NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Electrical and Electronic Engineering

MOBILE SWITCHING CENTER

Graduation Project
EE-400

Student: MOHAMMED AL MALLAHI (20001497)

Supervisor: Mr. Jamal Fathi

Lefkoşa-2005

ACKNOWLEDGMENT

First I want to thank Mr. jamal fathi to be my advisor. Under his gudance, I successfully overcome many difficulties and learn a lot about Mobile Communications. In each discussion, he explained my questions petiently, and I felt my quick progress from his advice. He always helps me a lot either in my study or my life. I asked him many questions in Electronics and Communication and he always answered my questions quickly and in detail.

I also want to thank my friend in NEU (UZUN-ABUMETLEQ-BATMAZ-ALBASHA-BATUMAN-SHAHEEN-BELAAL-ALAA-ABOSAMRA-ABUZAED-RAED-MAYAR-HATHAT-MESLEH-KOJOK) Begin with them make my years in NEU full of fun.

Finally, I want to thank my family, especially my parents. Without their endless support and love for me, I would never achieve my current position. I wish my mother lives happily always, and my father in palestine be proud of me.

LIST OF ABBREVIATIONS

AGCH Access Grant Channel

ATDMA Asynchronous TDMA

ATM Asynchronous Transfer Mode

BCCH Broadcast Control Channel

BSS Base Station System

BSSAP Base Station System Application Part

BSSMAP Base Station System Management Application Part

BTS Base Transceiver Station

BTSM Base Transceiver Station Management

CDMA Code Division Multiple Access

DTAP Direct Transfer Application part

EIR Equipment Identity Register

ES Earth Station

FACCH Fast Associated Control Channel

FCC Federal Communications Commission

FCCH Frequency Correction Channel

FDD Frequency Division Duplex

FDM Frequency Division Multiple Access

FDMA Frequency Division Access

FEC Forward Error Correction

GEO Geostationary

GMSC Gateway MSC

GMSK Gaussian Minimum Shift Keying

GOCC Ground Operator Control Central

GSM Global System For Mobile Communication

HLR HOME Location Register

IMEI International Mobile Equipment Identity

IMSI International Mobile Subscriber Identity

ISL Inter-Satellite Link

ISO International Standards Organization

IWF inter-Working Function

IWMSC Inter-Working Mobile Switching Center

LAPD Link Access Protocol For the ISDN D-channel

MEO Medium Earth Orbit

MS (GSM) Mobile Station

MSISDN MS ISDN (Integrated Services Digital Network) number

MSRN MS roaming number

MT (satellite) Mobile Terminal

MTP Message Transport part

OSI Open System Interconnect

PCH paging channel

PLMN Public Land Mobile Network

PSTN public switched Telephone Network

QPSK Quaternary Phase Shift Keying

RACH Random Access Channel

RF Radio Frequency

RPE/LTP Regular pulse Excited long Term (pitch) Prediction

RR Radio Recourse

SACCH Slow Associated Control Channel

SCCP Signaling Connection control part

SCH Synchronization Channel

SPCCH Stand-Alone Dedicated Control Channel

SDMA Sa\peace Division Multiple Access

SMS Short Message Service

SOCC Satellite Operations Control Contras

TCH Traffic Channel

TDD Time Division Duplex

TDMA Time Division Multiple Access

TRAU Transponder and Rate Adapter Unit

TT&C Telemetry, Tracking and Control

TX Transmit

UMTS Universal Mobile Telecommunications System

VLR Visitor Location Register

CONTENTS

ABSTRACT

The mobile switching center is one of the most important aspect in the mobile communication which is centered in the subsystem of the mobile network.

The main objective of this project is provide analysis and provides all the functionality needed to handle a mobile subscriber such as registration, authentication, Location updating, hand over (mobility), and call routing to a roaming subscriber which done using a mobile switching center.

For this purpose I start my project in general idea about mobile communications and then go to more specific section in mobiles which is GSM and after this I went to GSM architecture to explain the mobile switching area.

The MSC also has the interface to other networks such as private Land mobile networks, public switched telephone networks and integrated services digital networks (ISDN). The underling principle of MSC is based on controls the calls Setup, supervision and release and may interact with other nodes to successfully establish a call.

INDTRODUCTION

The mobile switching center is one of the most important aspects of the mobile communications. Mobile services Switching Center (MSC) is the main part of the Network Subsystem. It is performs the switching of calls between the mobile users, and between mobile and fixed network users.

The MSC also handles the mobility management operations. It acts like normal switching node of the PSTN or ISDN, and additionally provides all the functionality needed to handle a mobile subscriber

This project is aimed to provide analysis of MSC and to enhance where it use.

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

Chapter 1 introduces the basis of mobile communication system.

Chapter 2 presents an overview of Global System for Mobile Communications. In this Chapter, covers everything related to GSM. Like history of Gsm, services provided by GSM, GSM network architecture, Radio Link aspect and network aspect.

Chapter 3 studies the architecture and protocols of the GSM and make comparison with GPRS. In this chapter, I am attempt to go directly to the architecture of GSM and explain the GSM network to describe the area of MSC. And give other example to use MSC in the GPRS.

In chapter 4 it studies the mobile switching center, which covers the switching system, MSC function, Gat way MSC (GMSC), authentication procedure and service function.

CHAPTER 1

MOBILE COMMUNICATION SYSTEMS

1.1 Cordless Telephones

The cordless telephone consists of the base and portable units (see Figure 1.1). These units are linked by a low power PM system. The connecting wires of a conventional telephone between the portable unit and the base unit are replaced with low-power radio transmissions. Electronic circuits of the cordless telephone involve DTMF generators for dialing, electronic single -or dual -frequency ringers, and electronic speech circuits Cordless telephones are available with the same futures as the electronic telephones that use cords. The cordless telephone usually obtains the operating power directly from the telephone line. However, some cordless telephones, because of their greater power requirement, have to be plugged in to a household power source.

Figure 1.1 Cordless Telephone Units

This is a minor disadvantage since the cordless telephones do not operate if a utility power failure occurs. The cordless telephones have the following features.

1) Speech and volume control;

2) Security features to prevent unauthorized calling;

3) Keeping and displaying up to 50-100 incoming and outgoing calls;

4) Displaying the caller's phone number;

5) Displaying the date and time;

6) Recording the conversation;

7) Auto answering ability.

1.1.1 Base Unit

As shown in Figure 1.2 the base unit connects directly to the telephone line to complete local loop to the central office. The base unit transmits a frequency of 1.6 to 1.8 MHz. It uses AC power line that supplies the power for the base station electronics as well as works transmitting antenna. The nominal 1.7 MHz frequency modulated signal is fed from the base unit transmitter to the AC line through capacitors which block the line current, from the base transmitter while passing the 1.7 MHz output to the line. This uses of the house wiring, as antenna is not unique to cordless telephones. It also is used for wireless intercoms. This method provides good reception within and near the house as well as outside near power lines.

1.1.2 Portable Unit

An internal *lipstick antenna* (like that used in standard radio receivers) in the portable unit i receives the nominal 1. 7 MHz transmission from the base unit over a range from 50 to 1000 feet.

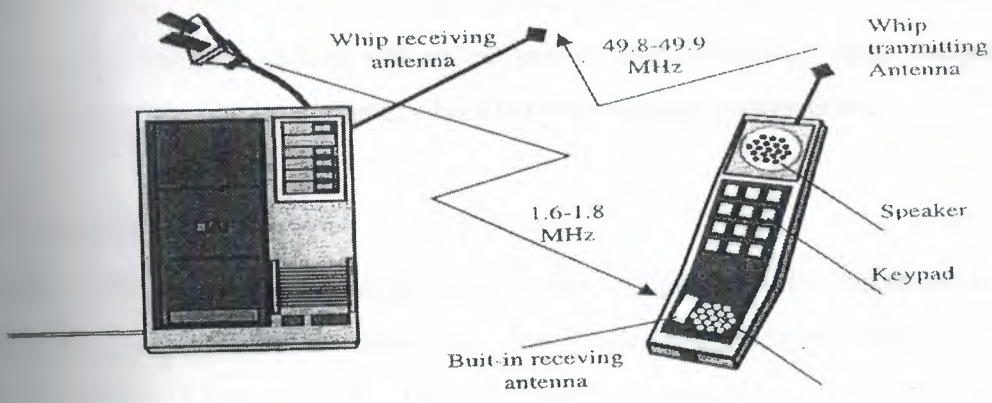


Figure 1.2 Portables Units

This range depends not only on the manufacturer's design, but also on such things as whether the house wiring is enclosed in metal conduct and weather foil -backed insulation is used in the walls. The ringing or voice signal is recovered by demodulation and drives the speaker in the portable unit. The portable unit is powered by a battery, which is recharged when placed in the receptacle in the base unit. The portable unit receives the locally radiated RF signal from the base unit's antenna (the house wiring) with its built -in lipstick antenna, much like a portable radio the portable unit is usually in a stand-by mode which corresponds to the on-hook condition of a telephone set. When the ringer sounds, the user operates on a talk switch, which as a result turns "on " the transmitter in the portable unit. This transmitter transmits a frequency in the range of 49.8 to 49.9 MHz and outputs the signal to the *whip antenna.* (Since the whip is used only for , transmission, it can be collapsed out of the way when the portable unit is on stand-by. If the r portable unit is only for voice transmission, it may have an internal antenna and its range is shorter). A similar whip antenna on the base unit receives the PM signal from the portable unit, demodulates it and applies the off -hook signal to the telephone local loop. Dialing transmits modulation tones to the base unit, which sends either tones or pulses over the telephone lines. After the two parties have been successfully connected, the transmitter and receiver operate simultaneously.

When the user dials the number for outgoing calls, the dial pulses produce tones, which modulate the carrier for transmission to the base unit. The base unit recovers the tones by demodulation. If DTMF service is used, the tones are sent on the telephone line. If pulse service is used the tones are converted to pulses and the telephone line is pulsed. When the connections between calling and called parties are established, both transmitters and receivers operate at the same time, which permits two-way conversation.

1.2 Mobile Telephones

Mobile telephones can be considered as cordless telephones with elaborated portable and base units. High-power transmitter and elevated antenna provide the radio carrier link over an area within 20 to 30 miles from the base station antennas. Using the multiplexing, detecting, and selecting features it is possible to provide simultaneously service up to 60

subscribers per ease station. This is the major difference between cordless telephones and mobile telephones.

1.2.1 Base Unit

The base station can transmit and receive on several different frequencies simultaneously, to provide several individual channels for use at the same time. The radio base station transmitter's output power is typically 500 watts. The mobile telephone base unit can operate on many channels simultaneously and can easily cover the average city with a power of several 100 watts. It covers a circular area of up to 30 miles in radius for clear reliable communications, but transmitters with the same frequency are not spaced closer than about 60 to 100 miles because of the noise interference levels.

The base unit receiver contains the necessary electronics to present its control terminal with a good audio signal. The control terminal interfaces the voice and control signals to the standard telephone circuits. The receiver contains filters, high -gain amplifiers, and demodulators to provide a useable voice signal to the telephone line. The control terminal contains the necessary detector and timing and logic circuits to control the transmissions link between the base unit and mobile units. The control terminal has the necessary interface circuits so that a call initiated at a mobile unit is interconnected through the national or international telephone system to the called party just as any other telephone call.

The national and international telephone system facilities are owned by the respective telephone companies. The base units and the mobile units may be owned by the Telephone Company or by a separate company called a Radio Common Carrier (RCC).

1.2.2 Mobile Unit

The mobile unit contains a receiver, a transmitter, control logic, control unit, and antennas. For the user it operates pretty much like and ordinary electronic telephones. Figure 1.3 shows the modern mobile telephones layouts.

Figure 1.3 The Modern Mobile Telephones Layouts

Mobile telephone communication setup is shown in Figure 1.4. The mobile unit in the user's vehicle consist of a receiver containing amplifiers, a mixer and a demodulator; a transmitter containing a modulator, carrier oscillators and amplifiers; the necessary control logic; a control unit with microphone, speaker, key pad and switches; antennas and the interconnecting cables. The control units perform all of the functions associated with normal telephone use. The mobile telephone user places and receives the calls in the same manner as with an ordinary telephone. When the hand set is lifted to place a call, the radio unit automatically selects an available channel. If no channel is available, the busy light comes on. If a channel is found, the user hears the normal dial tone from the telephone system, and can then dial the number and proceed as if the telephone was direct wired. An incoming call to the mobile unit is signaled by a ringing tone and is answered simply by lifting the handset and talking. Thus the automatic mobile telephone is as easily used as a home telephone. The mobile telephone combines the mobility of the radio link and the world -wide switched network of the existing telephone system to provide a communication link to any other telephone in the world.

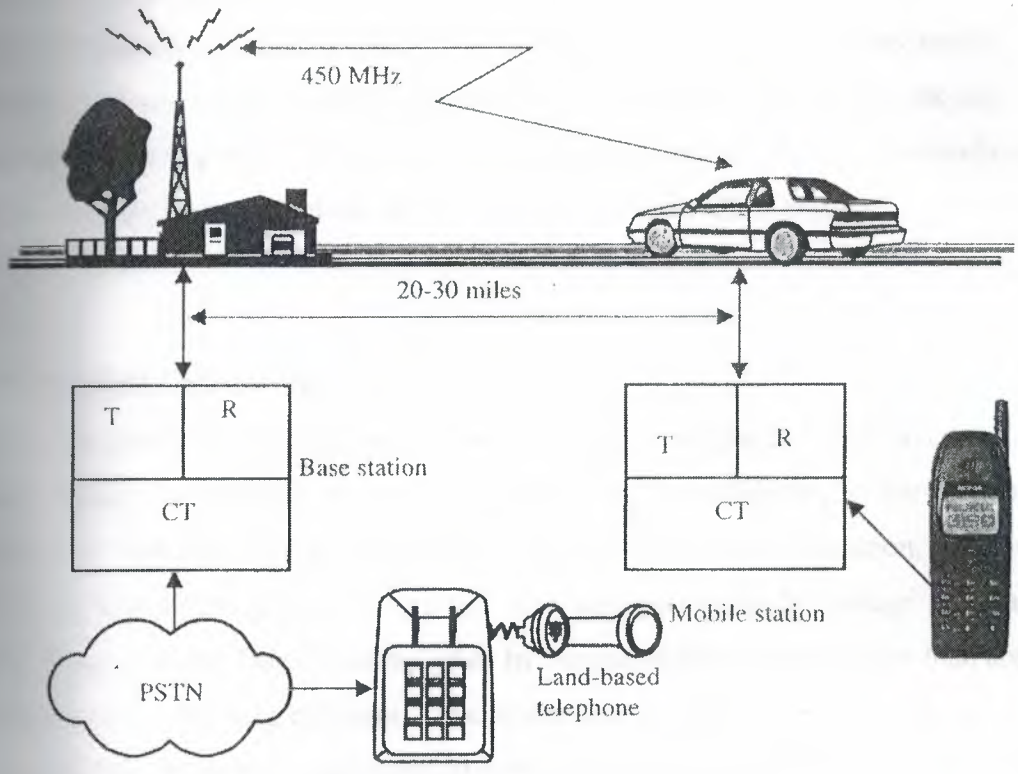


Figure 1.4 Mobile Telephone Communication Setup

1.3 Home Area and Roaming

As previously stated, the mobile system is designed for optimum use within a 20-30 miles radius of the base antenna. This is called the subscriber's home area and a subscriber usually would remain in the home area. However if the subscriber moves out of the home area into another area, the subscriber is referred to as a roamer and a different mode of operation applies. Each mobile telephone has a unique telephone number, which includes the home area's base station identification. When someone calls the mobile unit the calling party is connected first to the transmitter serving the subscriber's home area. As long as the subscriber is within radio range of that system, all is well; otherwise, the base station won't get an answer from the mobile unit and the caller will get a no-answer signal. If the subscriber roams outside the home area, he / she can still be reached if a similar mobile

telephone system exist in that area, provided proper advance arrangements have been made. If a subscriber goes outside the range of his base station, his mobile telephone can only reached through another similar adjacent mobile base station system.

