning. Topics, such as traffic engineering, cell coverage, and interference will be covered, and application examples will be given throughout the section so as to illustrate the main ideas. We start by recalling the basic concepts including cellular principles, performance measures and system requirements, and system expansion techniques.

3. 10. The GSM system-narrow band TDMA

GSM of CEPT were clearly faced with a difficult choice, perceiving features of merit in all the systems offered. The advantages of TDMA as far as base station design is concerned are evident in permitting many channels to be supported by a single base station transceiver, but the number of channels per carrier, and consequently the bit rate, should not be too high to create difficulties for mobiles in having time to scan a number of base station transmissions to determine hand-off requirements. Additionally, the number of channels per carrier should not be too high if peak power output requirements from hand-portables are to be met and the equaliser complexity/ performance compromise within reach of short to medium term DSP.

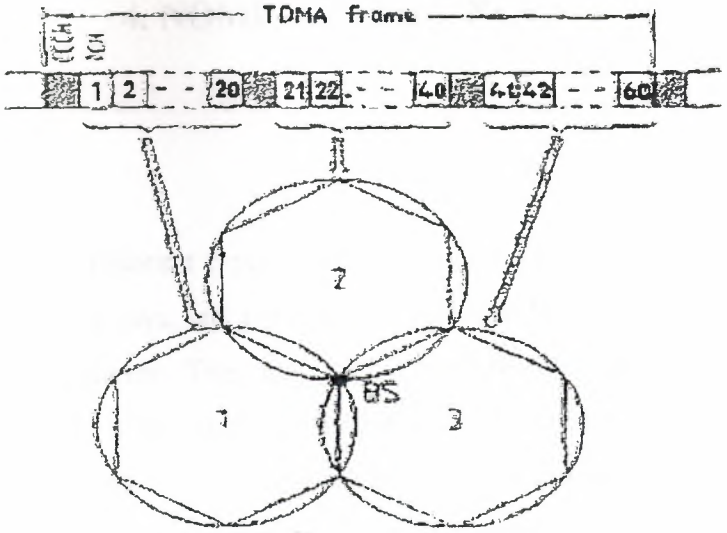


Figure 3.13 CD 100 frequency re-use strategy.

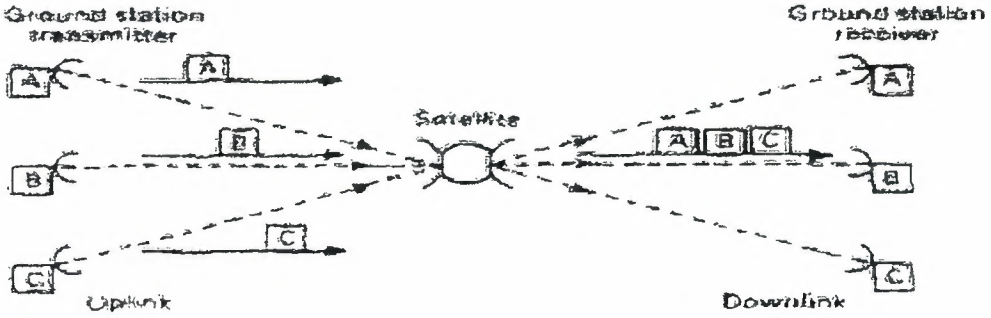


Figure 3.14 Basic TDMA operation.

4. NOMINAL CELL PLAN

4. 1. Waves

There are many seemingly different types of electromagnetic waves. They include radio waves, infrared rays, light, x-rays, and gamma rays among others. Radio waves are one type of electromagnetic radiation. They are typically generated as disturbances sent out by oscillating charges on a transmitting antenna. Other types of electromagnetic radiation are caused by intense heat, atomic reactions, and stimulated emission (lasers). Regardless of its origin, an electromagnetic wave is comprised of oscillating electric and magnetic fields. For a simple, traveling, plane wave, the electric and magnetic fields are perpendicular to each other and also to the direction of propagation. Waves can be described by simple sinusoidat functions (Figure 4.1) and are conveniently characterized by their wavelength, λ (the length of one cycle of oscillation), or equivalently with its frequency, f. The two are related via the speed of propagation, c, as

$$\lambda \times f = c$$

where:

λ = wavelength in meters per cycle

f = frequency in cycles per second (or hertz)

c = speed of light, a constant approximately equal to $3 \cdot 10^8$ meters/second for all electromagnetic waves.

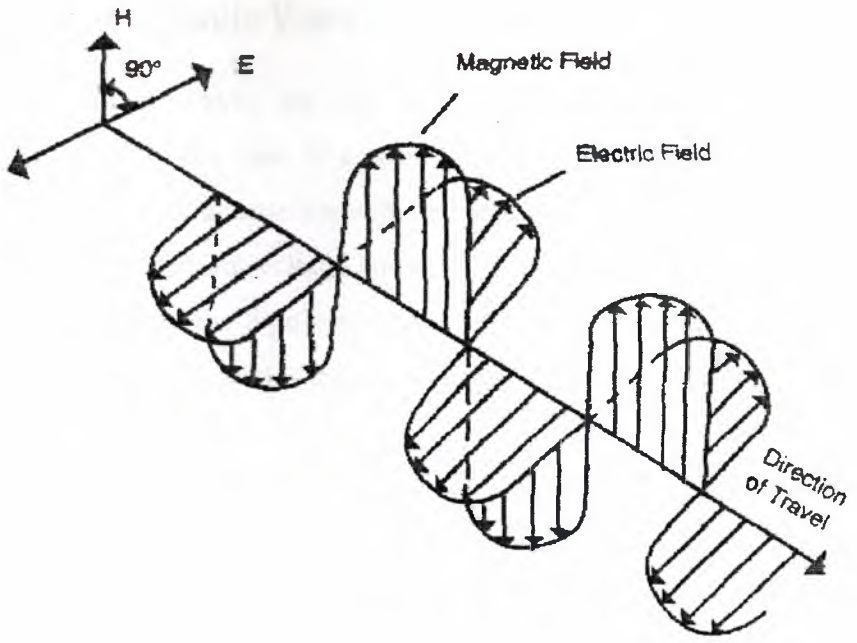


Figure 4.1 An electromagnetic plane wave "frozen" in time

Propagation properties are different across the frequency spectrum. Radio waves fall in the frequency spectrum between 3 Hz and 3000 GHz. This pan of the spectrum is divided into twelve bands (Table 4.1). Only the Ultra High Frequency (UHF) band is considered from now on, since properties of UHF waves and frequency allocations liave made this the mobile telephony frequency band.

Table 4.1 Frequency spectrum bands

FREQUENCY	CLASSIFICATION	DESIGNATION
3 - 30 Hz		
30 - 300 Hz	Extremely Low Frequency	ELF
300 - 3000 Hz	Voice Frequency	VF
3 - 30 kHz	Very-Low Frequency	VLF
30 - 300 kHz	Low Frequency	LF
300 - 3000 kHz	Medium Frequency	MF
3 - 30 MHz	High Frequency	HF
30 - 300 MHz	Very High Frequency	VHP
300 - 3000 MHz	Ultra High Frequency	UHF
3 - 30 GHz	Super High Frequency	SHF
30 - 300 GHz	Extremely High Frequency	EHF
300 - 3000 GHz		

4. 2. Generation of Radio Waves

High frequency radio waves are typically generated by oscillating charges on a transmitting antenna. In the case of a radio station, the antenna is often simply a long wire (a dipole) fed by an alternating voltage/current source; i.e., charges are placed on the antenna by the alternating voltage source. We can think of the electric field as being disturbances sent out by the dipole source and the frequency of the oscillating electric field (the electromagnetic wave) is the same as the frequency of the source.

Each antenna has a unique radiation pattern. This pattern can be represented graphically by plotting the received, time-averaged power, as a function of angle with respect to the direction of maximum power in a log-polar diagram. The pattern is representative of the antenna's performance in a test environment. However, it only applies to the free-space environment in which the test measurement takes place. Upon installation, the pattern becomes more complex due to factors affecting propagation in the reality. Thus, the real effectiveness of any antenna is measured in the field.

An isotropic antenna is a completely non-directional antenna that radiates equally in all directions. Since all practical antennas exhibit some degree of directivity, the isotropic antenna exists only as a mathematical concept. The isotropic antenna can be used as a reference to specify the gain of a practical antenna (see the appendix for a general discussion on gain/loss and logarithmic units). The gain of an antenna referenced isotropically is the ratio between the power required in the practical antenna and the power required in an isotropic antenna to achieve the same field strength in the desired direction of the measured practical antenna. Directive gain in relation to an isotropic antenna is expressed in units of "dBi".

A half-wave dipole antenna may also be used as a gain reference for practical antennas. The half-wave dipole is a straight conductor cut to one-half of the electrical wavelength with the radio frequency signal fed to the middle of the conductor. Figure 4.2 illustrates the radiation pattern of the half-wave dipole which normally is referred to as a dipole. Whereas the isotropic antenna's three dimensional radiation pattern is spherical, the dipole antenna's three dimensional pattern is shaped like a donut.