Calls to roamers are usually placed by calling special number for the mobile service operator who knows the roamer's location. The operator manually patches the call through base station serving the area of the roamer's location. Some systems can not handle roamers due to overload of their channels, and some system doesn't allow roamers.

1.4 Detailed Operation

Different signaling techniques have to used in a mobile telephone system in contrast with a wired facility. Since there are no wires connecting the telephone to the network, both speech and signaling must be transmitted via radio. For wireless operation, tones are used for those signaling functions, which are otherwise performed by voltage and current in hard- wired systems. This is accomplished by' the use of special tones rather than applying a voltage level or detecting a current.., The proper tone transmitted to the mobile unit will, for example, ring the mobile: telephone to indicate an incoming call just as with a standard telephone different tone is used to indicate off -hook, busy, etc. The Improved Mobile Telephone System (IMTS) uses in-band signaling tones from 1300Hz to 2200Hz. The older Mobile Telephone System (MTS) had in-band signaling tones in the 600 Hz to 1500 Hz range. Some systems use 2805 Hz as manual operation.

Incoming Call

To gain a better understanding of the system operation, conceder an incoming call from a facility subscriber through the base unit to a mobile unit. The base station controls all activity on all channels. It selects only one idle channel and places a 2000 Hz idle tone (1) as shown Figure 1.5. All on-hook mobile units that are turned on automatically search for the idle tone and lock or the idle channel because this is the channel over which the next call in either direction will be completed. After locking on the idle channel, all on-hook mobile units "listen" to their numbers that channel. When an idle channel becomes busy for a call in either direction, the base station, control terminal selects another unused channel

before. If the mobile does not answer within 45 seconds, ringing (6) is discontinued and the call abandoned. When the mobile subscriber goes off-hook to answer, the mobile supervisory unit sends a burst of connect tone (1633 Hz) as an answer signal (8). Upon receipt of the answer signal, the control terminal stops the ringing and establishes a talking path between the calling circuit and the radio channel (7). When the subscriber hangs-up (8) at the end of call, the mobile supervisory unit sends disconnect signal (12) alternating the disconnect tone (1336 Hz) and the guard tone. The mobile supervisory unit then turns of the mobile transmitter and begins searching for the market idle channel. Each on-hook mobile unit receiving the number transmission compares the received number to its unit number. Only the one mobile unit with a number match remains locked on that channel.

Outgoing Call

The sequence for a call originated by a mobile subscriber is illustrated by Figure 1.6. When the subscriber goes off-hook to place the call, the mobile unit must be locked on the marked-idle channel. If not, the handset will be inoperative and the busy lamp on the control unit will light, indicating to the subscriber that no channel is available. If the mobile unit is locked on the marked idle channel, the mobile supervisory unit will turn on the mobile transmitter to initiate the acknowledgment or handshake sequence. Then mobile unit transmits its own number so the control terminal can identify it as a subscriber and can charge the call to the number. The reaming functions of Figure 1.6 (b) are similar to those of Figure 1.5. When a call is originated from the field, the mobile unit finds a marked idle channel and broadcasts an acknowledgment to the base by sending its identification. The mobile unit than completes a call in the usual manner by receiving a dial tone, then dialing the number and waiting for the called party to answer.

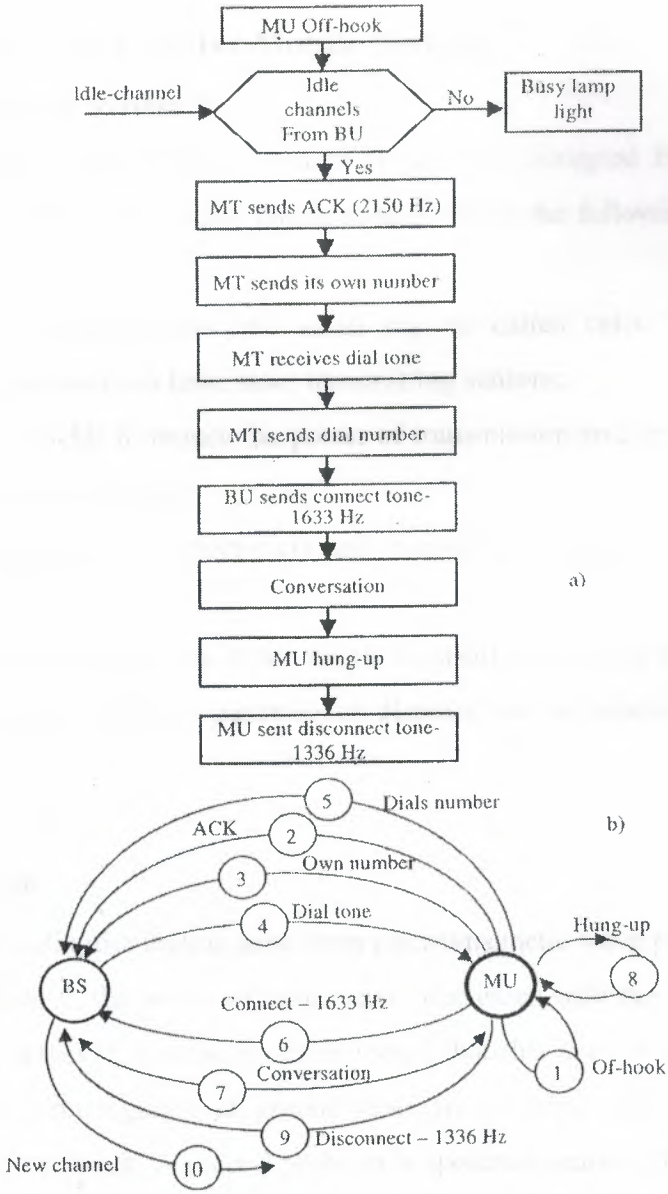


Figure 1.6 The Sequence for a Call Originated by a Mobile Subscriber.

1.5 The Architecture of the Cellular Mobile System

What Is a Cellular Telephone System?

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

1) Division of heavily populated areas into small regions called cells. In this way, concentrated I 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 inure acceptable value.

1.6 Cellular Coverage

The major problems with radio distribution arise from electromagnetic wave propagation. As mentioned in the chapter 1, 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 abase 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.

Cluster. The cells are grouped into clusters. The number of cells in cluster must be determined so that the cluster can be reputed 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 neighboring clusters. This interference is produced by the small size of the clusters (the size of the cluster is defined by the number of cells per cluster). The total number of channels per cell depends on the number of available channels and the type of cluster used.

There are following types of cells: macro cells, micro cells, selective cells, and umbrellas, Macrocells. The macrocells are large cells for remote and sparsely populated areas. **Microcell**s. These cells are used for densely populated areas. By splitting the existing areas smaller cells, the number of channels available are increased as well as the capacity of the. The power level of the transmitters used in these cells is then decreased, reducing the possibility of interference between neighboring cells.

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

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

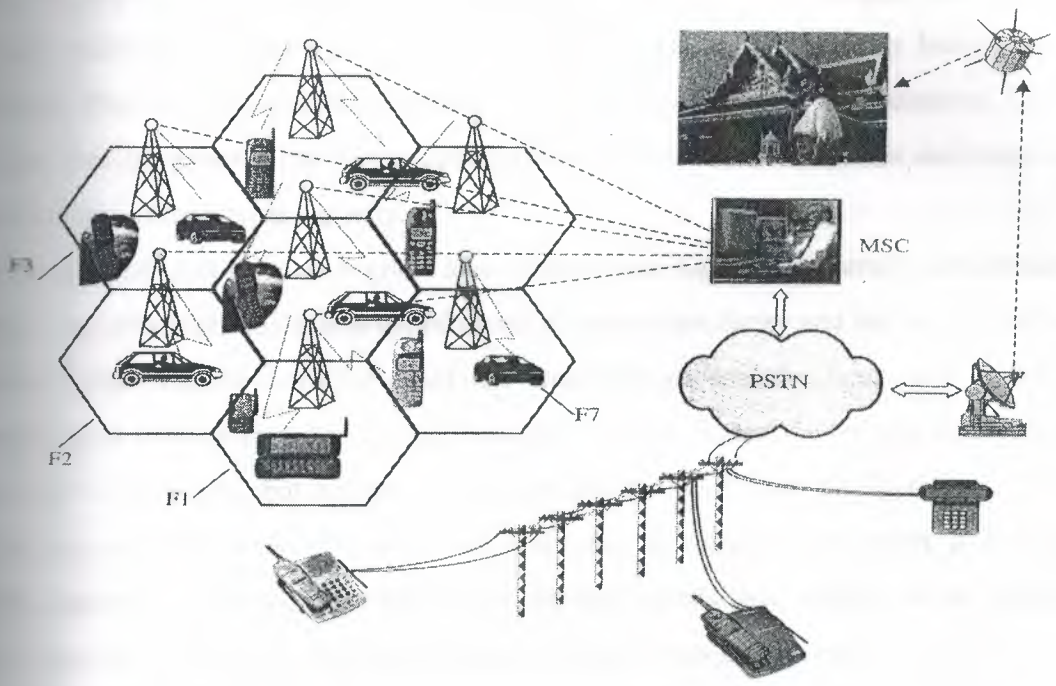


Figure 1.7 The Cellular Setup

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 center 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 diagram operates on a different frequency, denoted by Fl, F2. ..F7. In the Global System of Mobile Communication (GSM), the design was aimed at the beginning at medium-sized cells, of a diameter expressed in kilometres or tens of kilometers. Yet, the lower boundary is difficult to determine; cells of more than one kilometers 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 kilometres. 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 exists 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 1.7.

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 PM 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 telephone 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 telephone.

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.

1.6.1 Setting up a Cellular Telephone Call

When a phone call comes into the cellular system from the conventional telephone switched network PSTN or from another cellular telephone, the computer-based Mobile Switching Centre MSC follows the three steps depicted in Figure 1.8 in setting up the proper connection. In step 1 an appropriate paging message is directed by MSC to all the base stations BS. In the step 2 appropriate cellular telephone acknowledges (Figure 1.8 (b)) the page by sending digital pulse-train, back to the base station from which a signal came. In step 3 the base static automatically selects and activates a duplex voice channel to handle the call, then sign appropriate cellular telephone for transmission and reception (see Figure 1.8 (c)).

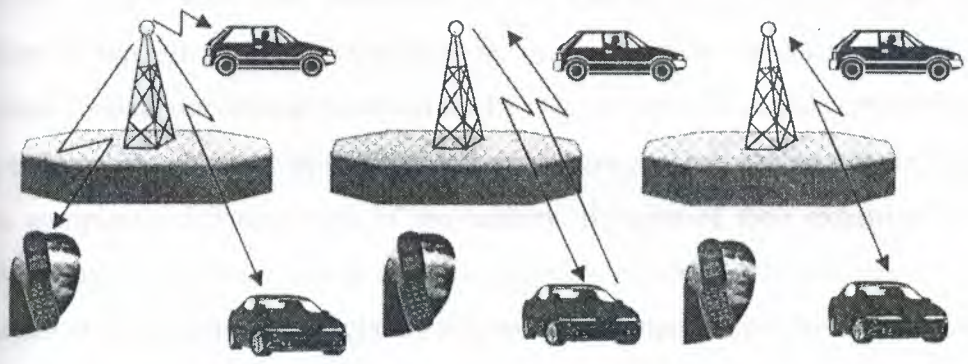


Figure 1.8 Setting up a Cellular Telephone Call

1.6.2 Roamers

The system is designed to make handling of roamers automatic. This is the principal goal the cellular approach. Locating and hand-off are the concept that comes directly from the use 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 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 Telephone 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 countryside toward a city, continue through the city's downtown, and not hang up until 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 Mobile Telephone Switching Center MSC a specifically designed computer telecommunications facility that sets up the pro connections, keeps the track of billing charges, and automatically handles any necessary hand-o Hand-offs to anew base station are attempted whenever the signal quality degrades as users travel through the cellular telephone coverage area from one cell to another.

Trunk lines connect the cellular switch to the PSTN, and from the mobile cellular telephone system can originate from or be directed toward ordinary telephones or cellular telephones local in completely different parts of the country. Because of their extensive frequency reuse in a small local area, cellular telephone systems can handle a multitude of users. In most urban areas government regulators maintain 'the proper competitive environment by licensing two separate cellular telephone 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 telephone to a. mobile unit, which has roamed, to another metropolitan area presents additional problems. While 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 be 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 unauthorized disclosure of the service area to which the mobile unit has roamed.

1.6.3 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 telephone 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 does this. Each transmitter covers only its own cell, and cells sufficiently far apart 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 is shown in Figure 1.9. 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 cell, and by not using the same frequency in adjacent cells. The cellular system can be -handed because cell splitting may occur as demand increases.

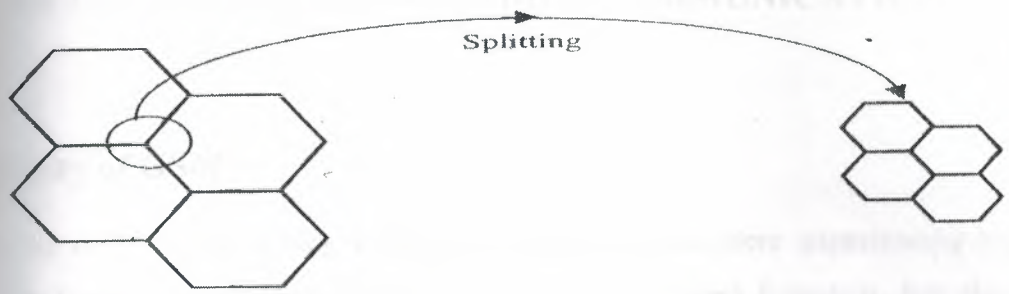


Figure 1.9 The principle of the cell splitting.

The spectrum scarcity is circum vented 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. total system throughput can, therefore, be increased by reducing the cell size.

The world's most popular cellular telephone systems was AMPS (Advanced Mob' Telephone System), developed in the United States, and TACS (Total Access Cellular System 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 AMPS system, TACS uses FM analog voice-channel modulations with digital frequency shi keying for the control channels.

CHAPTER 2

GLOBAL SYSTEM FOR MOBILE COMMUNICATION

2.1 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. 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 Groupe Spécial Mobile (GSM) to study and develop a pan-European public land mobile system. The proposed system had to meet certain criteria:

1) Good subjective speech quality

2) Low terminal and service cost

3) Support for international roaming

4) Ability to support handheld terminals

5) Support for range of new services and facilities

6) Spectral efficiency

7) ISDN compatibility

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. 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 interworking 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.

2.2 Services provided by GSM

From the beginning, the planners of GSM wanted ISDN compatibility in terms of the services offered and the control signalling 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, teleservices, and supplementary services. The most basic teleservice 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 interwork 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 bidirectional 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 teleservices 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.

2.3 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 Mobile Station is carried by the subscriber. The Base Station Subsystem controls the radio link with the Mobile Station. The Network Subsystem, the main part of which is the Mobile services Switching Center (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 Um 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.

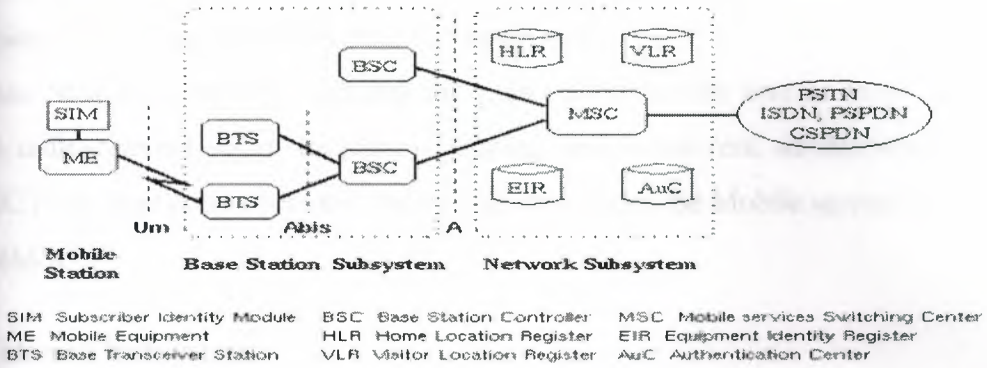


Figure 2.1 General architecture of a GSM network

2.3.1 Mobile Station

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

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

2.3.2 Base Station Subsystem

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

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

2.3.3 Network Subsystem

The central component of the Network Subsystem is the Mobile services Switching Center (MSC). It acts like a normal switching node of the PSTN or ISDN, and 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 conjuction 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). Signalling between functional entities in the Network Subsystem uses Signalling System Number 7 (SS7), used for trunk signalling 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 signalling address of the VLR associated with the mobile station. The actual routing procedure will be described later. There is logically one HLR per GSM network, although it may be implemented as a distributed database.

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

The other two registers are used for authentication and security purposes. The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile

equipment on the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI). An IMEI is marked as invalid if it has been reported stolen or is not type approved. The Authentication Center (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.

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.

2.4.1.1 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 2.2). 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).

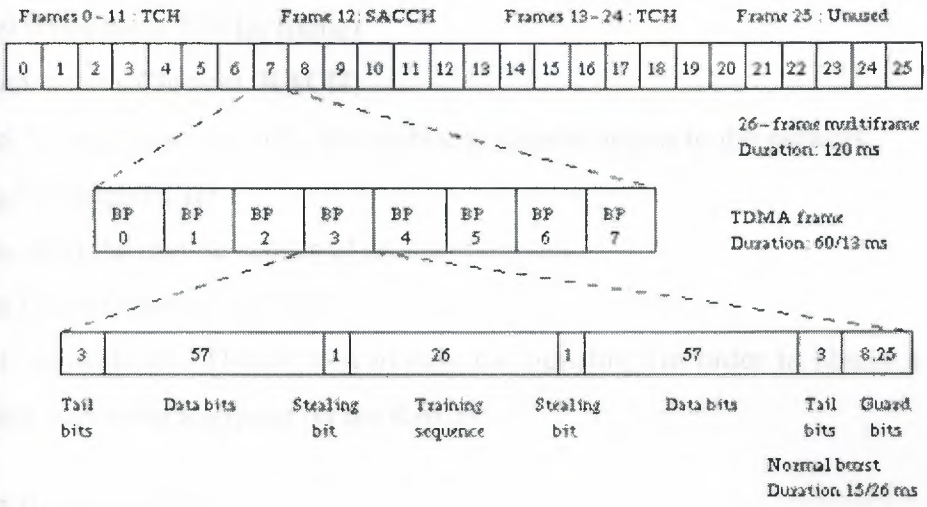


Figure 2.2 Organization of bursts, TDMA frames, and multiframes for speech and data

2.4.1.2 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 signaling 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 Synchronization Channel (SCH)

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

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 signaling (in order to obtain a dedicated channel), following a request on the RACH.

2.4.1.3 Burst structure

There are four different types of bursts used for transmission in GSM . The normal burst is used to carry data and most 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 convolution 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:

1) **Class Ia** 50 bits - most sensitive to bit errors

2) **Class Ib** 132 bits - moderately sensitive to bit errors

3) **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 Network aspects

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 protocol.

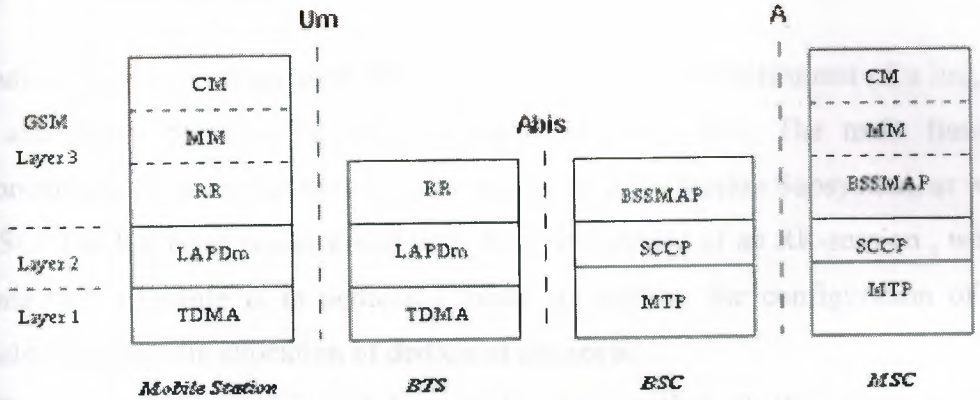


Figure 2.3 Signaling protocol structure in GSM

The signaling protocol in GSM is structured into three general layers , depending on the interface, as shown in Figure 2.3. 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 Signaling System Number 7 is used. Layer 3 of the GSM signaling 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.

Connection Management

Handles general call control, similar to CCITT Recommendation Q.931, 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 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.

2.5.1.1 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:

1) Channels (time slots) in the same cell

2) Cells (Base Transceiver Stations) under the control of the same Base Station Controller (BSC),

3) Cells under the control of different BSCs, but belonging to the same Mobile services Switching Center (MSC), and

4) 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.

2.5.2 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.

2.5.2.1 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.

2.5.2.2 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.

2.5.3 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.

2.5.3.1 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 (see the location updating section). 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 Figure2.4).

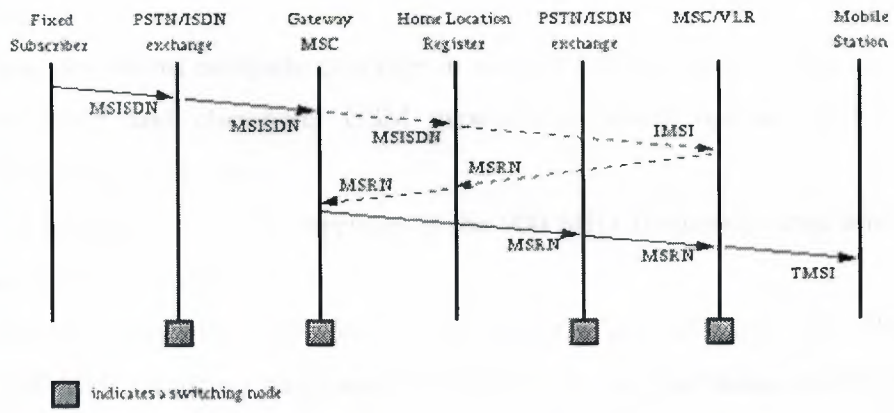


Figure 2.4. Call routing for a mobile terminating call

CHAPTER 3

OVERVIEW AND COMPARISON OF THE ARCHITECTURE AND PROTOCOLS OF THE GSM AND THE GPRS

3.1 Overview of Wireless Wide Area Network

3.1.1 GSM

GSM is a wireless platform that uses radio frequencies, and this way users can be fully mobile, and do wireless data computing anywhere, without worrying about adapters,telephone jacks, cables, etc. The unique roaming features of GSM allow cellular subscribers to use their services in any GSM service area in the world in which their provider has a roaming agreement. GSM-enabled phones have a "smart card" inside called the Subscriber Identity Module (SIM). The SIM card is personalized to the user. It identifies the user's account to the network and provides authentication, which allows appropriate billing.

GSM has been designed for speech services. It uses circuit switched transmission,reserving one radio channel for the user's traffic. It also uses cells which enables it to reuse different frequencies.

GSM, provides almost complete coverage in western Europe, and growing coverage in the Americas, Asia and elsewhere. GSM networks presently operate in three different frequency ranges. These are:

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

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, UK, and Russia.

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.

GSM standard circuit is a digital data bearer service offering 9.6kb/s. This data transmission in these networks is regarded as too slow and often too expensive for many applications. The cost is the total time that the user occupied that channel eventhough he was using the channel all the time. The performance of services such as Internet Applications in a cellular environment is typically characterized by the low available bandwidth, and an inefficient use of the rare air link capacity. Furthermore, long connection setup delay is a problem for bursty services requiring occasional data transfers.

3.1.2 GPRS

GSM's use of circuit switched systems meant that in the case of bursty traffic, the traffic channel will be idle for some time. As the demand for data services increased, GPRS was developed to support packet switching . The work on the GPRS specification began in 1994 as a part of GSM phase 2+ specification. GPRS is a separate packet data network within GSM which provides a packet base platform both for the data transfer and signaling. GPRS is compatible with the GSM architecture. Voice and GPRS services coexist in the same environment with the minimum changes in the system[8].

GPRS focused strongly on the development of a service, which overcomes these drawbacks of a mobile Internet Access. It allows allow reduced connection setup-times,supports existing packet oriented protocols like X.25 and IP, and provides an optimized usage of radio resources.

The main idea is to allocate resources depending on the GPRS demand. This feature operates in a capacity-on-demand mode. The capacity-on-demand concept has been introduced in order to keep compatibility with the existing GSM circuit-switched resources. Resources for GPRS may be dynamically allocated depending on how many users require them with a given quality of service and depending also on how many resources are available at the moment. The operator can decide whether to permanently dedicate some physical resources for GPRS. Load supervision is carried out in the MAC layer to monitor the load of the GPRS physical resources, and it's the function that will allow increasing or decreasing the number of allocated resources according to the existing demand. The operator has also the choice to dedicate temporarily physical resources for GPRS as long as no other higher-priority GSM services require them[8].

Since GPRS is packet oriented it enables volume based charging in contrast to GSM like charging of online time. It therefore allows users to stay constantly online while only paying for the occasional data transfer. Another important factor is the Quality of Service (QoS) offered by these services. The QoS can be negotiated when starting the session and can be renegotiated if it is required. The QoS agreed between the user and the network can be used to charge the service.

In addition, GPRS increases the capacity of the system and reduces the idle periods of the radio channels. This is done by allowing for multiple users per physical channel and using a channel only when it is needed, and releasing it immediately after the transmission is complete.

3.2 Architecture Comparison

This section analyzes the GSM architecture first, as it was the base upon which GPRS was uilt. GPRS architecture is then described while at the same time any differences/similarities are stated.

3.2.1 GSM

A GSM network is composed of several subsystems whose functions and interfaces are specified. Figure 3.1 shows the layout of a generic GSM network. These are the:

1) base station subsystem(BSS)

2) mobile station(MS)

3) network and switching subsystem(NSS)

4) operations subsystem(OSS)

5) operations and maintenance Center(OMC)

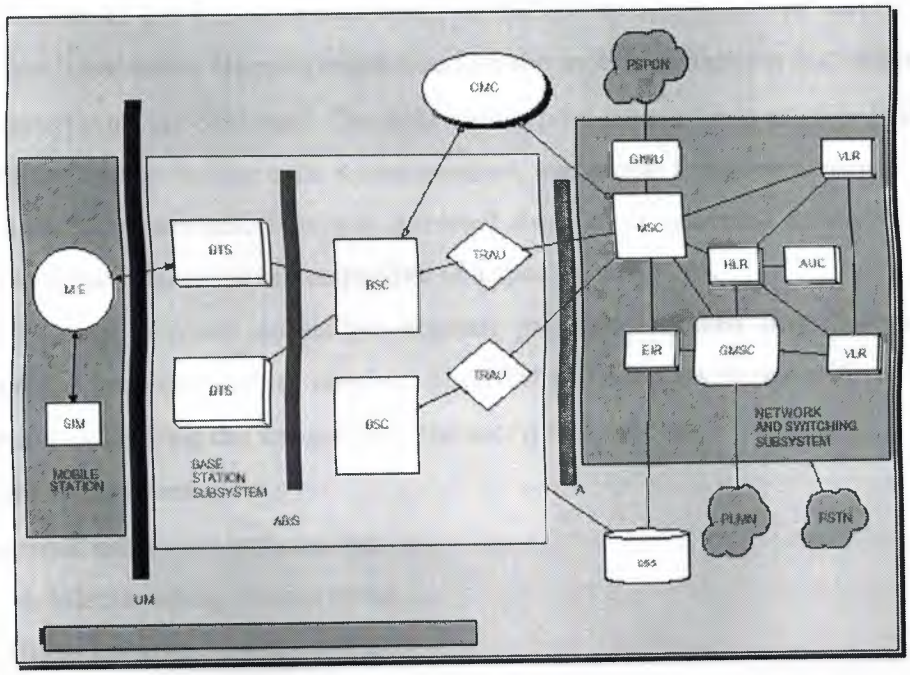


Figure 3.1 GSM Arcitecture [1][3][12]

Base Station Subsystem

The Base Station Subsystem controls the radio link with the Mobile Station. It is mainly composed of the Base Transceiver Station (BTS) and the Base Station Controller (BSC).