Directive gain in relation to a dipole is expressed in units of "dBd". For a dipole and an isotropic antenna with the same input power, the energy is more concentrated in certain directions by the dipole. The difference in directive gain between the dipole and the isotropic antenna is 2.15 dB. Figure 4.3 illustrates the differences in gain between the isotropic, dipole and practical antenna. The vertical pattern (Figure 4.3) for the practical antenna is that of a directional antenna.

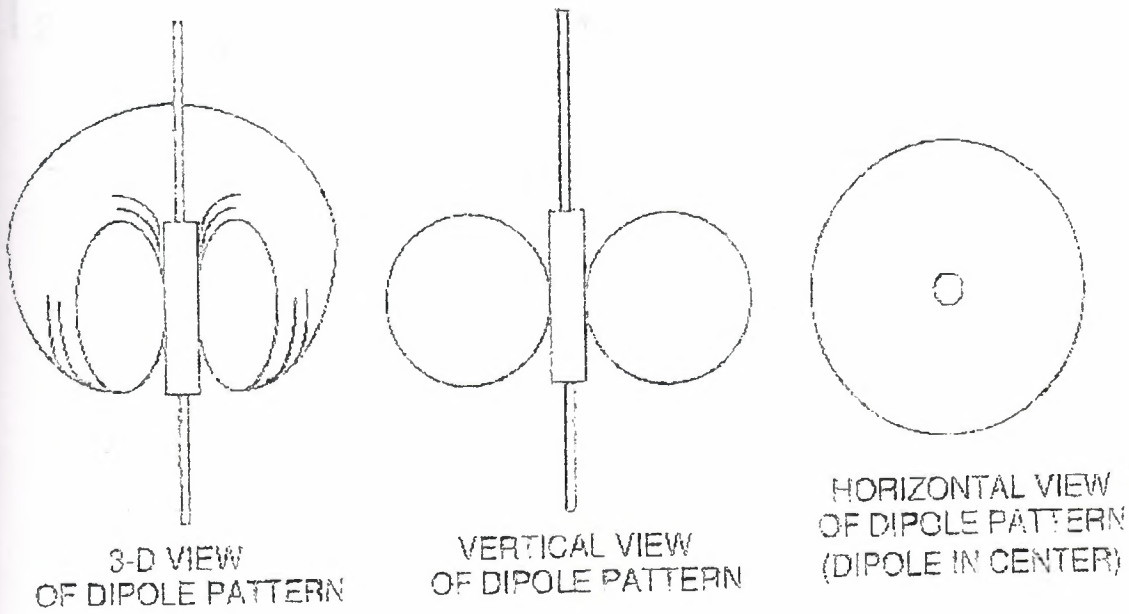


Figure 4.2 Dipole radiation pattern

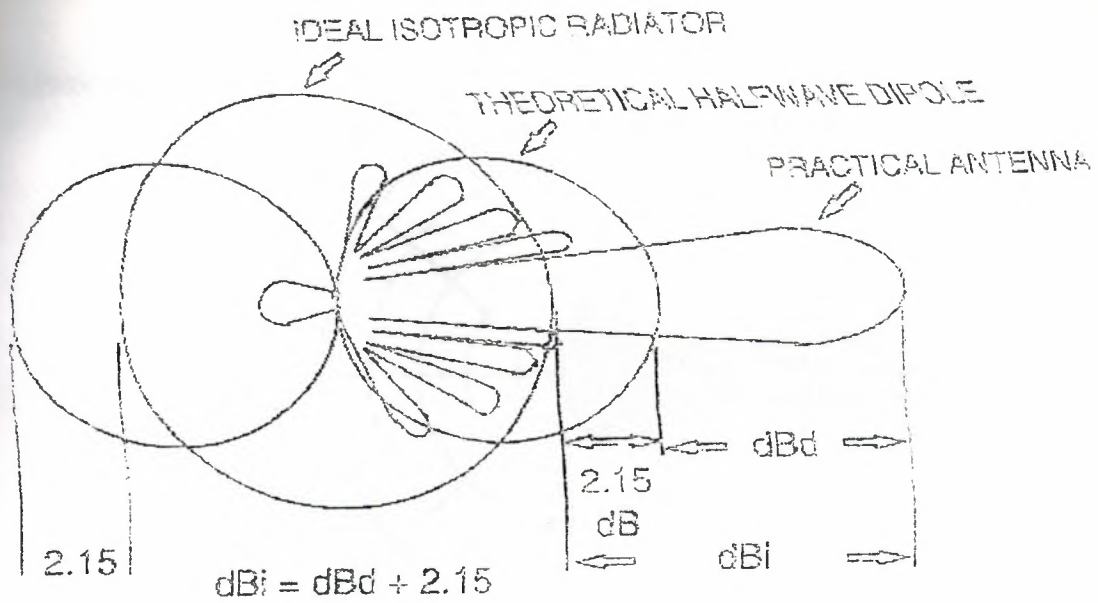


Figure 4.3 Gain comparison

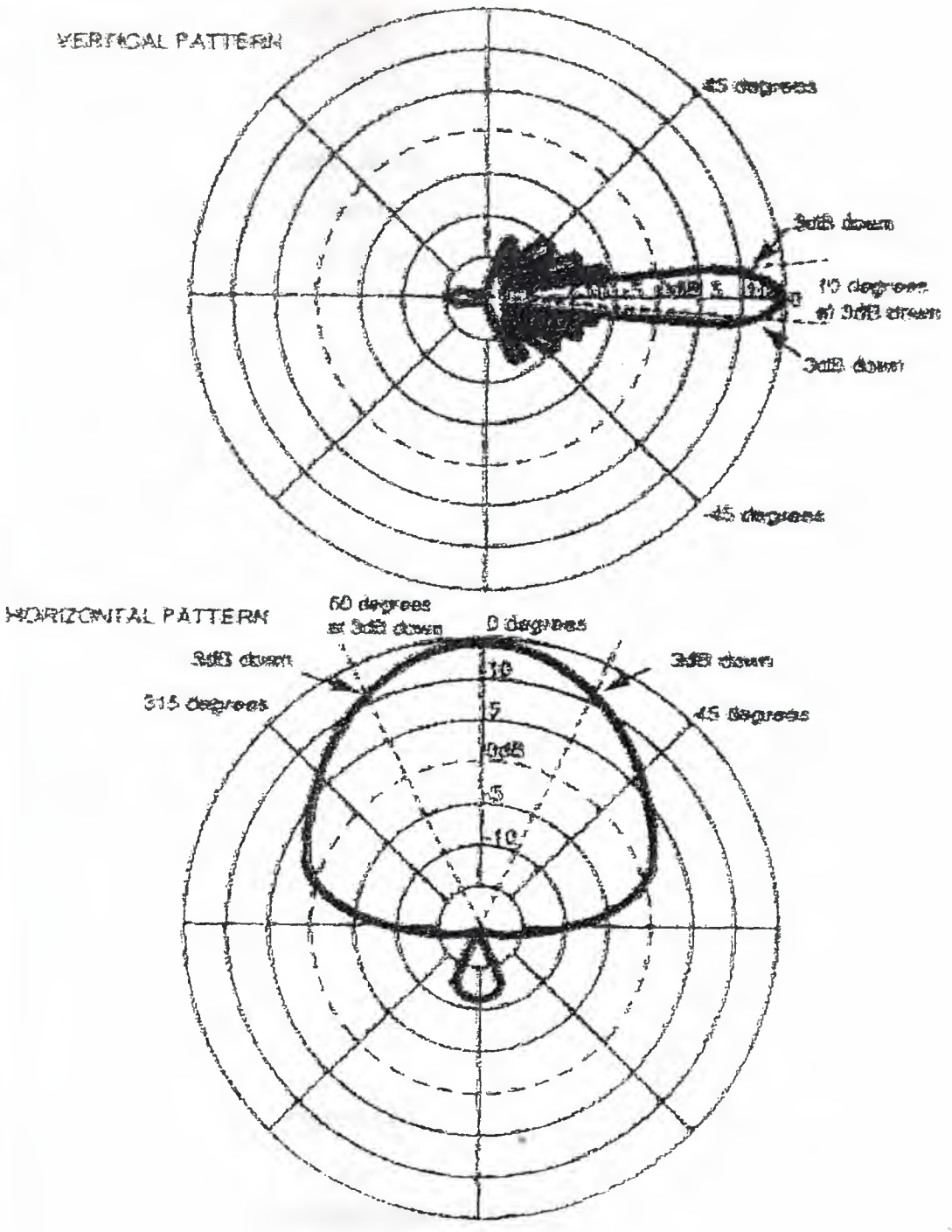


Figure 4.4 Vertical and horizontal antenna patterns for a "real" antenna

When choosing an antenna for a specific application, the manufacturer's data sheet must be consulted. The data sheet contains information including antenna gain, beamwidth (vertical and horizontal), and graphs showing the vertical and horizontal patterns. Examples of the graphs normally found in a data sheet are shown in Figure 4.4, The

patterns displayed are those of a directional antenna. The antenna's gain is approximately 15 dBd.

The beamwidth, B, is defined as the opening angle between the points where the radiated power is 3 dB lower than in the main direction (Figure 4.5). Both the horizontal and vertical beamwidths are found using the 3 dB down points, alternatively referred to as half-power points.