The BSC-to-BTS link is called the Abis interface which is cable or an optical fiber interface, and allows operation between components made by different suppliers.

The BTS is made up of the antenna and the radio transceivers. A BTS houses the radio ranceivers that define a cell, and handles the radio-link protocols with the Mobile Station. BSC manages the radio resources and handles radio-channel setup, frequency hopping, and handovers among a number of different cells.

The BSC connection between the MS and the Mobile service Switching Center (MSC) is done through the Translation and Adaptation Unit(TRAU). Usually, 20 to 30 BTS will be controlled by one BSC.

Mobile Station

The MS, both hand-held (or portables) and traditional mobiles, is carried by the subscriber. The MS is made up of the mobile equipment(ME), also known as the terminal, and a smart card known as the Subscriber Identity Module (SIM).

The mobile equipment is uniquely identified by the International Mobile Equipment Identity (IMEI).

The SIM card contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication, and other information. GSM subscriber information are not programmed on the mobile equipment but rather stored in a computer chip on the SIM card. The SIM card can be inserted into another GSM terminal, enabling the user to receive calls at that terminal, make calls from that terminal, and receive other subscribed services. This way personal mobility is provided as the user can have access to subscribed services irrespective of a specific terminals.

The SIM card provides subscriber account protection against unauthorized use by a password or personal identity number. The SIM provides assistance with voice and data encryption by deriving the variables for the encryption process.

Network Subsystem

The network subsystem includes the:

1) the Mobile Switching Center(MSC)
2) the Home Location Register(HLR)
3) the Visitor Location Register(VLR)
4) the Equipment Identity Register(EIR)
5) the Authentication Register(AUC)

The central component of the Network Subsystem is the MSC. It is an advanced electronic switch that provides all the functionality needed to handle a mobile subscriber,such as registration, authentication, location updating, handovers(mobility), and call routing to a roaming subscriber. The MSC also has the interface to other networks such as private land mobile networks, public switched telephone networks and integrated services digital

networks (ISDN). Signaling between functional entities in the Network Subsystem uses Signaling System Number 7 (SS7).

The MSC is connected to the HLR. Logically there is only one HLR per GSM network,although it may be implemented as a distributed database. 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. Each MSC will also have a VLR that 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. Usually the VLR is implemented together with the MSC, so that the geographical area controlled by the MSC corresponds to that controlled by the VLR. This way the signaling required is simplified.

The MSC is also connected to the EIR and the AUC. The EIR is a database that contains a list of all valid mobile equipment on the network. The Authentication Center is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and encryption over the radio channel.

Operations and Maintenance Center

The OMC is the command center for monitoring every part of the network. The system is equipped with alarms for all kinds of failures such as when a tower is being hit.

Operation Subsystem

The OSS contains contains al the parts of the network that are needed to run day to day operations. That includes the inventory systems, customer billing, and gateways totransport information.

A higher lever overview of the GSM network in a public local mobile network is shown in Figure 3.2.The diagram demonstrates how the different subsystems come together.

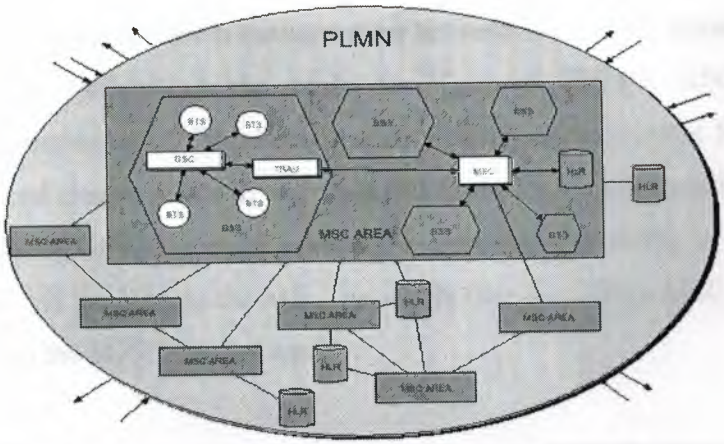


Figure 3.2 GSM view of a Public Local Mobile Network[1]

UM or Air Interface

The air interface is the central interface of every mobile system and typically the only one to which a customer is exposed. GSM utilizes a combination of frequency division multiple access(FDMA) and time division multiple access(TDMA).

Abis-Interface

The Abis-interface in the interface between the BTS and the BSC. It is a pulse code modulation(PCM) 30 interface. The transmission rate is 2.048 Mbps which is partitioned into 32 channels of 64 Kbps each. The compression techniques that GSM utilized packs up 8 GSM traffic channels into a single 64 Kbps channel.

A –Interface

On the physical level the A-interface consists of one or more pulse code modulation (PCM) links between the MSC and the BSC. Each one has a transmission capacity of 2 Mbps.

3.2.2 GPRS

GPRS is an addition to the existing GSM infrastructure. As a result the GPRS architecture is very similar to the GSM's. The existing GSM nodes are upgraded with GPRS functionality. The sametransmission links can be reused for both GSM and GPRS. eg the link between BSCs and BTSs.

The GSM network provided only circuit- switched services and thus two new network nodes were defined to give support for packet switching. This way packet data traffic separated from traditional GSM speech and data traffic. The two nodes are the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN)(see figure 3).

SGSN and GGSN are mobile aware routers and are interconnected via an IP backbone network.

The SGSN is responsible for the communication between the mobile station (MS) and the GPRS network. It carries out the basic functions of GSM'S BSC of providing authentication, ciphering and IMEI check, mobility management, logical link management towards the MS, and charging data. It also connects to the HLR, MSC,and BSC and handles packet data traffic of GPRS users in a geographical area. The traffic is routed from the SGSN to the BSC via the BTS to the MS. The SGSN like the GSM's MSC provides packet routing to and from the SGSN service area.

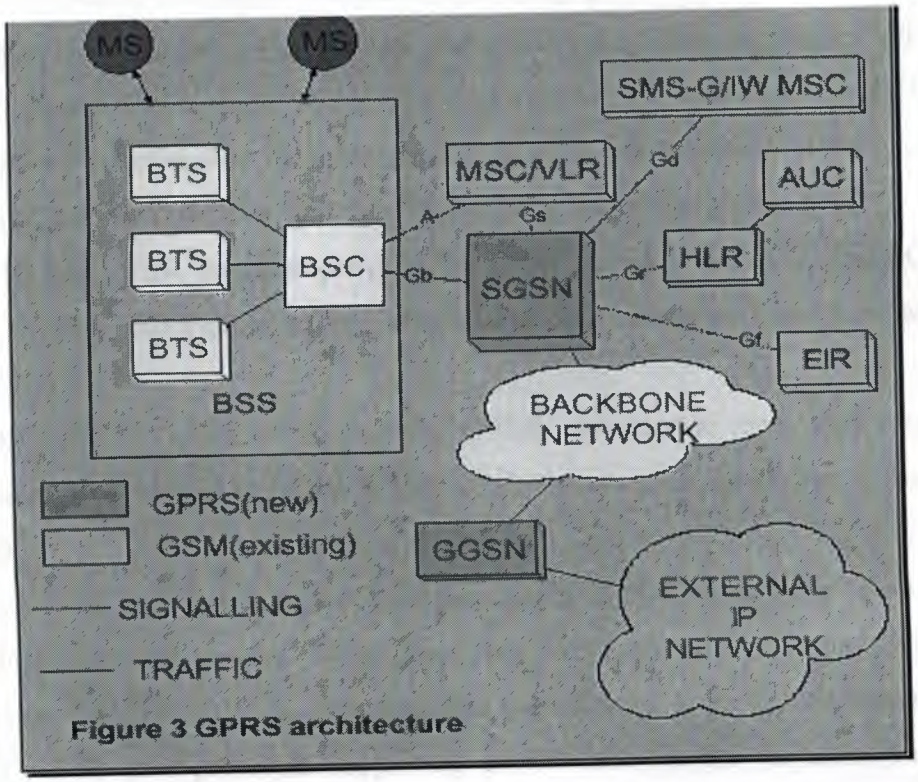


Figure 3.3 GPRS Architecture

The GGSN connects to outside data networks and to other GPRS networks. The GGSN provides the interface to external packet data networks like X.25 and external IP networks which are not supported by GSM. It routes incoming packets to the appropriate SGSN for a particular mobile station.

It also provides mobility management, access server functionality, and routing to the right SGSN and protocol conversion. The GPRS protocols are limited to just setting up an IP bearer, a logical link, between the MS and the Access Server. It translates data formats,

signaling protocols and address information permitting communication between the different networks and enabling compatibility with the GSM network. GGSN is a host owning all IP addresses of all subscribers served by the GPRS network thus replacing the functionality of GSM'S VLR.

GPRS uses the GSM'S BSS but with enhanced functionality to support GPRS(see figure 3.3). The GSM's BSS is used as a shared resource of both circuit switched and packet switched network elements to ensure backward compatibility and keep the requirements for the introduction of GPRS at a reasonable level.The main change that GPRS brought compared to GSM is the addition of the packet control unit (PCU) into the BSC which controls the packet channels, separating the data flows of circuit and packet switched data. Circuit switched data are send through the A-interface on the MSC whereas packet data are send to the SGSN into the GPRS backbone. The BSC of GSM is given new functionality for mobility management, for handling GPRS paging. The new traffic and signaling interface from the SGSN is terminated in the BSC.

GPRS uses the MSC/VLR interface provided by GSM, between the MSC and SGSN co-ordinated signaling for mobile stations which have both circuit switched and packet switched capabilities.

The HLR of GSM is modified to contain GPRS subscription data and routing information and is accessible from the SGSN. It also maps each subscriber to one or more GGSNS.

The HLR may be in a different PLMN than the current SGSN for roaming terminals. The GSM interfaces are re-used except that they are enhanced to support GPRS nodes(see figure 3.4). The existing Abis interface transmission towards BSC is reused. In the GSM's BTS new protocols supporting packet data for the air interface and functions for resource allocation for slot and channel allocation are implemented. GPRS uses the same pool of physical channels as speech. This way GPRS channels (PDCH) are mixed with circuit switched channels (TCH) in one cell. A TCH is allocated to one single user whereas several users can multiplex their traffic on one and the same PDCH.

NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Electrical and Electronic Engineering

MOBILE SWITCHING CENTER

Graduation Project
EE-400

Student: MOHAMMED AL MALLAHI (20001497)

Supervisor: Mr. Jamal Fathi

Lefkoşa-2005

ACKNOWLEDGMENT

First I want to thank Mr. jamal fathi to be my advisor. Under his gudance, I successfully overcome many difficulties and learn a lot about Mobile Communications. In each discussion, he explained my questions petiently, and I felt my quick progress from his advice. He always helps me a lot either in my study or my life. I asked him many questions in Electronics and Communication and he always answered my questions quickly and in detail.

I also want to thank my friend in NEU (UZUN-ABUMETLEQ-BATMAZ-ALBASHA-BATUMAN-SHAHEEN-BELAAL-ALAA-ABOSAMRA-ABUZAED-RAED-MAYAR-HATHAT-MESLEH-KOJOK) Begin with them make my years in NEU full of fun.

Finally, I want to thank my family, especially my parents. Without their endless support and love for me, I would never achieve my current position. I wish my mother lives happily always, and my father in palestine be proud of me.

LIST OF ABBREVIATIONS

AGCH Access Grant Channel

ATDMA Asynchronous TDMA

ATM Asynchronous Transfer Mode

BCCH Broadcast Control Channel

BSS Base Station System

BSSAP Base Station System Application Part

BSSMAP Base Station System Management Application Part

BTS Base Transceiver Station

BTSM Base Transceiver Station Management

CDMA Code Division Multiple Access

DTAP Direct Transfer Application part

EIR Equipment Identity Register

ES Earth Station

FACCH Fast Associated Control Channel

FCC Federal Communications Commission

FCCH Frequency Correction Channel

FDD Frequency Division Duplex

FDM Frequency Division Multiple Access

FDMA Frequency Division Access

FEC Forward Error Correction

GEO Geostationary

GMSC Gateway MSC

GMSK Gaussian Minimum Shift Keying

GOCC Ground Operator Control Central

GSM Global System For Mobile Communication

HLR HOME Location Register

IMEI International Mobile Equipment Identity

IMSI International Mobile Subscriber Identity

ISL Inter-Satellite Link

ISO International Standards Organization

IWF inter-Working Function

IWMSC Inter-Working Mobile Switching Center

LAPD Link Access Protocol For the ISDN D-channel

MEO Medium Earth Orbit

MS (GSM) Mobile Station

MSISDN MS ISDN (Integrated Services Digital Network) number

MSRN MS roaming number

MT (satellite) Mobile Terminal

MTP Message Transport part

OSI Open System Interconnect

PCH paging channel

PLMN Public Land Mobile Network

PSTN public switched Telephone Network

QPSK Quaternary Phase Shift Keying

RACH Random Access Channel

RF Radio Frequency

RPE/LTP Regular pulse Excited long Term (pitch) Prediction

RR Radio Recourse

SACCH Slow Associated Control Channel

SCCP Signaling Connection control part

SCH Synchronization Channel

SPCCH Stand-Alone Dedicated Control Channel

SDMA Sa\peace Division Multiple Access

SMS Short Message Service

SOCC Satellite Operations Control Contras

TCH Traffic Channel

TDD Time Division Duplex

TDMA Time Division Multiple Access

TRAU Transponder and Rate Adapter Unit

TT&C Telemetry, Tracking and Control

TX Transmit

UMTS Universal Mobile Telecommunications System

VLR Visitor Location Register

CONTENTS

ABSTRACT

The mobile switching center is one of the most important aspect in the mobile communication which is centered in the subsystem of the mobile network.

The main objective of this project is provide analysis and provides all the functionality needed to handle a mobile subscriber such as registration, authentication, Location updating, hand over (mobility), and call routing to a roaming subscriber which done using a mobile switching center.

For this purpose I start my project in general idea about mobile communications and then go to more specific section in mobiles which is GSM and after this I went to GSM architecture to explain the mobile switching area.

The MSC also has the interface to other networks such as private Land mobile networks, public switched telephone networks and integrated services digital networks (ISDN). The underling principle of MSC is based on controls the calls Setup, supervision and release and may interact with other nodes to successfully establish a call.

INDTRODUCTION

The mobile switching center is one of the most important aspects of the mobile communications. Mobile services Switching Center (MSC) is the main part of the Network Subsystem. It is performs the switching of calls between the mobile users, and between mobile and fixed network users.

The MSC also handles the mobility management operations. It acts like normal switching node of the PSTN or ISDN, and additionally provides all the functionality needed to handle a mobile subscriber

This project is aimed to provide analysis of MSC and to enhance where it use.

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

Chapter 1 introduces the basis of mobile communication system.

Chapter 2 presents an overview of Global System for Mobile Communications. In this Chapter, covers everything related to GSM. Like history of Gsm, services provided by GSM, GSM network architecture, Radio Link aspect and network aspect.

Chapter 3 studies the architecture and protocols of the GSM and make comparison with GPRS. In this chapter, I am attempt to go directly to the architecture of GSM and explain the GSM network to describe the area of MSC. And give other example to use MSC in the GPRS.

In chapter 4 it studies the mobile switching center, which covers the switching system, MSC function, Gat way MSC (GMSC), authentication procedure and service function.

CHAPTER 1

MOBILE COMMUNICATION SYSTEMS

1.1 Cordless Telephones

The cordless telephone consists of the base and portable units (see Figure 1.1). These units are linked by a low power PM system. The connecting wires of a conventional telephone between the portable unit and the base unit are replaced with low-power radio transmissions. Electronic circuits of the cordless telephone involve DTMF generators for dialing, electronic single -or dual -frequency ringers, and electronic speech circuits Cordless telephones are available with the same futures as the electronic telephones that use cords. The cordless telephone usually obtains the operating power directly from the telephone line. However, some cordless telephones, because of their greater power requirement, have to be plugged in to a household power source.

Figure 1.1 Cordless Telephone Units

This is a minor disadvantage since the cordless telephones do not operate if a utility power failure occurs. The cordless telephones have the following features.

1) Speech and volume control;

2) Security features to prevent unauthorized calling;

3) Keeping and displaying up to 50-100 incoming and outgoing calls;

4) Displaying the caller's phone number;

5) Displaying the date and time;

6) Recording the conversation;

7) Auto answering ability.

1.1.1 Base Unit

As shown in Figure 1.2 the base unit connects directly to the telephone line to complete local loop to the central office. The base unit transmits a frequency of 1.6 to 1.8 MHz. It uses AC power line that supplies the power for the base station electronics as well as works transmitting antenna. The nominal 1.7 MHz frequency modulated signal is fed from the base unit transmitter to the AC line through capacitors which block the line current, from the base transmitter while passing the 1.7 MHz output to the line. This uses of the house wiring, as antenna is not unique to cordless telephones. It also is used for wireless intercoms. This method provides good reception within and near the house as well as outside near power lines.

1.1.2 Portable Unit

An internal *lipstick antenna* (like that used in standard radio receivers) in the portable unit i receives the nominal 1. 7 MHz transmission from the base unit over a range from 50 to 1000 feet.

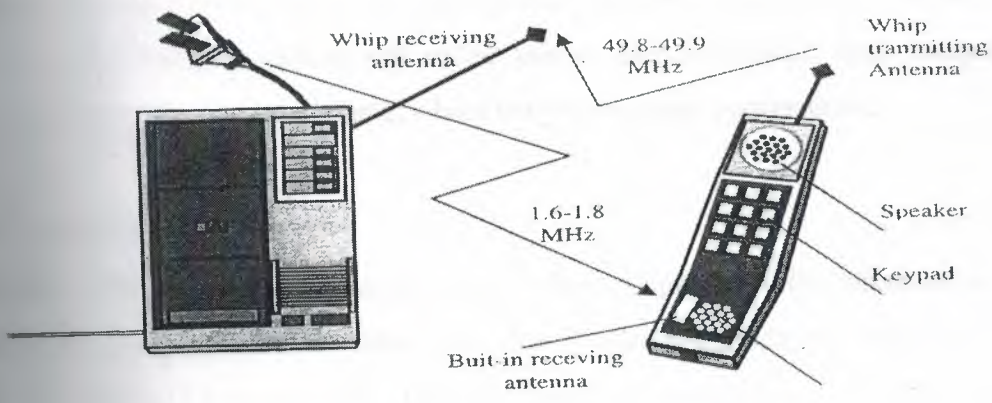


Figure 1.2 Portables Units

This range depends not only on the manufacturer's design, but also on such things as whether the house wiring is enclosed in metal conduct and weather foil -backed insulation is used in the walls. The ringing or voice signal is recovered by demodulation and drives the speaker in the portable unit. The portable unit is powered by a battery, which is recharged when placed in the receptacle in the base unit. The portable unit receives the locally radiated RF signal from the base unit's antenna (the house wiring) with its built -in lipstick antenna, much like a portable radio the portable unit is usually in a stand-by mode which corresponds to the on-hook condition of a telephone set. When the ringer sounds, the user operates on a talk switch, which as a result turns "on " the transmitter in the portable unit. This transmitter transmits a frequency in the range of 49.8 to 49.9 MHz and outputs the signal to the *whip antenna.* (Since the whip is used only for , transmission, it can be collapsed out of the way when the portable unit is on stand-by. If the r portable unit is only for voice transmission, it may have an internal antenna and its range is shorter). A similar whip antenna on the base unit receives the PM signal from the portable unit, demodulates it and applies the off -hook signal to the telephone local loop. Dialing transmits modulation tones to the base unit, which sends either tones or pulses over the telephone lines. After the two parties have been successfully connected, the transmitter and receiver operate simultaneously.

When the user dials the number for outgoing calls, the dial pulses produce tones, which modulate the carrier for transmission to the base unit. The base unit recovers the tones by demodulation. If DTMF service is used, the tones are sent on the telephone line. If pulse service is used the tones are converted to pulses and the telephone line is pulsed. When the connections between calling and called parties are established, both transmitters and receivers operate at the same time, which permits two-way conversation.

1.2 Mobile Telephones

Mobile telephones can be considered as cordless telephones with elaborated portable and base units. High-power transmitter and elevated antenna provide the radio carrier link over an area within 20 to 30 miles from the base station antennas. Using the multiplexing, detecting, and selecting features it is possible to provide simultaneously service up to 60

subscribers per ease station. This is the major difference between cordless telephones and mobile telephones.

1.2.1 Base Unit

The base station can transmit and receive on several different frequencies simultaneously, to provide several individual channels for use at the same time. The radio base station transmitter's output power is typically 500 watts. The mobile telephone base unit can operate on many channels simultaneously and can easily cover the average city with a power of several 100 watts. It covers a circular area of up to 30 miles in radius for clear reliable communications, but transmitters with the same frequency are not spaced closer than about 60 to 100 miles because of the noise interference levels.

The base unit receiver contains the necessary electronics to present its control terminal with a good audio signal. The control terminal interfaces the voice and control signals to the standard telephone circuits. The receiver contains filters, high -gain amplifiers, and demodulators to provide a useable voice signal to the telephone line. The control terminal contains the necessary detector and timing and logic circuits to control the transmissions link between the base unit and mobile units. The control terminal has the necessary interface circuits so that a call initiated at a mobile unit is interconnected through the national or international telephone system to the called party just as any other telephone call.

The national and international telephone system facilities are owned by the respective telephone companies. The base units and the mobile units may be owned by the Telephone Company or by a separate company called a Radio Common Carrier (RCC).

1.2.2 Mobile Unit

The mobile unit contains a receiver, a transmitter, control logic, control unit, and antennas. For the user it operates pretty much like and ordinary electronic telephones. Figure 1.3 shows the modern mobile telephones layouts.

Figure 1.3 The Modern Mobile Telephones Layouts

Mobile telephone communication setup is shown in Figure 1.4. The mobile unit in the user's vehicle consist of a receiver containing amplifiers, a mixer and a demodulator; a transmitter containing a modulator, carrier oscillators and amplifiers; the necessary control logic; a control unit with microphone, speaker, key pad and switches; antennas and the interconnecting cables. The control units perform all of the functions associated with normal telephone use. The mobile telephone user places and receives the calls in the same manner as with an ordinary telephone. When the hand set is lifted to place a call, the radio unit automatically selects an available channel. If no channel is available, the busy light comes on. If a channel is found, the user hears the normal dial tone from the telephone system, and can then dial the number and proceed as if the telephone was direct wired. An incoming call to the mobile unit is signaled by a ringing tone and is answered simply by lifting the handset and talking. Thus the automatic mobile telephone is as easily used as a home telephone. The mobile telephone combines the mobility of the radio link and the world -wide switched network of the existing telephone system to provide a communication link to any other telephone in the world.

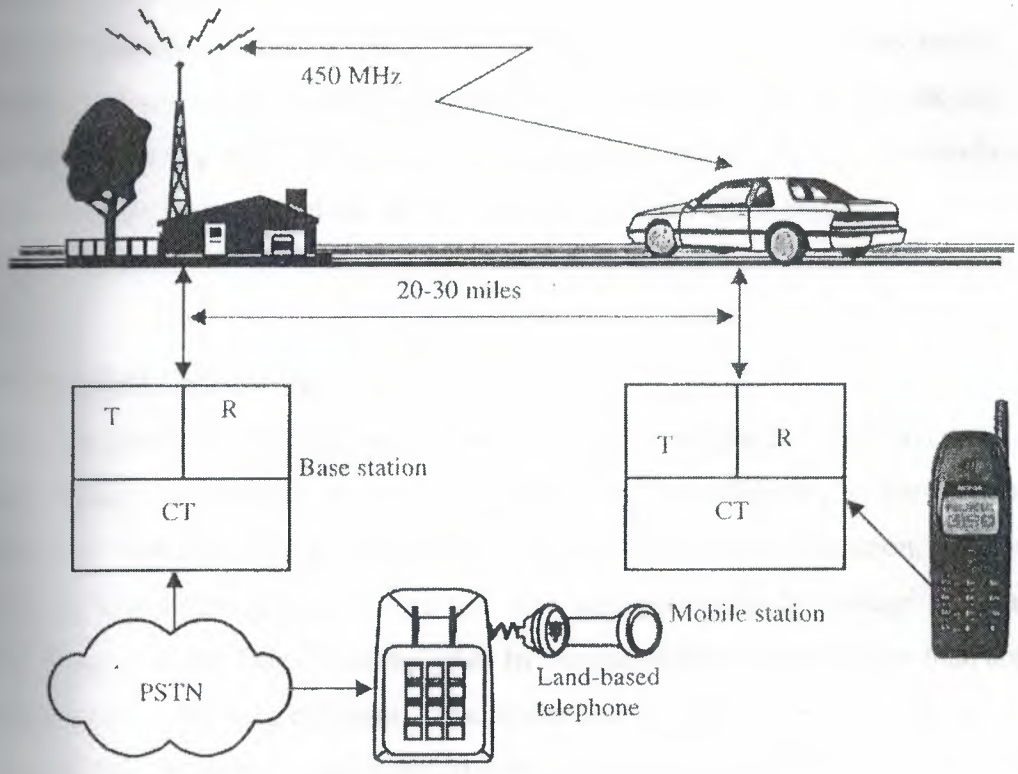


Figure 1.4 Mobile Telephone Communication Setup

1.3 Home Area and Roaming

As previously stated, the mobile system is designed for optimum use within a 20-30 miles radius of the base antenna. This is called the subscriber's home area and a subscriber usually would remain in the home area. However if the subscriber moves out of the home area into another area, the subscriber is referred to as a roamer and a different mode of operation applies. Each mobile telephone has a unique telephone number, which includes the home area's base station identification. When someone calls the mobile unit the calling party is connected first to the transmitter serving the subscriber's home area. As long as the subscriber is within radio range of that system, all is well; otherwise, the base station won't get an answer from the mobile unit and the caller will get a no-answer signal. If the subscriber roams outside the home area, he / she can still be reached if a similar mobile

telephone system exist in that area, provided proper advance arrangements have been made. If a subscriber goes outside the range of his base station, his mobile telephone can only reached through another similar adjacent mobile base station system.

Calls to roamers are usually placed by calling special number for the mobile service operator who knows the roamer's location. The operator manually patches the call through base station serving the area of the roamer's location. Some systems can not handle roamers due to overload of their channels, and some system doesn't allow roamers.

1.4 Detailed Operation

Different signaling techniques have to used in a mobile telephone system in contrast with a wired facility. Since there are no wires connecting the telephone to the network, both speech and signaling must be transmitted via radio. For wireless operation, tones are used for those signaling functions, which are otherwise performed by voltage and current in hard- wired systems. This is accomplished by' the use of special tones rather than applying a voltage level or detecting a current.., The proper tone transmitted to the mobile unit will, for example, ring the mobile: telephone to indicate an incoming call just as with a standard telephone different tone is used to indicate off -hook, busy, etc. The Improved Mobile Telephone System (IMTS) uses in-band signaling tones from 1300Hz to 2200Hz. The older Mobile Telephone System (MTS) had in-band signaling tones in the 600 Hz to 1500 Hz range. Some systems use 2805 Hz as manual operation.

Incoming Call

To gain a better understanding of the system operation, conceder an incoming call from a facility subscriber through the base unit to a mobile unit. The base station controls all activity on all channels. It selects only one idle channel and places a 2000 Hz idle tone (1) as shown Figure 1.5. All on-hook mobile units that are turned on automatically search for the idle tone and lock or the idle channel because this is the channel over which the next call in either direction will be completed. After locking on the idle channel, all on-hook mobile units "listen" to their numbers that channel. When an idle channel becomes busy for a call in either direction, the base station, control terminal selects another unused channel

before. If the mobile does not answer within 45 seconds, ringing (6) is discontinued and the call abandoned. When the mobile subscriber goes off-hook to answer, the mobile supervisory unit sends a burst of connect tone (1633 Hz) as an answer signal (8). Upon receipt of the answer signal, the control terminal stops the ringing and establishes a talking path between the calling circuit and the radio channel (7). When the subscriber hangs-up (8) at the end of call, the mobile supervisory unit sends disconnect signal (12) alternating the disconnect tone (1336 Hz) and the guard tone. The mobile supervisory unit then turns of the mobile transmitter and begins searching for the market idle channel. Each on-hook mobile unit receiving the number transmission compares the received number to its unit number. Only the one mobile unit with a number match remains locked on that channel.

Outgoing Call

The sequence for a call originated by a mobile subscriber is illustrated by Figure 1.6. When the subscriber goes off-hook to place the call, the mobile unit must be locked on the marked-idle channel. If not, the handset will be inoperative and the busy lamp on the control unit will light, indicating to the subscriber that no channel is available. If the mobile unit is locked on the marked idle channel, the mobile supervisory unit will turn on the mobile transmitter to initiate the acknowledgment or handshake sequence. Then mobile unit transmits its own number so the control terminal can identify it as a subscriber and can charge the call to the number. The reaming functions of Figure 1.6 (b) are similar to those of Figure 1.5. When a call is originated from the field, the mobile unit finds a marked idle channel and broadcasts an acknowledgment to the base by sending its identification. The mobile unit than completes a call in the usual manner by receiving a dial tone, then dialing the number and waiting for the called party to answer.