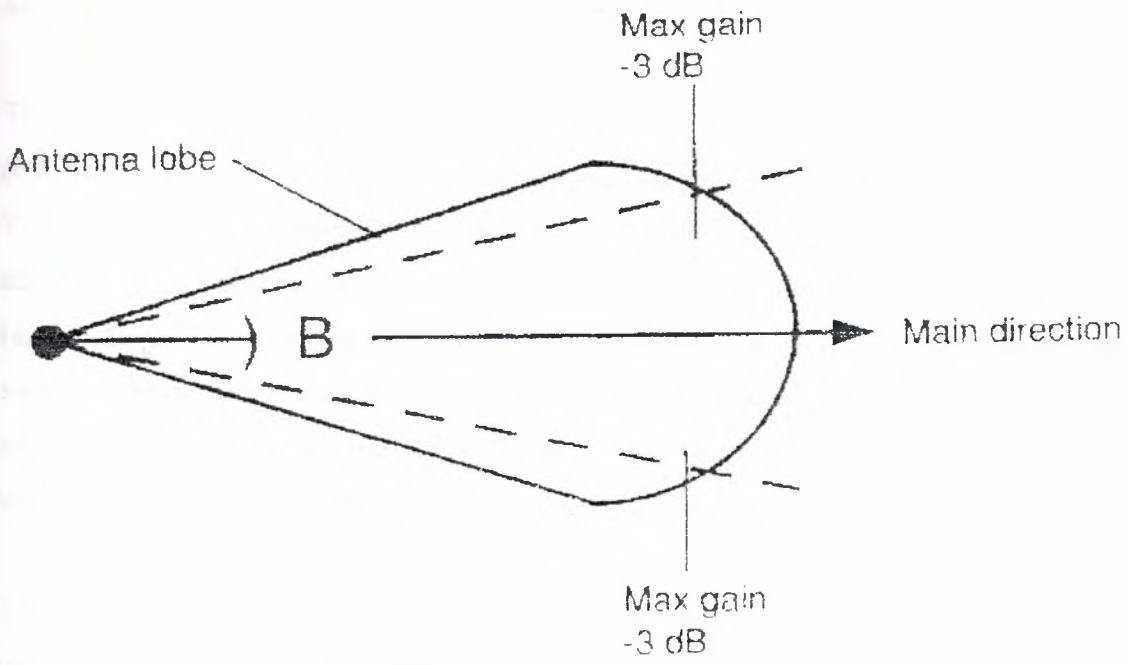


Figure 4.5 Definition of beamwidth

4. 3. Superimposing Information on Radio Waves

Information is seldomly transmitted in the same frequency range as it was generated. The reason is that if, as an example, we want to broadcast a 2 kHz signal, the antenna would liave to be 75 km long (half a wavelength). However, by translating the signal to a much higher frequency band (e.g., the UHF band of cellular telephony) antenna sizes drop to a few decimeters. In addition, in order to have numerous "channels" simultaneously, a higher frequency is required.

Frequency translation is implemented by modulating the amplitude, frequency or phase of a so-called carrier wave in accordance with the wave form of the wanted signal. Several modulation schemes exist (e.g.amplitude modulation) common for analog radio signals and phase modulation. Any modulation scheme increases the carrier bandwidth and hence limits the capacity of the frequency band available. Since the bandwidth of the carrier increases if the bit rate increases, a high carrier frequency is necessary to obtain many different "channels". The cell planner cannot choose modulation techniques, but the consequences of the system choice are very important, since carrier bandwidth and carrier separation affects, e.g., interference properties. Wave propagation also behaves differently in different frequency bands.

The modulation technique used in GSM is called Gaussian Minimum Shift Keying (GMSK). This narrow-band digital modulation technique is based on phase shifting. That is, bits are represented by continuous positive or negative phase shifts. By changing the phase continuously, sharp discontinuities are avoided, thus narrowing the bandwidth of the modulated carrier. GMSK modulation also involves filtering the incotning bit stream with a Gaussian filter to obtain a more narrow bandwidth of the modulated carrier. In fact the full width at half maximum of the carrier becomes 162 kHz, corresponding nicely to the 200 kHz carrier separation.

Transmitting the information on the air interface in digitized form has an advantage over analog techniques, since channel coding protects bits, the signal is less sensitive to perturbations. In addition, it enables Time Division Multiple Access (TDMA) which means that one carrier frequency can be used for several connections. Each connection uses only one particular time slot (out of the eight available in GSM). This has the advantage that the mobile is released from transmitting/receiving continuously and can perform, e.g., measurements on neighboring cells. One main advantage with TDMA is that it enables Mobile Assisted Hand Over (MAHO) which is essential for effective connection control.

4. 4. Air Interface Data

Below is a summary of some important air interface data for GSM 900, GSM 1800, and GSM 1900.

4.4.1 Frequency Spectrum

Different frequency bands are used for GSM 900, GSM 1800, and GSM 1900 (refer to Figure 4.10). In some countries, operators apply for the available frequencies. In other countries e.g., the United Stales), operators purchase frequency bands at auctions.

In December of 1994, the Federal Communications Commission (FCC) auctioned "broadband" licenses to prospective operators offering personal communications services. Each operator owns the rights to the licenses for a period of ten years. The United States is divided into 51 regions or Major Trading Areas (MTA) and 493 Basic Trading Areas (BTA). The FCC issued two GSM 1900 licenses for each MTA and four for each BTA. One MTA can be geographically as large as a state, while one BTA can be compared in size to a large city. BTAs are designed for use in major metropolitan areas.

The FCC has specified the frequency range and output power. The frequency band is divided into six frequency blocks (Figure 4.6): three duplex blocks A, B, and C (90 MHz total spectrum bandwidth) and three other duplex blocks D, E, and F (30 MHz total spectrum bandwidth).

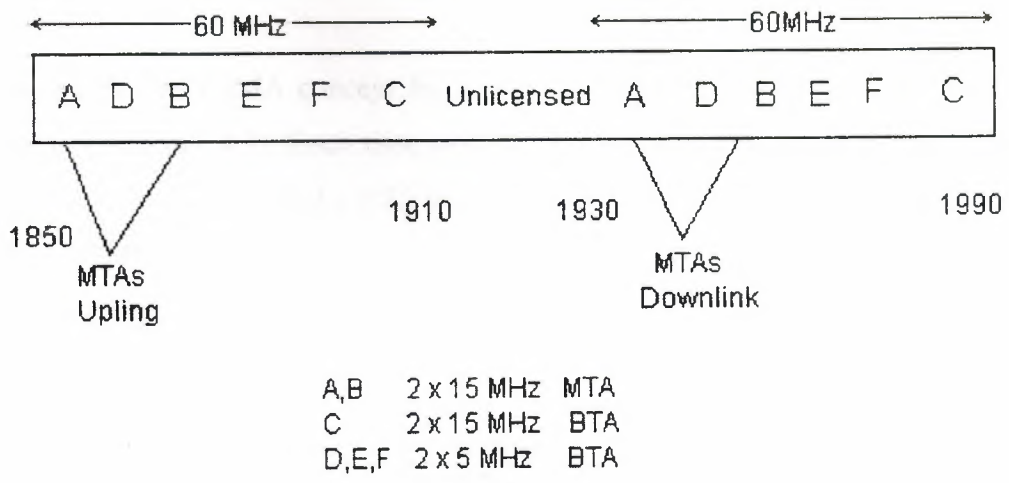


Figure 4.6 Spectrum allocation for GSM 1900 in United States. 140 MHz tor GSM 1900 (120 MHz licensed and 20 MHz unlicensed)

4.4.2 Duplex Distance

The distance between the uplink and downlink frequencies is known as duplex distance. The duplex distance is different for the different frequency bands (Table 4.2)

Table 4.2 Duplex differences for different frequency bands

Standard	GSM 900	GSM1800	GSM1900
Duplex dist.	45MHz	95MHz	80MHz

4.4.3 Channel Separation

The distance between adjacent frequencies on the uplink or the downlink is called channel separation. The channel separation is 200 kHz, regardless of the standard chosen from the ones mentioned above. This separation is needed to reduce interference from one carrier to another neighboring frequency.

4.4.4 Access Method and Transmission Rate

GSM has chosen the TDMA concept for access. In GSM, there are eight TDMA time slots per frame (Figure 4.7). Each time slot is 0.577 ms long and has room for 156.25 bits (148 bits of information and a 8.25 bits long guard period) yielding a bit rate on the air interface of 270.8 kbits.