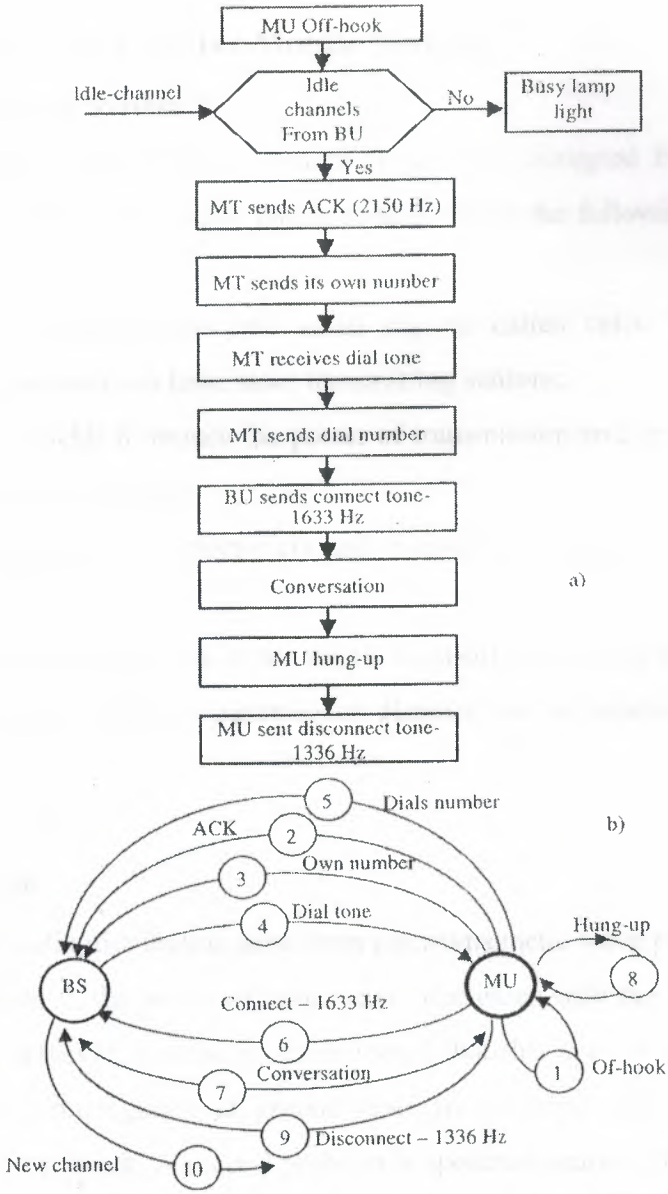


Figure 1.6 The Sequence for a Call Originated by a Mobile Subscriber.

1.5 The Architecture of the Cellular Mobile System

What Is a Cellular Telephone System?

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

1) Division of heavily populated areas into small regions called cells. In this way, concentrated I 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 inure acceptable value.

1.6 Cellular Coverage

The major problems with radio distribution arise from electromagnetic wave propagation. As mentioned in the chapter 1, 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 abase 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.

Cluster. The cells are grouped into clusters. The number of cells in cluster must be determined so that the cluster can be reputed 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 neighboring clusters. This interference is produced by the small size of the clusters (the size of the cluster is defined by the number of cells per cluster). The total number of channels per cell depends on the number of available channels and the type of cluster used.

There are following types of cells: macro cells, micro cells, selective cells, and umbrellas, Macrocells. The macrocells are large cells for remote and sparsely populated areas. **Microcell**s. These cells are used for densely populated areas. By splitting the existing areas smaller cells, the number of channels available are increased as well as the capacity of the. The power level of the transmitters used in these cells is then decreased, reducing the possibility of interference between neighboring cells.

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

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

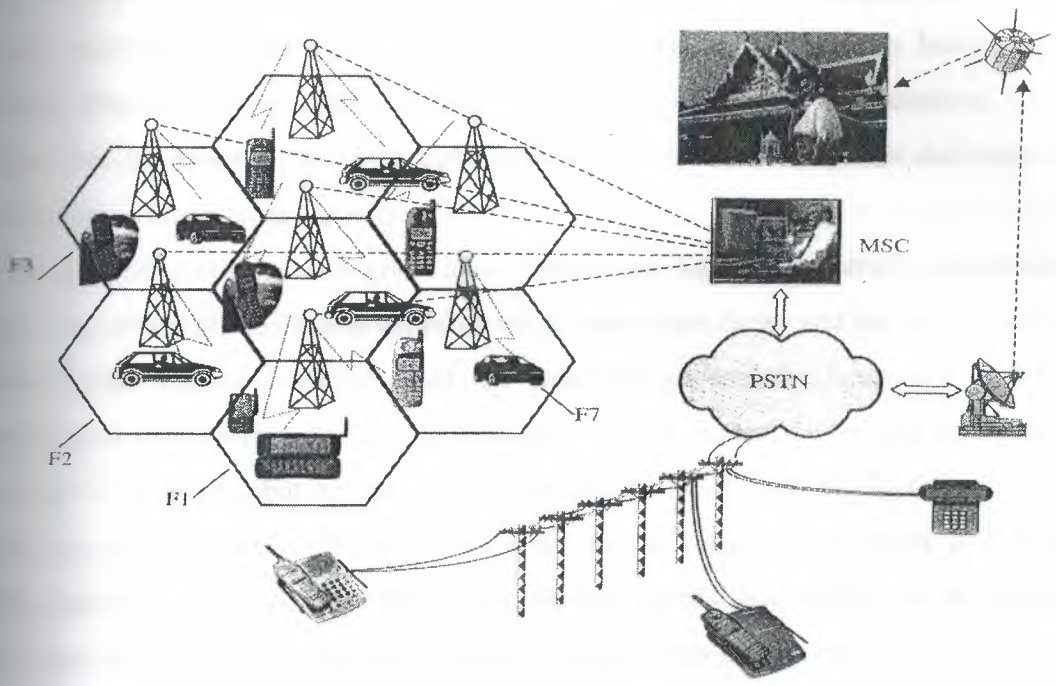


Figure 1.7 The Cellular Setup

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 center 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 diagram operates on a different frequency, denoted by Fl, F2. ..F7. In the Global System of Mobile Communication (GSM), the design was aimed at the beginning at medium-sized cells, of a diameter expressed in kilometres or tens of kilometers. Yet, the lower boundary is difficult to determine; cells of more than one kilometers 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 kilometres. 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 exists 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 1.7.

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 PM 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 telephone 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 telephone.

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.

1.6.1 Setting up a Cellular Telephone Call

When a phone call comes into the cellular system from the conventional telephone switched network PSTN or from another cellular telephone, the computer-based Mobile Switching Centre MSC follows the three steps depicted in Figure 1.8 in setting up the proper connection. In step 1 an appropriate paging message is directed by MSC to all the base stations BS. In the step 2 appropriate cellular telephone acknowledges (Figure 1.8 (b)) the page by sending digital pulse-train, back to the base station from which a signal came. In step 3 the base static automatically selects and activates a duplex voice channel to handle the call, then sign appropriate cellular telephone for transmission and reception (see Figure 1.8 (c)).

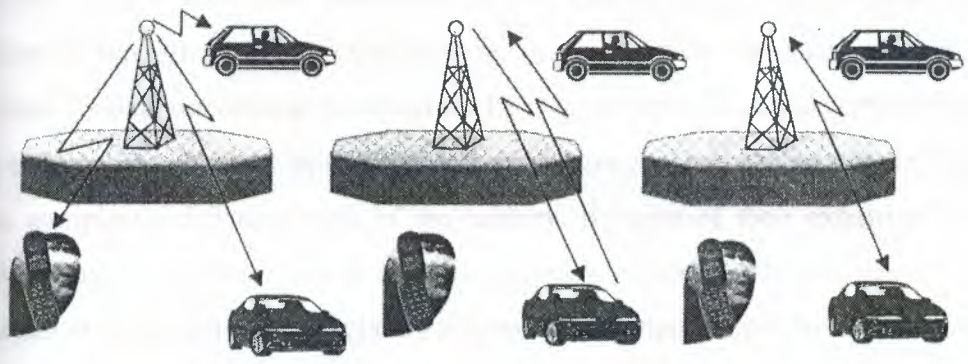


Figure 1.8 Setting up a Cellular Telephone Call

1.6.2 Roamers

The system is designed to make handling of roamers automatic. This is the principal goal the cellular approach. Locating and hand-off are the concept that comes directly from the use 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 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 Telephone 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 countryside toward a city, continue through the city's downtown, and not hang up until 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 Mobile Telephone Switching Center MSC a specifically designed computer telecommunications facility that sets up the pro connections, keeps the track of billing charges, and automatically handles any necessary hand-o Hand-offs to anew base station are attempted whenever the signal quality degrades as users travel through the cellular telephone coverage area from one cell to another.

Trunk lines connect the cellular switch to the PSTN, and from the mobile cellular telephone system can originate from or be directed toward ordinary telephones or cellular telephones local in completely different parts of the country. Because of their extensive frequency reuse in a small local area, cellular telephone systems can handle a multitude of users. In most urban areas government regulators maintain 'the proper competitive environment by licensing two separate cellular telephone 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 telephone to a. mobile unit, which has roamed, to another metropolitan area presents additional problems. While 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 be 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 unauthorized disclosure of the service area to which the mobile unit has roamed.

1.6.3 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 telephone 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 does this. Each transmitter covers only its own cell, and cells sufficiently far apart 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 is shown in Figure 1.9. 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 cell, and by not using the same frequency in adjacent cells. The cellular system can be -handed because cell splitting may occur as demand increases.

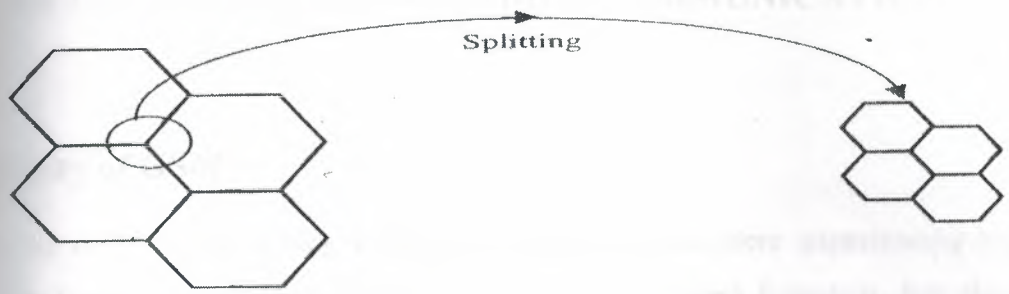


Figure 1.9 The principle of the cell splitting.

The spectrum scarcity is circum vented 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. total system throughput can, therefore, be increased by reducing the cell size.

The world's most popular cellular telephone systems was AMPS (Advanced Mob' Telephone System), developed in the United States, and TACS (Total Access Cellular System 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 AMPS system, TACS uses FM analog voice-channel modulations with digital frequency shi keying for the control channels.

CHAPTER 2

GLOBAL SYSTEM FOR MOBILE COMMUNICATION

2.1 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. 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 Groupe Spécial Mobile (GSM) to study and develop a pan-European public land mobile system. The proposed system had to meet certain criteria:

1) Good subjective speech quality

2) Low terminal and service cost

3) Support for international roaming

4) Ability to support handheld terminals

5) Support for range of new services and facilities

6) Spectral efficiency

7) ISDN compatibility

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. 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 interworking 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.

2.2 Services provided by GSM

From the beginning, the planners of GSM wanted ISDN compatibility in terms of the services offered and the control signalling 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, teleservices, and supplementary services. The most basic teleservice 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 interwork 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 bidirectional 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 teleservices 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.

2.3 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 Mobile Station is carried by the subscriber. The Base Station Subsystem controls the radio link with the Mobile Station. The Network Subsystem, the main part of which is the Mobile services Switching Center (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 Um 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.

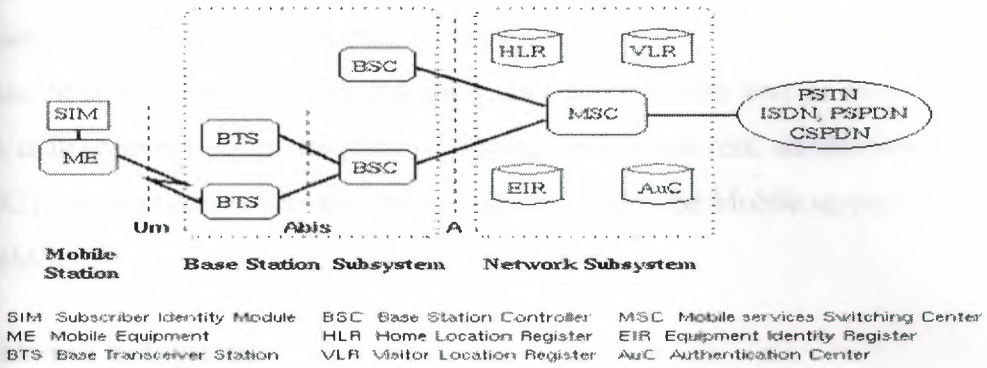


Figure 2.1 General architecture of a GSM network

2.3.1 Mobile Station

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

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

2.3.2 Base Station Subsystem

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

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

2.3.3 Network Subsystem

The central component of the Network Subsystem is the Mobile services Switching Center (MSC). It acts like a normal switching node of the PSTN or ISDN, and 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 conjuction 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). Signalling between functional entities in the Network Subsystem uses Signalling System Number 7 (SS7), used for trunk signalling 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 signalling address of the VLR associated with the mobile station. The actual routing procedure will be described later. There is logically one HLR per GSM network, although it may be implemented as a distributed database.

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

The other two registers are used for authentication and security purposes. The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile

equipment on the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI). An IMEI is marked as invalid if it has been reported stolen or is not type approved. The Authentication Center (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.

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.

2.4.1.1 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 2.2). 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).

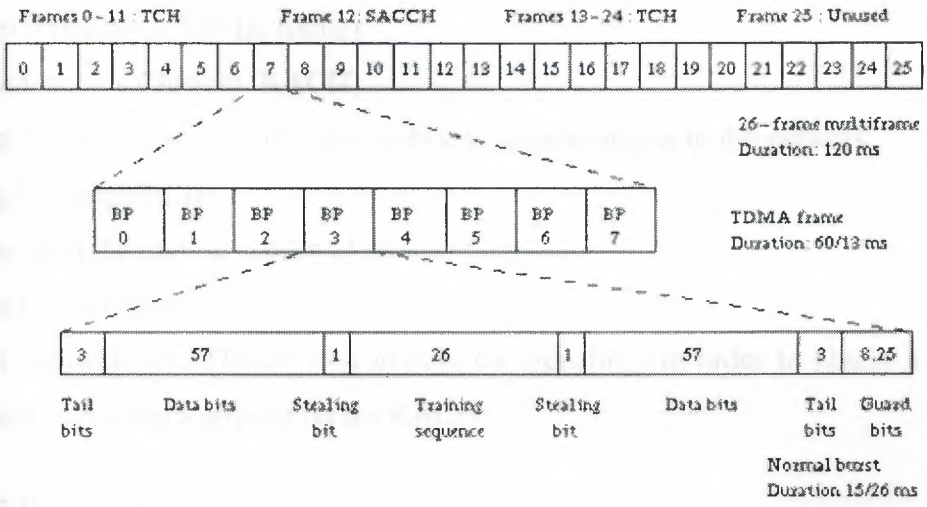


Figure 2.2 Organization of bursts, TDMA frames, and multiframes for speech and data

2.4.1.2 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 signaling 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 Synchronization Channel (SCH)

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

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 signaling (in order to obtain a dedicated channel), following a request on the RACH.