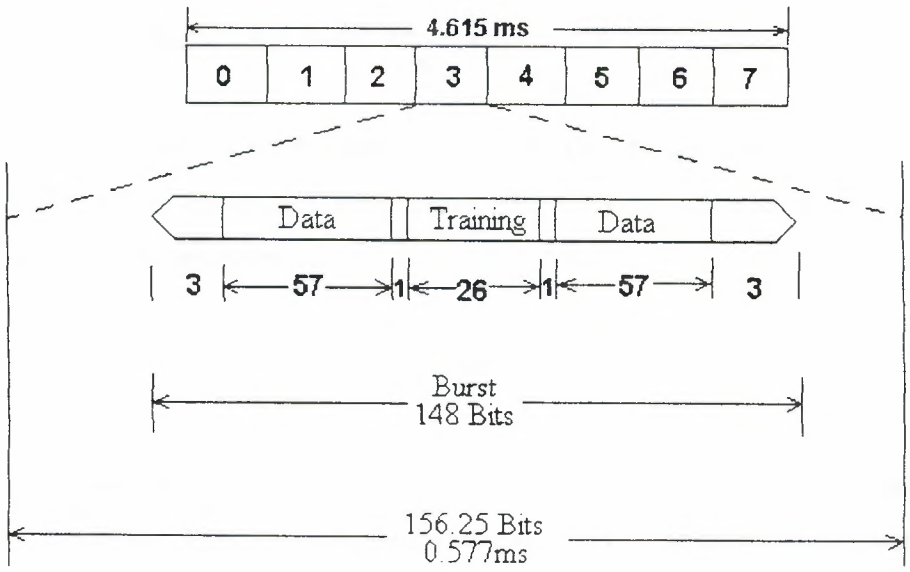


Figure 4.7 Basic TDMA frame, timeslot, and burst structures

4. 5. Radio Wave Propagation

In this project we arc primarily interested in the transmission loss between two antennas: the transmitter/emitter and the receiver. Many factors including absorption, refraction, reflection, diffraction, and scattering affect the wave propagation. However, in free space an electromagnetic wave travels indefinitely if unimpeded. This does not mean that there are no transmission losses, as we will see in this first simple model where isotropic emission from the transmitter and line of sight between the two antennas separated by a distance, d, in free space are assumed (Figure 4.8).

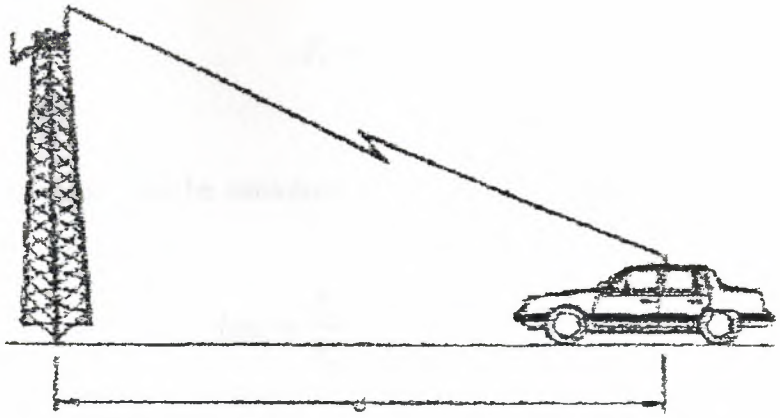


Figure 4.8 Radio wave propagation in free space

Since an isotropic antenna by definition distributes the emitted power, Pt, equally in all directions, the power density, Sr, (power per area unit) decreases as the irradiated area, $4\pi d^2$, at distance d, increases, i.e.:

$$S_r = \frac{P_t}{4\pi d^2}$$

If the transmitting antenna has a gain, G_t, it means that it is concentrating the radiation towards the receiver. The power density at the receiving antenna increases with a factor proportional to G_t, i.e.

$$S_r = \frac{P_t G_t}{4\pi d^2}$$

The power received by the receiving antenna, Pr, is proportional to the effective area, Ar, of that antenna, i.e.

$$P_r = S_r \cdot A_r$$

It can be shown that the effective area of an antenna is proportional to the antenna gain, *Gr*, and the square of the wavelength, lamda, of the radio wave involved, i.e.

$$A_r = \frac{G_r \lambda^2}{4\pi}$$

and hence the received power becomes

$$P_r = \frac{P_t G_t G_r \lambda^2}{(4\pi d)^2}$$

The transmission loss can be calculated as the ratio between the transmitted power and received power, i.e.

$$loss = \frac{P_t}{P_r} = \frac{(4\pi d)^2}{G_t G_r \lambda^2}$$

Note that the wavelength dependency of the pathless does not correspond to losses in free space as such. It is a consequence of the finite effective receiver area.

This expression is fairly general. The only thing which changes when we improve our models is the expression for the pathloss. The antenna gain is normally given in dB(i), i.e., as 10 log(G), where gain means a reduction of the total transmission loss, L, between a transmitting and receiving antenna.

This model helps us to understand the most important features of radio wave propagation. That is, the received power decreases when the distance between the antennas increases and the transmission loss increases when the wavelength decreases (or alternatively when the frequency increases).

For cell planning, it is very important to be able to estimate the signal strengths in all parts of the area to be covered, i.e. to predict the pathless. The model described in this section can be used as a first approximation. However, more complicated models exist. Improvements can be made by accounting for:

- The fact that radio waves are reflected towards the earth's surface (the conductivity of the earth is thus an important parameter)
- Transmission losses due to obstructions in the line of sight
- The finite radius of the curvature of the earth

The topographical variations in a real case as well as the different attenuation properties of different terrain types such as forests, urban areas, etc.

The best models used are semi-empirical, i.e., based on measurements of pathloss/attenuation in various terrains. The use of such models are motivated by the fact that radio propagation can not be measured everywhere. However, if measurements are taken in typical environments, the parameters of the model can be fine-tuned so that the model is as good as possible for that particular type of terrain.

4. 6. Signal Variations

The models described in the previous section can be used to estimate the average signal level (called the "global mean") at the receiving antenna. However, a radio signal envelope is composed of a fast fading signal super-imposed on a slow fading signal (Table 4.2). These fading signals are The result of obstructions and reflections. They yield a signal which is the sum of a possibly weak, direct, line-of-sight signal and several indirect or reflected signals.

The fast fading signal (peak-to-peak distance = $\lambda/2$) is usually present during radio communication due to the fact that the mobile antenna is lower than the surrounding structures such as trees and buildings. These act as reflectors. The resulting signal consists of several waves with various amplitudes and phases. Sometimes these almost completely cancel out each other, This can lead to a signal level below the receiver sensitivity. In open fields where a direct wave is dominating, this type of fading is less noticeable.

Short-term fading is Rayleigh distributed with respect to the signal voltage. Therefore, it is often called Rayleigh fading. This type of fading affects the signal quality, and as a result some measures must be taken to counter it.

The first and most simple solution is to use more power at the transmitters(s), thus providing a fading margin. Another way to reduce the harm done by Rayleigh fading is to use space diversity, which reduces the number of deep fading dips. Diversity means that two signals are received which have slightly different "histories" and, therefore, the "best" can be used.

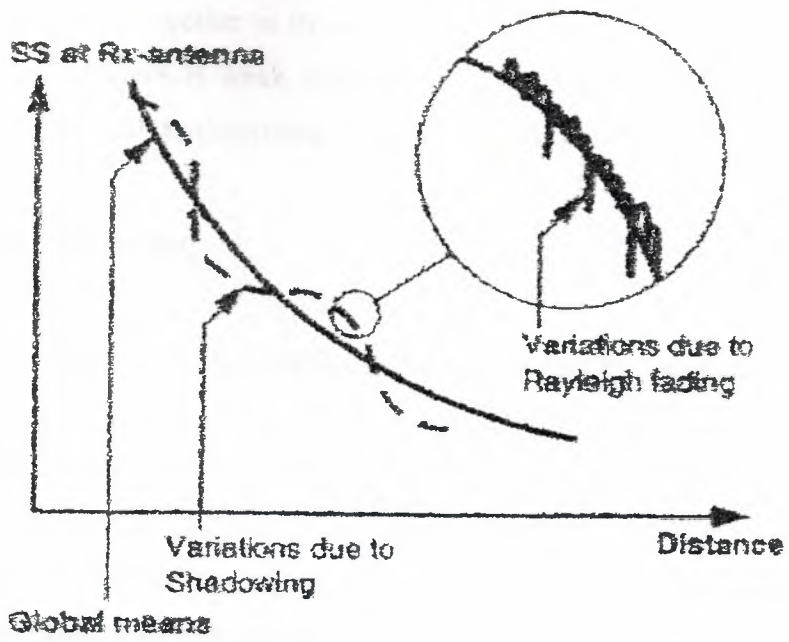


Figure 4.9 Short-term (fast) and long-term (slow) fading

The signal variation received if we smooth out the short-term fading is called the "local mean". Its power is often called the local average power, is expressed in a logarithmic scale, and is normally distributed. Therefore, this slow fading is called "log-normal fading". If we drive through a flat desert without any obstructions, the signal varies slowly with distance. However, in normal cases the signal path is obstructed.

Obstructions near the mobile (e.g., buildings, bridges, trees, etc,) cause a rapid change of the local mean (in the range of five to fifty meters), while topographical obstructions cause a slower signal variation. Because log-normal fading reduces the average strength received, the total coverage from the transmitter is reduced. To combat this, a fading margin must be used. Problems generated by multi-path reflections are made more severe by tog-normal fading since the direct beam is weakened by the obstructing object.

Phases between various reflected waves are different. This is due to the fact that they propagate over different distances or equivalently use different times to reach the receiver. This time dispersion can cause particular problems if the phase difference between the reflected waves is very large. For GSM 900, a large phase difference is on

the order of several thousands of wavelengths (i.e. one kilometer or more). In this case, different waves added together in the receiver carry information about different symbols (bits). If the direct wave is weak, and consequently the reflected waves are relatively strong, it can be difficult to determine which symbol (bit) was transmitted.

4. 7. System Balancing

An area is referred to as being covered if the signal strength received by an MS in that area is higher than some minimum value. A typical value in this case is around -90 dBm (1 pW). However, coverage in a two-way radio communication system is determined by the weakest transmission direction. Both uplink and downlink are taken into consideration here. That is, the signal received by the BTS from an MS in an area must be higher than some minimum value. It makes no sense to have different coverage on uplink and downlink because (his causes an excess amount of energy to be dissipated into the system adding extra interferences and costs. A system balance must be obtained before coverage calculation can start.

To achieve this balance it is necessary to make sure that the sensitivity limit, MS_{sens} of the MS (fur downlink transmission) is reached at the same point as the sensitivity limit, BTS_{sens}, of the BTS (for uplink transmission).

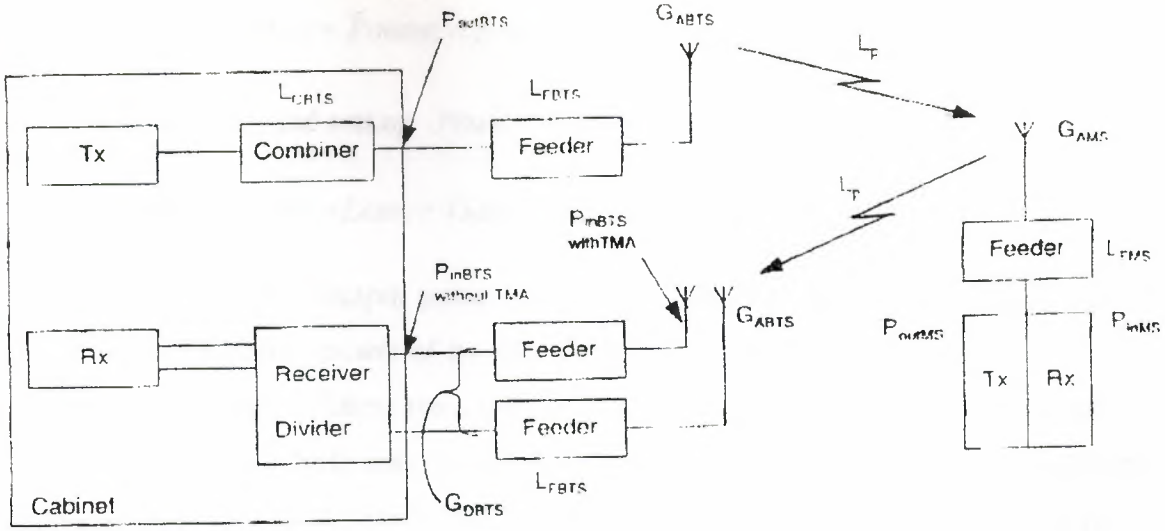


Figure 4.10 Schematic graph of the compionents included in a system balance.

Abbreviations have the following translations:

G=Gain, L=Loss, A=Antenna, F=Feeder, C-=Combiner, MS=Mobile Station, BTS=Base Transceiver Station, D=Diversity, Pin=inpul power, Pout=output power, and Lp=path loss

The input power, PinMS, at the MS receiver equals the output power, PoutBTS, of the BTS plus gains and losses.

$$Pin_{MS} = Pout_{BTS} - Lc_{BTS} - Lf_{BTS} + Ga_{BTS} - Lp + Ga_{MS} - Lf_{MS}$$

and

$$Pin_{BTS} = Pout_{MS} - Lf_{MS} + Ga_{MS} - Lp + Ga_{BTS} + Gd_{BTS} - Lf_{BTS}$$

For some configurations the duplex loss, $Ldupl_{BTS}$, can be important. If polarization diversity is used it may be necessary to introduce a slant polarization (±45°) downlink loss, $Lslant_{BTS}$. Assuming that the pathless, Lp, is identical on uplink and downlink (a good assumption since the difference in frequency is only on the order of 5%) and that the transmitting and receiving antennas of the BTS have the same gain, subtracting the second equation from the first

$Pin_{MS} - Pin_{BTS} = Pout_{BTS} - Pout_{MS} - L_{CBTS} - Gd_{BTS}$

is obtained, and setting $Pin_{MS} - Pout_{BTS} = MS_{SENS} - BTS_{SENS}$

$Pout_{BTS} = Pout + L_{CBTS} + Gd_{BTS} + (MS_{SENS} - BTS_{SENS})$

is obtained. The BTS output power, POUT BTS, measured at the RX output' must be higher than the output power of the MS, $Pout_{BTS}$, by a value corresponding to the sum of the diversity gain, Gd_{BTS}, the combiner loss, L_{CBTS}, and the difference in sensitivity $(MS_{SENS} - BTS_{SENS})$. Note that the reference points for the sensitivities may be different when balancing, e.g. a GSM 1800 system using an Antenna Low Noise Amplifier (ALNA).

For example, balancing the system for GSM 900 class 4 mobile stations, i.e. $Pout_{MS}$ =2 W or 33 dBm, using Gd_{BTS} = 3.5 dB, L_{CBTS} = 3 dB, and using values for the sensitivities as MS_{SENS} = -104 dBm and BTS_{SENS} = -110 dBm, an output power of the BTS

$Pout_{BTS} = 33 + 3 + 3.5 + (-104 + 110) = 45.5$ dBm

is obtained. Hence, an 35 W BTS is needed. The output power of the BTS needs to be higher than the output power of the MS because not only is the BTS more sensitive (and hence can accept a smaller signal strength) it has also an extra loss when transmitting, LCBTS and an extra gain when receiving, Gd_{BTS}. Note that the balance is independent of the BTS antenna gain

However, the coverage can now be changed by changing the antenna gain, since it is symmetrical, i.e. increasing the coverage downlink by increasing ihe antenna gain is matched by a corresponding increase in coverage on the uplink.

The BTS output power should never be changed once the system is balanced for a particular configuration and mobile class. Note: If "smaller cells" are desired, the power can be decreased because it can be matched by a corresponding, forced, decrease in the output power of the MS.

4. 8. Channel Loading Plan

The simplest cell planning problem solution is to have one cell and use all available carriers in that cell (Figure 4.11). However, such a solulion has severe limitations. It is seldom that coverage can be maintained in the entire area desired. In addition, even though the channel utilization may be very high. limited capacity soon becomes a problem due to the limited number of carriers available to any operator.

A cellular system is based upon re-use of the same set of frequencies which is obtained by dividing the area needing coverage into smaller areas (cells) which togelher form clusters (Figure 4.12). A cluster is a group of cells in which all available carriers have been used once (and only once). Since the same carriers are used in cells in neighboring clusters, interference may become a problem. Indeed, the frequency re-use distance, i.e. the distance belween two sites using the same carrier, must be kept as large as possible from a interference point-of-view. At the same time they must be kept as small as possible from a capacity point of view.

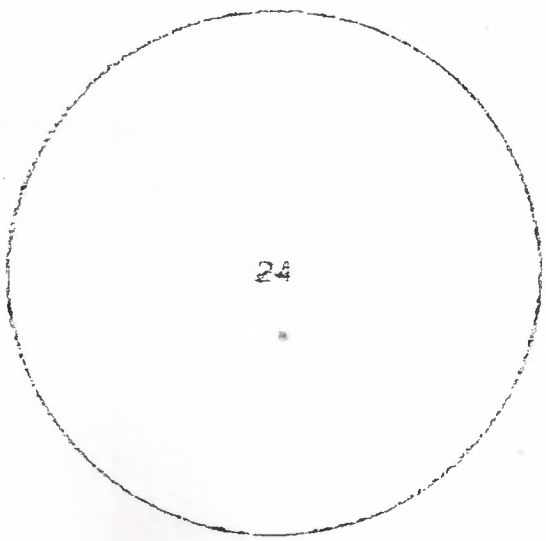


Figure 4.11 Example of an area served from one cell by 24 carriers

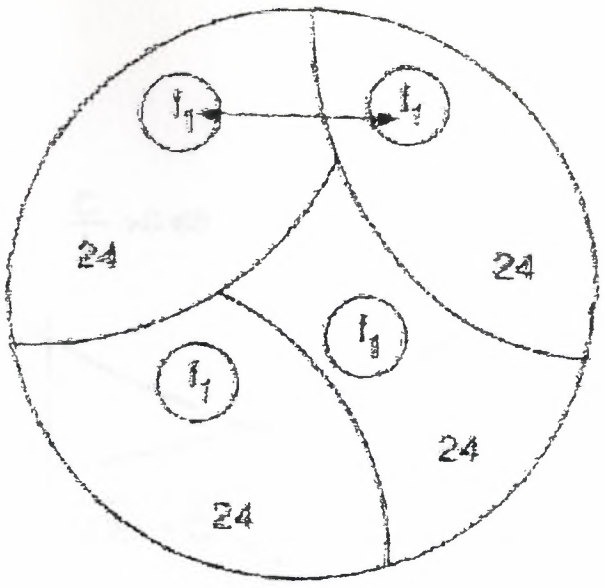


Figure 4.12 The same area as in Table 4.1 but now schematically divided into four clusters, each cluster using all (here 24) carriers. The small circles indicate individual cells where the frequency f_1 is used and a distance between the corresponding sites, known as frequency re-use distance, is indicated by the double arrow.