2.4.1.3 Burst structure

There are four different types of bursts used for transmission in GSM . The normal burst is used to carry data and most 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 convolution 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:

1) **Class Ia** 50 bits - most sensitive to bit errors

2) **Class Ib** 132 bits - moderately sensitive to bit errors

3) **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 Network aspects

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 protocol.

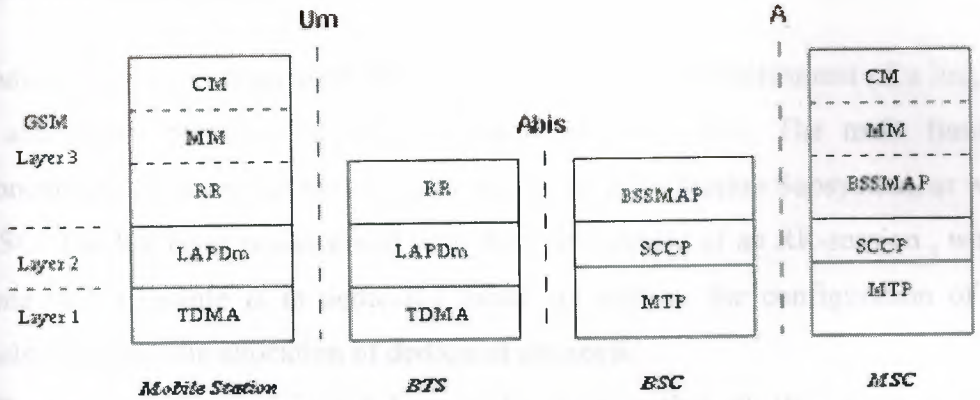


Figure 2.3 Signaling protocol structure in GSM

The signaling protocol in GSM is structured into three general layers , depending on the interface, as shown in Figure 2.3. 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 Signaling System Number 7 is used. Layer 3 of the GSM signaling 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.

Connection Management

Handles general call control, similar to CCITT Recommendation Q.931, 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 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.

2.5.1.1 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:

1) Channels (time slots) in the same cell

2) Cells (Base Transceiver Stations) under the control of the same Base Station Controller (BSC),

3) Cells under the control of different BSCs, but belonging to the same Mobile services Switching Center (MSC), and

4) 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.

2.5.2 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.

2.5.2.1 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.

2.5.2.2 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.

2.5.3 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.

2.5.3.1 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 (see the location updating section). 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 Figure2.4).

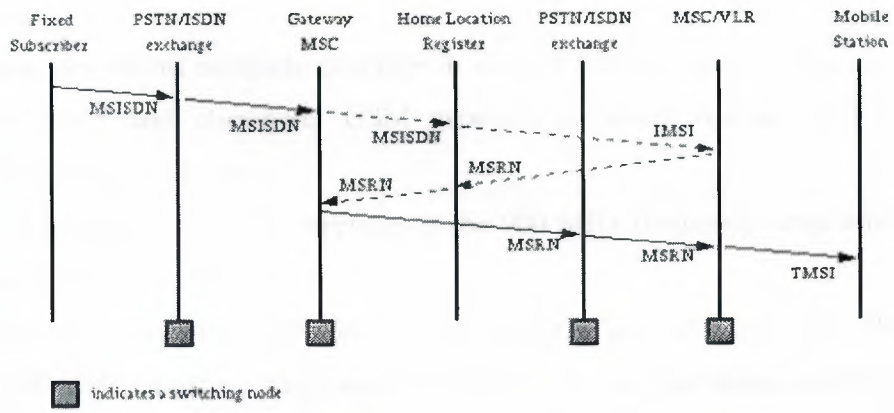


Figure 2.4. Call routing for a mobile terminating call

CHAPTER 3

OVERVIEW AND COMPARISON OF THE ARCHITECTURE AND PROTOCOLS OF THE GSM AND THE GPRS

3.1 Overview of Wireless Wide Area Network

3.1.1 GSM

GSM is a wireless platform that uses radio frequencies, and this way users can be fully mobile, and do wireless data computing anywhere, without worrying about adapters,telephone jacks, cables, etc. The unique roaming features of GSM allow cellular subscribers to use their services in any GSM service area in the world in which their provider has a roaming agreement. GSM-enabled phones have a "smart card" inside called the Subscriber Identity Module (SIM). The SIM card is personalized to the user. It identifies the user's account to the network and provides authentication, which allows appropriate billing.

GSM has been designed for speech services. It uses circuit switched transmission,reserving one radio channel for the user's traffic. It also uses cells which enables it to reuse different frequencies.

GSM, provides almost complete coverage in western Europe, and growing coverage in the Americas, Asia and elsewhere. GSM networks presently operate in three different frequency ranges. These are:

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

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, UK, and Russia.

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.

GSM standard circuit is a digital data bearer service offering 9.6kb/s. This data transmission in these networks is regarded as too slow and often too expensive for many applications. The cost is the total time that the user occupied that channel eventhough he was using the channel all the time. The performance of services such as Internet Applications in a cellular environment is typically characterized by the low available bandwidth, and an inefficient use of the rare air link capacity. Furthermore, long connection setup delay is a problem for bursty services requiring occasional data transfers.

3.1.2 GPRS

GSM's use of circuit switched systems meant that in the case of bursty traffic, the traffic channel will be idle for some time. As the demand for data services increased, GPRS was developed to support packet switching . The work on the GPRS specification began in 1994 as a part of GSM phase 2+ specification. GPRS is a separate packet data network within GSM which provides a packet base platform both for the data transfer and signaling. GPRS is compatible with the GSM architecture. Voice and GPRS services coexist in the same environment with the minimum changes in the system[8].

GPRS focused strongly on the development of a service, which overcomes these drawbacks of a mobile Internet Access. It allows allow reduced connection setup-times,supports existing packet oriented protocols like X.25 and IP, and provides an optimized usage of radio resources.

The main idea is to allocate resources depending on the GPRS demand. This feature operates in a capacity-on-demand mode. The capacity-on-demand concept has been introduced in order to keep compatibility with the existing GSM circuit-switched resources. Resources for GPRS may be dynamically allocated depending on how many users require them with a given quality of service and depending also on how many resources are available at the moment. The operator can decide whether to permanently dedicate some physical resources for GPRS. Load supervision is carried out in the MAC layer to monitor the load of the GPRS physical resources, and it's the function that will allow increasing or decreasing the number of allocated resources according to the existing demand. The operator has also the choice to dedicate temporarily physical resources for GPRS as long as no other higher-priority GSM services require them[8].

Since GPRS is packet oriented it enables volume based charging in contrast to GSM like charging of online time. It therefore allows users to stay constantly online while only paying for the occasional data transfer. Another important factor is the Quality of Service (QoS) offered by these services. The QoS can be negotiated when starting the session and can be renegotiated if it is required. The QoS agreed between the user and the network can be used to charge the service.

In addition, GPRS increases the capacity of the system and reduces the idle periods of the radio channels. This is done by allowing for multiple users per physical channel and using a channel only when it is needed, and releasing it immediately after the transmission is complete.

3.2 Architecture Comparison

This section analyzes the GSM architecture first, as it was the base upon which GPRS was uilt. GPRS architecture is then described while at the same time any differences/similarities are stated.

3.2.1 GSM

A GSM network is composed of several subsystems whose functions and interfaces are specified. Figure 3.1 shows the layout of a generic GSM network. These are the:

1) base station subsystem(BSS)

2) mobile station(MS)

3) network and switching subsystem(NSS)

4) operations subsystem(OSS)

5) operations and maintenance Center(OMC)

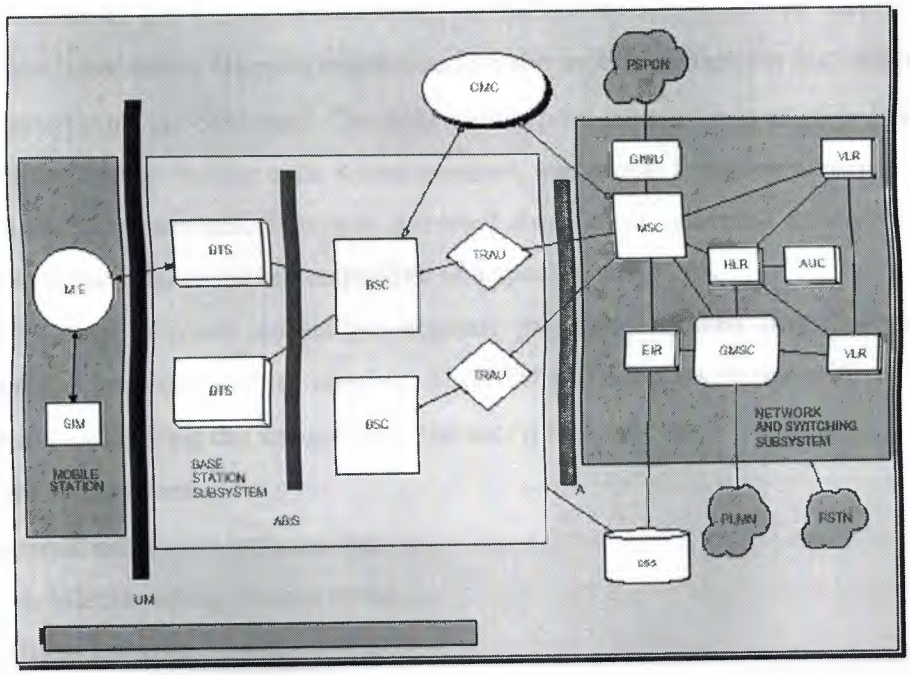


Figure 3.1 GSM Arcitecture [1][3][12]

Base Station Subsystem

The Base Station Subsystem controls the radio link with the Mobile Station. It is mainly composed of the Base Transceiver Station (BTS) and the Base Station Controller (BSC).

The BSC-to-BTS link is called the Abis interface which is cable or an optical fiber interface, and allows operation between components made by different suppliers.

The BTS is made up of the antenna and the radio transceivers. A BTS houses the radio ranceivers that define a cell, and handles the radio-link protocols with the Mobile Station. BSC manages the radio resources and handles radio-channel setup, frequency hopping, and handovers among a number of different cells.

The BSC connection between the MS and the Mobile service Switching Center (MSC) is done through the Translation and Adaptation Unit(TRAU). Usually, 20 to 30 BTS will be controlled by one BSC.

Mobile Station

The MS, both hand-held (or portables) and traditional mobiles, is carried by the subscriber. The MS is made up of the mobile equipment(ME), also known as the terminal, and a smart card known as the Subscriber Identity Module (SIM).

The mobile equipment is uniquely identified by the International Mobile Equipment Identity (IMEI).

The SIM card contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication, and other information. GSM subscriber information are not programmed on the mobile equipment but rather stored in a computer chip on the SIM card. The SIM card can be inserted into another GSM terminal, enabling the user to receive calls at that terminal, make calls from that terminal, and receive other subscribed services. This way personal mobility is provided as the user can have access to subscribed services irrespective of a specific terminals.

The SIM card provides subscriber account protection against unauthorized use by a password or personal identity number. The SIM provides assistance with voice and data encryption by deriving the variables for the encryption process.

Network Subsystem

The network subsystem includes the:

1) the Mobile Switching Center(MSC)
2) the Home Location Register(HLR)
3) the Visitor Location Register(VLR)
4) the Equipment Identity Register(EIR)
5) the Authentication Register(AUC)

The central component of the Network Subsystem is the MSC. It is an advanced electronic switch that provides all the functionality needed to handle a mobile subscriber,such as registration, authentication, location updating, handovers(mobility), and call routing to a roaming subscriber. The MSC also has the interface to other networks such as private land mobile networks, public switched telephone networks and integrated services digital

networks (ISDN). Signaling between functional entities in the Network Subsystem uses Signaling System Number 7 (SS7).

The MSC is connected to the HLR. Logically there is only one HLR per GSM network,although it may be implemented as a distributed database. 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. Each MSC will also have a VLR that 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. Usually the VLR is implemented together with the MSC, so that the geographical area controlled by the MSC corresponds to that controlled by the VLR. This way the signaling required is simplified.

The MSC is also connected to the EIR and the AUC. The EIR is a database that contains a list of all valid mobile equipment on the network. The Authentication Center is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and encryption over the radio channel.

Operations and Maintenance Center

The OMC is the command center for monitoring every part of the network. The system is equipped with alarms for all kinds of failures such as when a tower is being hit.

Operation Subsystem

The OSS contains contains al the parts of the network that are needed to run day to day operations. That includes the inventory systems, customer billing, and gateways totransport information.

A higher lever overview of the GSM network in a public local mobile network is shown in Figure 3.2.The diagram demonstrates how the different subsystems come together.

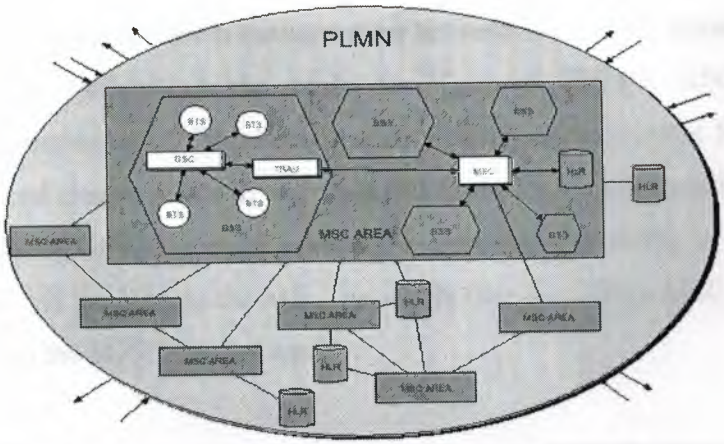


Figure 3.2 GSM view of a Public Local Mobile Network[1]

UM or Air Interface

The air interface is the central interface of every mobile system and typically the only one to which a customer is exposed. GSM utilizes a combination of frequency division multiple access(FDMA) and time division multiple access(TDMA).

Abis-Interface

The Abis-interface in the interface between the BTS and the BSC. It is a pulse code modulation(PCM) 30 interface. The transmission rate is 2.048 Mbps which is partitioned into 32 channels of 64 Kbps each. The compression techniques that GSM utilized packs up 8 GSM traffic channels into a single 64 Kbps channel.

A –Interface

On the physical level the A-interface consists of one or more pulse code modulation (PCM) links between the MSC and the BSC. Each one has a transmission capacity of 2 Mbps.