4.8.1 Interference

Cellular systems are often interference limited rather than signal strength limited. Therefore some elementary information about different problems associated with the re-use of carriers is provided in this section.

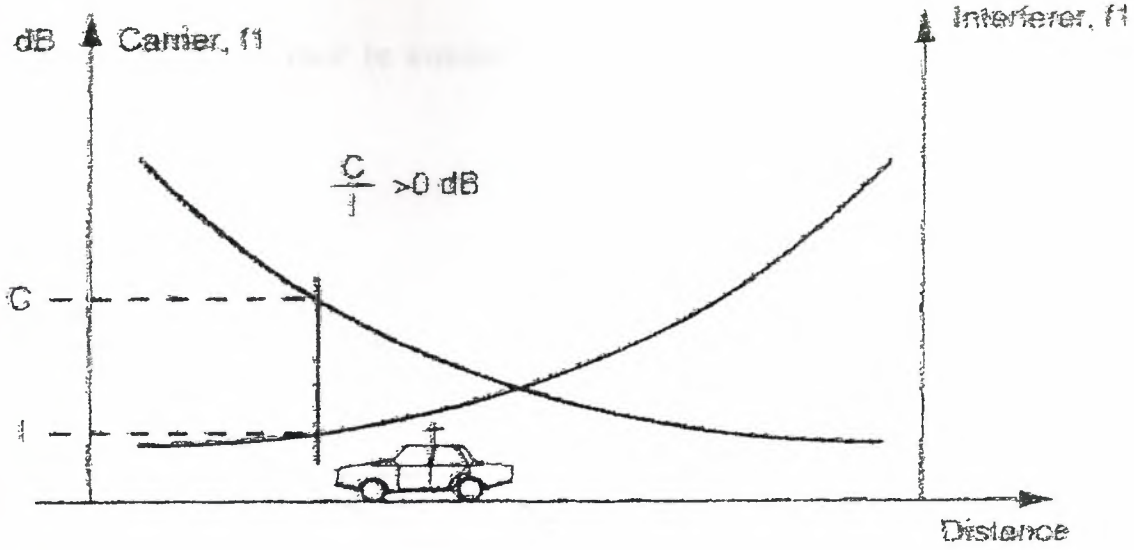


Figure 4.13 Co-channel interference

Co-channel interference is the term used for inlerference in a cell by carriers with the same frequency present in other cells. Figure 4.13 illustrates the situation. Since the same carrier frequency is used for the wanted carrier as for the unwanted carrier, quality problems can arise if the signal from the unwanted carrier is too strong.

The GSM specification states that the signal strength ratio, C/I, between the carrier, C, and the interferer, I, must he larger than 9 dB. If frequency hopping is implemented, it adds extra diversity to the system corresponding to a margin of approximately 3 dB, i.e.:

C/I > 12 dB (without frequency hopping)

C/I > 9 dB (with frequency hopping)

Adjacent carrier frequencies (i.e., frequencies shifted ±200 kHz) with respect to the carrier cannot be allowed to have too strong a signal strength either. Even though they are at different frequencies, part of the signal can interfere with the wanted carrier's signal and cause quality problems (Figure 4.4). The GSM specification states that the signal strength ratio, C/A, between the carrier and the adjacent frequency interferer, A, must be larger than -9 dB. However, adjacent channel interference also degrades the sensitivity as well as the C/I performance. During cell planning the aim should be to have C/A higher than 3 dB, i.e.:

C/A > 3 dB

Adjacent frequencies must be avoided in the same cell and preferably in neighboring cells as well.

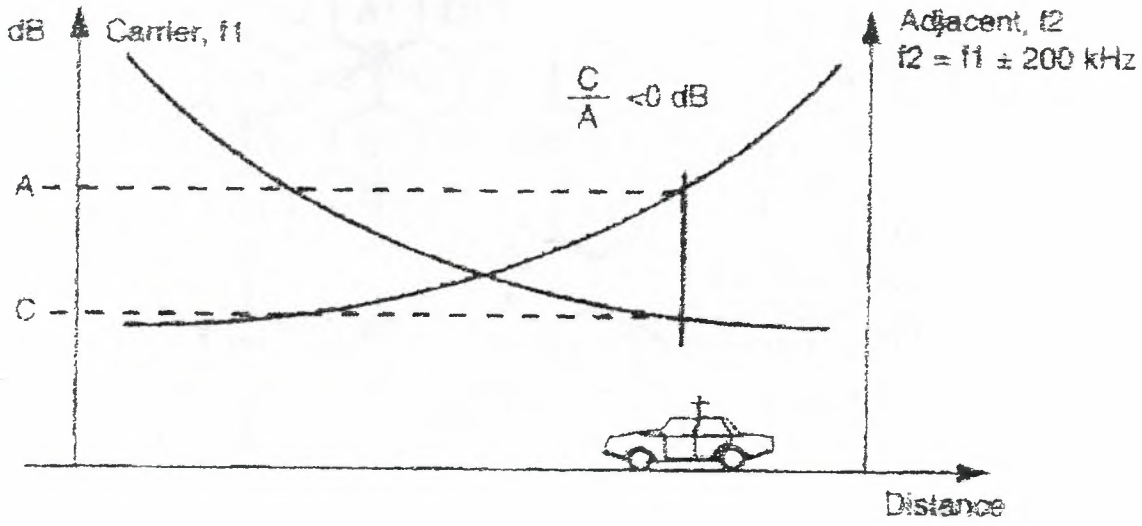


Figure 4.14 Adjacent channel interference

By re-using the carrier frequencies according to well-proven reuse patterns (Figure 4.5 and Figure 4.6), neither co-channel interference nor adjacent channel interference will cause problems, provided the cells have isolropic propagation properties for the radio waves. Unfortunately this is hardly ever the case. Cells vary in size depending on the amount of traffic they are expected to carry, and nominal cell plans must be verified by means of predictions or radio measurements to ensure that interference does not become a problem.

The re-use patterns recommended for GSM are 4/12- and 3/9-pattems. 4/12 means that each cluster has four three-sector sites Supporting twelve cells (Figure 4.15).

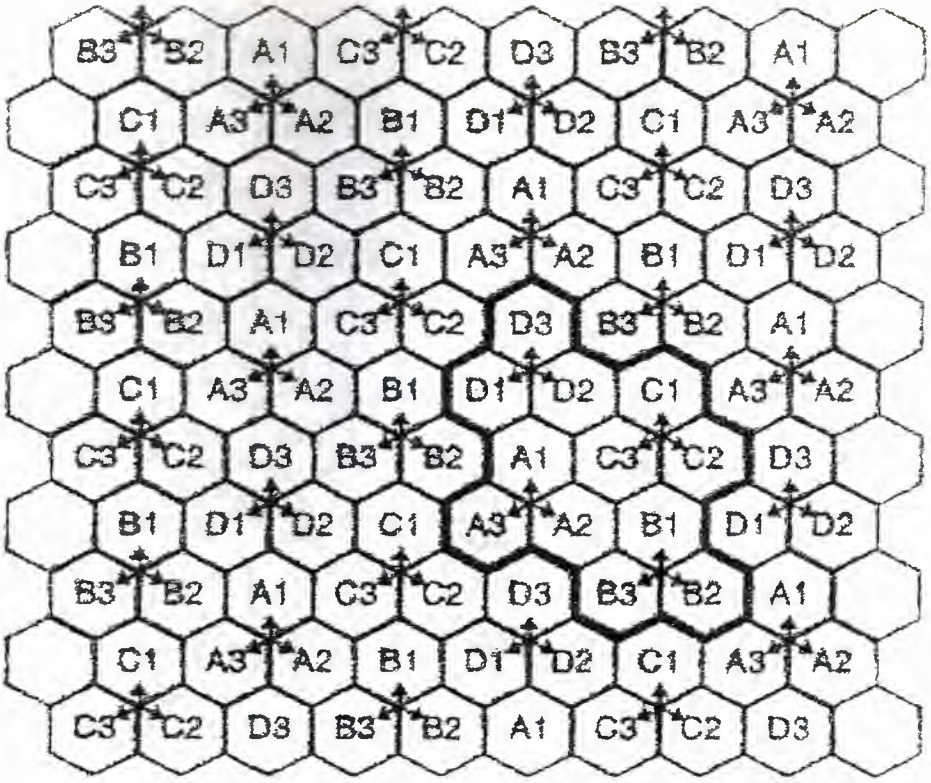


Figure 4.15 4/12 re-use pattern

The re-use pattern in Figure 4.15 is compatible with the condition C/I>12 dB. A shorter re-use distance, given a smaller C/I-ratio, is used in the 3/9-pattern (Figure 4.16).

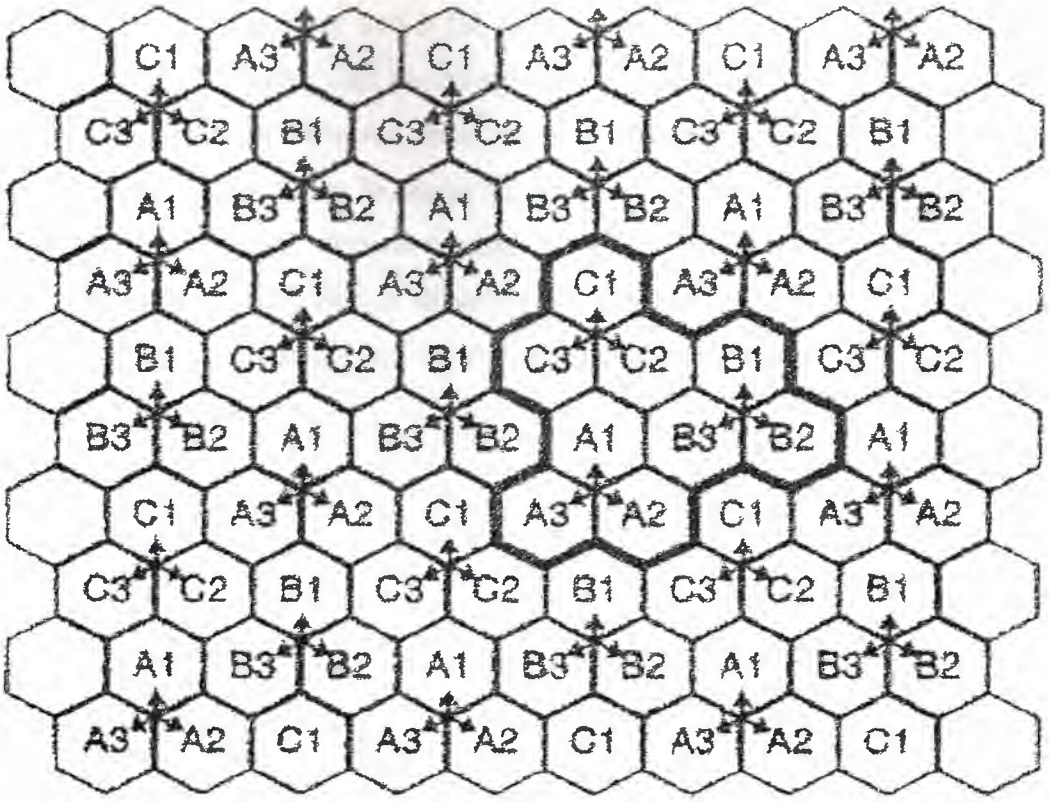


Figure 4.16 3/9 re-use pattern

This re-use pattern (Figure 4.16) is recommended only if frequency hopping is implemented. It has a higher channel utilization because the carriers are distributed among nine cells rather than 12. Other re-use patterns with much higher re-use distances (such as the 7/21) must be used for systems which are more sensitive to interference; e.g. analog mobile telephone systems.

4.8.2 Intersymbol Interference (ISI)

InterSymbol Interference (ISI) is caused by excessive time dispersion. It may be present in all cell re-use patterns. ISI can be thought of as co-channel interference. However in this case the interferer, R, is a time delayed reflection of the wanted carrier. According to GSM specifications, the signal strength ratio C/R must be larger than 9 dB (compared to the C/I-criterion). However, if the time delay is smaller than 15μs (i.e., 4 bits or approximately 4,4 km), the equalizer can solve the problem. ISI is not affected by the re-use pattern chosen, but is still an issue for the cell planner.

How can the cell planner avoid ISI in the cellular network? Normally, the reflected waves are much weaker than the direct wave. However, if the direct wave is obstructed (shadowed), or if the reflected wave has a very advantageous path of propagation, the C/R ratio may creep down lo dangerous values if the time delay is outside the equalizer window. Hence, time dispersion may cause problems in environments with, e.g., mountains, lakes with steep or densely built shores, hilly cities, and high metal-covered buildings. The location of the BTS can thus be crucial. Figure 4.17 Figure 4.18 suggest some possible solutions.

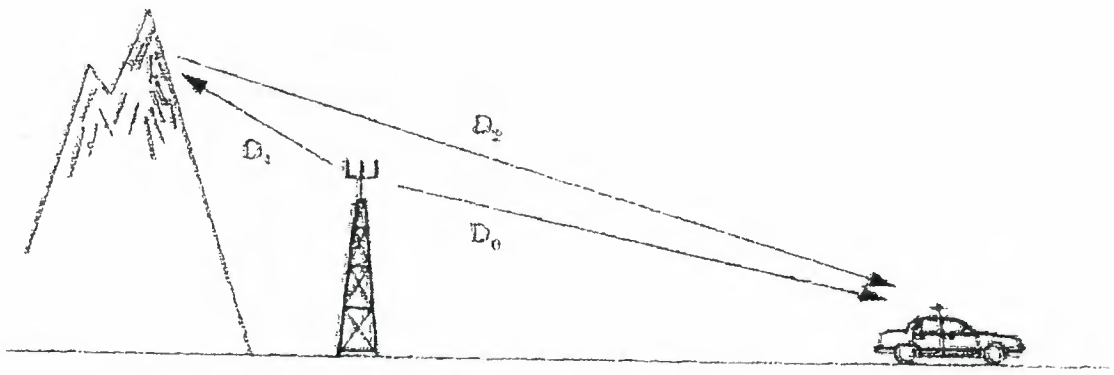


Figure 4.17 Locating the BTS dose to the reflecting object to combat ISI

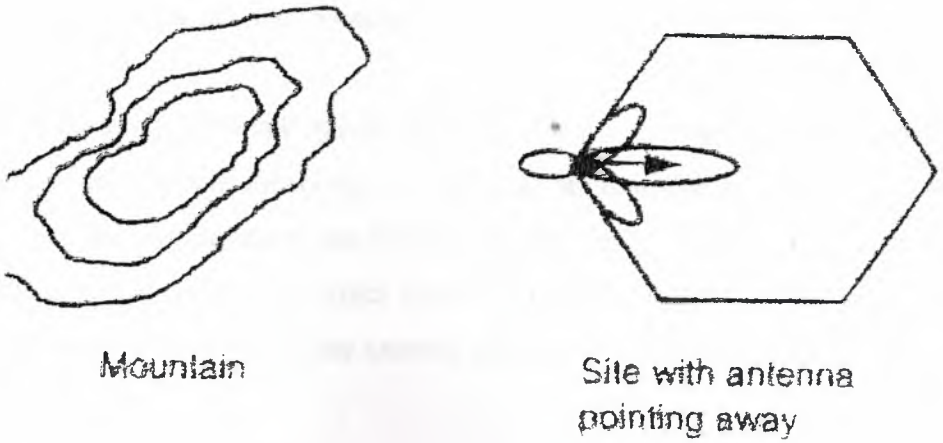


Figure 4.18 Pointing the antenna away from the refiecting object to combat ISI

5. SURVEYS

5. 1. Radio Network Survey

5.1.1 Basic Considerations

It is likely that the system operator has a number of alternative buildings which may be used in the cellular network planning phase. One reason for this is to reduce the initial cost.

The following aspects of site selection must be studied:

- Position relative to nominal grid
- Space for antennas
- Antenna separations
- Nearby obstacles
- Space for radio equipment
- Power supply/battery backup
- Transmission link
- Service area study
- Contract with the owner

5.1.2 Position Relative to Nominal Grid

The initial study for a cell system often results in a theoretical cell pattern with nominal positions for the site locations. The existing buildings must then be adapted in such a way that the real positions are established and replace the nominal positions. The visit to the site is to ensure the exact location (address/coordinates and ground level). It is also possible for more than one existing site to be used for a specific nominal position.

5.1.3 Space for Antennas

The radio propagation predictions provide an indication on what type of antennas can be used on the base station and in what direction the antennas should be oriented.

The predicted antenna height should be used as a guideline when the on-site study starts. If space can be found within a maximum deviation of 15% from the predicted height the original predictions can be used with sufficient accuracy.

If it is possible to install the antennas at a higher position than the predicted position, the operator must ensure that there is no risk force-channel interference. If the antennas are to be installed at a lower position than predicted, new predictions must be carried out based on this position.

It is not necessary that all antennas in one particular cell have the same height or direction. That is, it is possible to have cells on the same base station with different antenna heights. This can be the case if space is limited in some directions. There are also cell planning reasons for placing antennas at different heights. These include coverage, isolation, diversity, and/or interference.

5.1.4 Antenna Separations

There are two reasons for antennas to be separated from each other and from other antenna systems:

- To achieve space diversity
- To achieve isolation

The horizontal separation distance to obtain sufficient space diversity between antennas is 12-18 λ or 4-6 meter for GSM 900 and 2-3 m for GSM 1800/1900. Typical values of separation distances between antennas to obtain sufficient isolation (normally 30 dB) are 0.4 m (horizontal) and 0.2 m (vertical) for GSM 900.

5.1.5 Nearby Obstacles

One very important part in the Radio Network Survey is to classify the close surroundings with respect to influence on radio propagation. In traditional point-to-point communication networks, a line-of-sight path is required. A planning criterion is to have the first fresnel zone free from obstacles. (NOTE: The fresnel zone is the area in

open space that must be practically free of obstructions for a microwave radio path to function property; some degree of fresnel consideration is required in the immediate vicinity of the microwave radio RF envelope/field.)

It is not possible to follow this guideline because the path between the base and the mobile subscriber is normally not line-of-sight. In city areas, one cell planning criterion is to provide margins for these types of obstacles.

If optimal coverage is required, it is necessary to have the antennas free for the nearest 50-100 m. The first fresnel zone is approximately five meters at this distance (for 900 MHz). This means the lower part of the antenna system has to be five meters above the surroundings.

5.1.6 Space for Radio Equipment

Radio equipment should be placed as close as possible to the antennas in order to reduce the feeder loss and the cost for feeders. However, if these disadvantages can be accepted, other locations for the equipment can be considered. In addition, sufficient space should be allotted for future expansions.

The radio network survey includes a brief study with respect to this matter. A more detailed analysis takes place when the location is chosen to be included in the cellular network.

5.1.7 Power Supply / Battery Backup

The equipment power supply must be estimated and the possibility of obtaining this power must be checked. Space for battery back-up may be required.

5.1.8 Transmission Link

The base station must be physically connected to the BSC. This can be carried out via radio link, fiber cable, or copper cable. Detailed transmission planning is not included in this project.

5.1.9 Service Area Study

During the network survey it is important to study the intended service areas from the actual and alternate base station lucations. Coverage predictions must be checked with respect to critical areas.

5.1.10 Contract With the Owner

The necessary legal documentation must exist between the land owner and the proposed site user, e.g., a contract for site leasing. Even though cost is a major consideration in the site acquisition process, cost is not discussed as a factor in this project.

5. 2. Radio Measurements

5.2.1 Path Loss Parameters

A radio survey involves installation of a transportable test transmitter somewhere in the area where the base station is to be installed. Using a specially equipped vehicle, signal strength can be measured. A locating unit, a measuring receiver with antenna, a control and processing unit, and a tape recorder are among the equipment contained in the unit. Signal level can be measured on a number of channel and, for each channel, samples are taken at an adjustable speed. Normally, samples are taken several times per wavelength traveled.

The data is pre-processed before it is stored on either the hard drive or a diskette and presented off-line after the survey. Results can be presented with respect to median value, standard deviation, and number of "measuring squares" along the test routes. The

recorded files can be imported into EET and displayed on the map. The residual values (i.e., the difference between the prediction and the measurement) can also he displayed. If there is a difference, the path loss parameters in the prediction model can be adjusted according to the measurements.

5.2.2 Time Dispersion

Measurements must be performed to verify the time dispersion predictions. In addition, if there are quality problems, time dispersion measurements must be taken to verify that time dispersion is actually causing the poor quality.

The equipment used for time dispersion measurements consists of a transmitter and a receiver (Figure 5.1). The transmitter sends a short pulse, the signal is received, and the pulse response is evaluated in a controller(Figure 5.2). In this way, the time delay and the carrier to reflection ratio can be found.

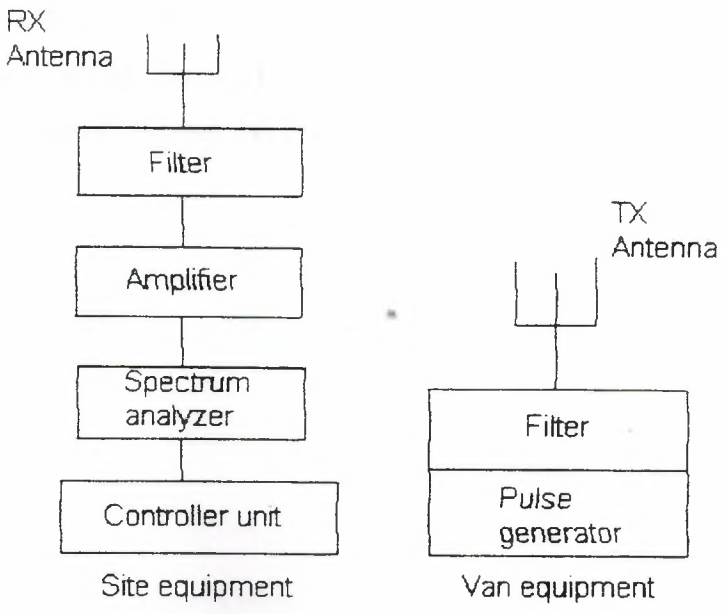


Figure 5.1 Time dispersion measurement equipment

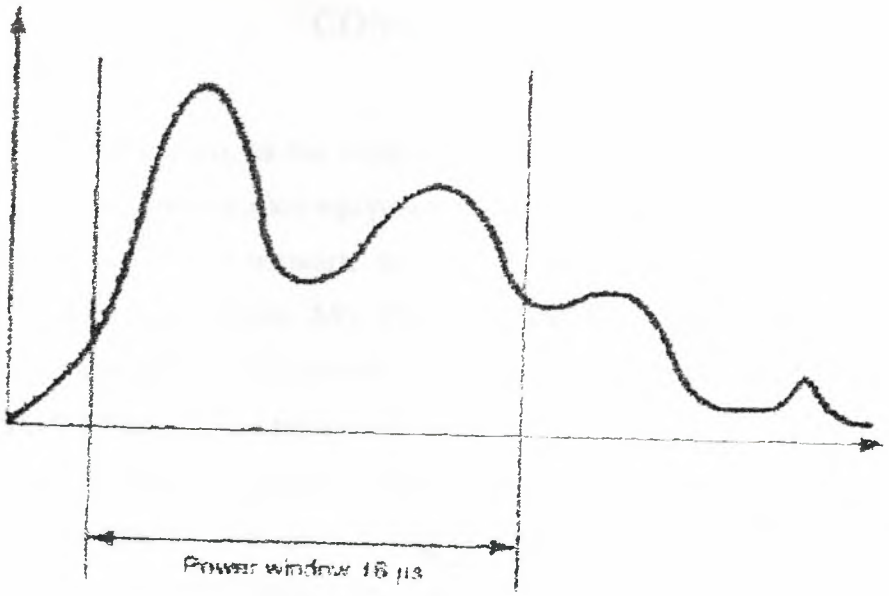


Figure 5.2 Impulse response

5.2.3 Interfering Transmitters

For sites where a number of other radio transmitters are co-located.These include a computer controlled spectrum analyzer and computer programs for calculating interference levels at different frequencies. The end result of a radio spectrum measurement is to accept the site from an interference point of view, to accept it with reservations, or to reject the site and find another one.

CONCLUSION

GSM has been well known, as the world's the most popular standard for new cellular radio and personal communication equipment throughout the world.

In the architecture of GSM network, an overview of the GSM network is presented. GSM consist of four subsystems: MS, BSS, NSS and OSS. Also the functional entities in each of the subsystems are described. The geographical areas of network, radio link aspects and GSM functions are presented.

Coverage analysis should produce information about the geographical area and expected need of capacity. The types of data collected are: cost, capacity, coverage, and grade of services, available frequencies and speech quality index and system growth capability.

Radio measurements are performed in order to verify the coverage and interference predictions. Visiting the real environment to determine whether it is suitable site location when planning a cellular network is necessary.

Once we have optimized and can trust the predictions generated by the planning tool, the dimensioning of the BSC and MSC is performed. Then, the final cell plan is produced.

The system needs constant retuning, because the traffic and the numbers of subscribers increase continuously. Eventually the system reaches a point where it must be expanded so that it can manage the increasing load and new traffic. At this point, cell planning process starts again.

REFERENCES

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

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

[3] GSM Specification Series 1.02-1.06, "GSM Overview, Glossary, Abbreviations, Service Phases."

[4] GSM Specification Series 3.01-3.88, "GSM PLMN Functions, Architecture, Numbering and Addressing, Procedures."

[5] Padgett, Jay E., Gunther, Christoph G., Hattori, Takeshi, " Overview of Wireless Personal Communications". IEEE Communications Magazine, V33, n1, January, 1995:28, 14 pages.

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

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

[8] Mouly, M, and Poutet, M, "The GSM System for Mobile Communications", Palaiseau, France, 1992.

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

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

[11] Javier Gozalvez Sempere Research Engineer in Mobile Communications "An Overview of the GSM System" University of Strothclyde Glasgow, Scotland.

[12] John Scourios (University of Waterloo). "Overview of the Global System for Mobile Communications". http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html

[13] GSM Cell Planning Principles, Ericsson Radio Systems AB, Stockholm, 2000.

[14] AXE / GSM Overview, Ericsson Radio System AB, Stockholm, 1999.

[15] BSC Operation and Mention, Ericsson Radio System AB, Stockholm, 1999.

[16] MSC Operation and Mention, Ericsson Radio System AB, Stockholm, 2000

[17] RBS 2000, Ericsson Radio System AB, Stockholm,2000.