3.2.2 GPRS

GPRS is an addition to the existing GSM infrastructure. As a result the GPRS architecture is very similar to the GSM's. The existing GSM nodes are upgraded with GPRS functionality. The sametransmission links can be reused for both GSM and GPRS. eg the link between BSCs and BTSs.

The GSM network provided only circuit- switched services and thus two new network nodes were defined to give support for packet switching. This way packet data traffic separated from traditional GSM speech and data traffic. The two nodes are the Serving GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN)(see figure 3).

SGSN and GGSN are mobile aware routers and are interconnected via an IP backbone network.

The SGSN is responsible for the communication between the mobile station (MS) and the GPRS network. It carries out the basic functions of GSM'S BSC of providing authentication, ciphering and IMEI check, mobility management, logical link management towards the MS, and charging data. It also connects to the HLR, MSC,and BSC and handles packet data traffic of GPRS users in a geographical area. The traffic is routed from the SGSN to the BSC via the BTS to the MS. The SGSN like the GSM's MSC provides packet routing to and from the SGSN service area.

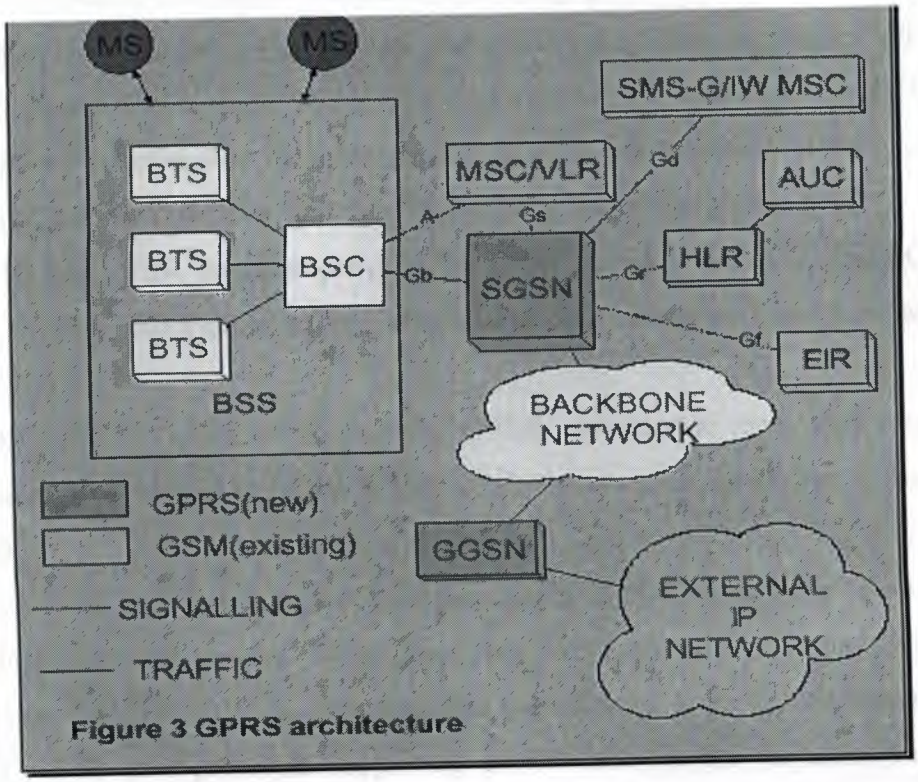


Figure 3.3 GPRS Architecture

The GGSN connects to outside data networks and to other GPRS networks. The GGSN provides the interface to external packet data networks like X.25 and external IP networks which are not supported by GSM. It routes incoming packets to the appropriate SGSN for a particular mobile station.

It also provides mobility management, access server functionality, and routing to the right SGSN and protocol conversion. The GPRS protocols are limited to just setting up an IP bearer, a logical link, between the MS and the Access Server. It translates data formats,

signaling protocols and address information permitting communication between the different networks and enabling compatibility with the GSM network. GGSN is a host owning all IP addresses of all subscribers served by the GPRS network thus replacing the functionality of GSM'S VLR.

GPRS uses the GSM'S BSS but with enhanced functionality to support GPRS(see figure 3.3). The GSM's BSS is used as a shared resource of both circuit switched and packet switched network elements to ensure backward compatibility and keep the requirements for the introduction of GPRS at a reasonable level.The main change that GPRS brought compared to GSM is the addition of the packet control unit (PCU) into the BSC which controls the packet channels, separating the data flows of circuit and packet switched data. Circuit switched data are send through the A-interface on the MSC whereas packet data are send to the SGSN into the GPRS backbone. The BSC of GSM is given new functionality for mobility management, for handling GPRS paging. The new traffic and signaling interface from the SGSN is terminated in the BSC.

GPRS uses the MSC/VLR interface provided by GSM, between the MSC and SGSN co-ordinated signaling for mobile stations which have both circuit switched and packet switched capabilities.

The HLR of GSM is modified to contain GPRS subscription data and routing information and is accessible from the SGSN. It also maps each subscriber to one or more GGSNS.

The HLR may be in a different PLMN than the current SGSN for roaming terminals. The GSM interfaces are re-used except that they are enhanced to support GPRS nodes(see figure 3.4). The existing Abis interface transmission towards BSC is reused. In the GSM's BTS new protocols supporting packet data for the air interface and functions for resource allocation for slot and channel allocation are implemented. GPRS uses the same pool of physical channels as speech. This way GPRS channels (PDCH) are mixed with circuit switched channels (TCH) in one cell. A TCH is allocated to one single user whereas several users can multiplex their traffic on one and the same PDCH.

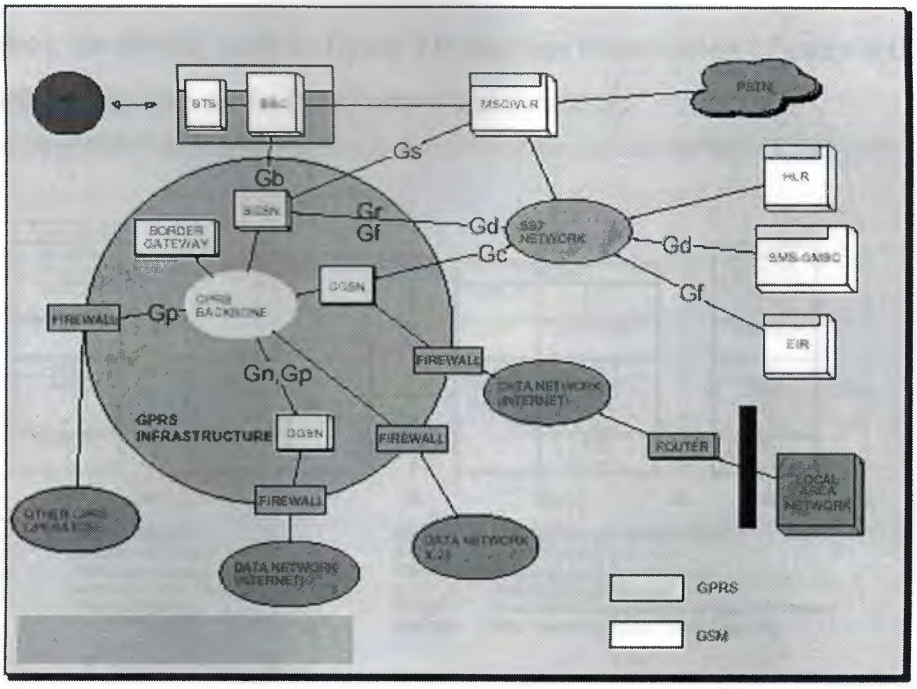


Figure 3.4 GPRS Infrastructure

.3 GSM and GPRS PROTOCOLS

his section compares the protocols stacks of both systems. This is done by briefly ntroducing the systems' protocol stacks and then analyzing the differences and/or imilarities.

he signaling protocol in GSM is structured into three general layers, depending on the nterface, as shown in Figure 3.5.

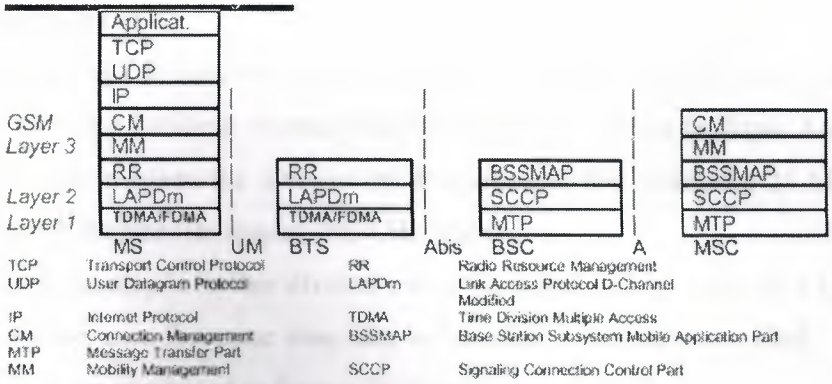


Figure 3.5 GSM Protocol Stack[12]

The protcol stack for GPRS, show in figure 3.6 provides transmission of users data and its associated signaling such as for flow control and detection.

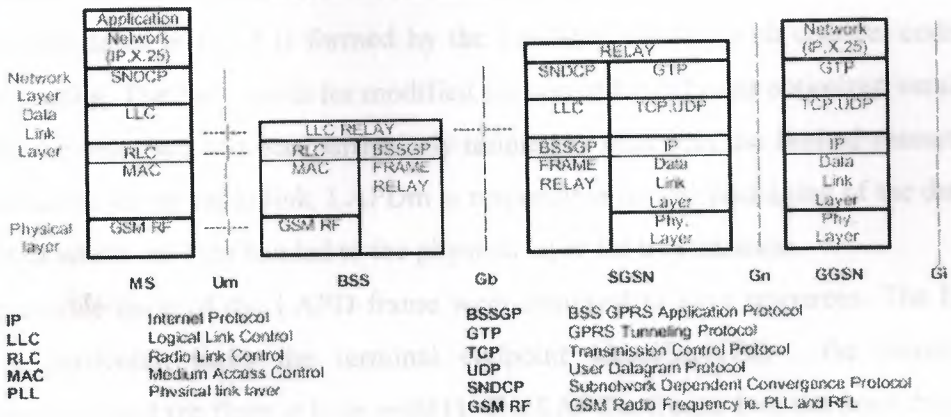


Figure 5.6 GPRS Protocol Stack[2]

3.3.1 Physical Layer

In both systems the physical layer between MS and BSS is divided into the two sublayers: the physical link layer (PLL) and the physical RF Layer (RFL).

The PLL provides a hysical channel between the MS and the BSS. Its tasks include channel coding (detection of transmission errors, forward error correction (FEC), indication of uncorrectable odewords), interleaving, and detection of physical link congestion. The RFL operates below the PLL.

Among other things, it includes modulation and demodulation.GSM uses a combination of Frequency Division Multiple Access (FDMA) and Time ivision Multiple Access (TDMA). The FDMA part involves the division by frequency of the maximum 25 MHz bandwidth into 124 carrier frequencies spaced 200 kHz apart.

Each carrier frequency is further divided into 8 time slots, which make up a TDMA frame. A mobile station uses the same time slot in both the uplink and downlink. A group of 26 TDMA frames are combined to form a 26-frame multiframe[12].

GPRS is compatible with the standard TDMA scheme of GSM. With GPRS mobile stations can use more than one time slot within the same TDMA frame.

It also uses a 52-frame multiframe compared to the 26-frame multiframe used by GSM.

3.2 Link Layer

n the air interfaces between the two systems there are a lot of different protocols. The SM system uses LAPDm whereas GPRS uses LLC and RLC/MAC.

ne data link layer in GSM is formed by the LAPDm together with channel coding and rst formatting. The "m" stands for modified version of LAPD is an optimized version for e GSM Air-Interface and was particularly tailored to deal with the limited resources and e peculiarities of the radio link. LAPDm is responsible for the packaging of the data to be nsmitted which are then handed to the physical layer for transmission.

l dispensable parts of the LAPD frame were removed to save resources. The LAPDm me is particular, lacks the terminal endpoint identifier(TEI) , the frame check quence(FCS) and the flags at both ends[1]. The LAPDm frame does not need those parts, ce their tasks is performed by other GSM protocols. The task of the FCS can be rformed by channel coding/decoding.

owever on the GPRS, the LLC(between MS-SGSN) and RLC/MAC (between MS-BSS) er that make up the data link between the MS and the network. The protocol is mainly an apted version of the LAPDm protocol used in GSM.The LLC Protocol establishes a gical link between MS and SGSN. Its functionality includes sequence control, in-order livery, flow control,detection of transmission errors, and retransmission (automatic repeat quest (ARQ)). The data confidentiality is ensured by ciphering functions. It operates her in an unacknowledged mode, not taking care of packet losses, or in an acknowledged ode, which applies retransmissions and flow control to ensure a correct delivery of data. ne RLC/MAC layer at the air interface includes two functions. The main purpose of the dio link control (RLC) layer is to establish a reliable link between the MS and the BSS. LC is always operated in an acknowledged mode with a sliding window flow control echanism and a selective ARQ mode providing a reliable link between MS and BSS. This cludes the segmentation and reassembly of LLC frames into RLC data blocks and ARQ of correctable codewords.

his new medium access control (MAC) scheme was changed to meet the demands of the cket oriented data transmission. The RLC/MAC layer ensures the concurrent access to dio resources in a more flexible way compared to the unmodified TDMA structure of SM. It controls the access attempts of an MS on the radio channel shared by several MSs. employs algorithms for contention resolution, multiuser multiplexing on a PDTCH, and cheduling and prioritizing based on the negotiated QoS. The flexibility is achieved by the ntroduction of a logical Packet Data Traffic Channel (PDTCH) which is multiplexed onto a

ysical data channel, the Packet Data Channel(PDCH), which corresponds to one timeslot S) in the GSM TDMA frame. Up to eight of these PDTCHs share one PDCH.

3.3 Network Layer

nother difference is the Network Layer of the air interface of GSM. GSM uses three otocols named Connection Management (CM) , Mobility Management (MM) and Radio esources (RR) and GPRS uses the Subnetwork Dependent Convergence Protocol NDCP).

GSM:

IM manages the location updating and registration procedures, as well as security and uthentication[12]. MM uses the channels that RR provides to transparently exchange data etween the MS and the NSS. From a hierarchical prospective, the MM lies above the RR, ecause MM data already are user data. The BSS does not, with a few exceptions, process IM messages. A typical application of MM is location update[1].

CM handles general call control and manages Supplementary Services and the Short Message Service[12]. Like MM, CM uses the connection that RR provides for information exchange. In contrast to MM, which is use only to maintain the mobility of a subscriber, CC s a real application that at the same time provides an interface to ISDN[1].

RR management controls the setup, maintenance, and termination of radio and fixed channels, including handovers[12]. Messages in the area of RR are necessary to manage the logical as well as the physical channels on the Air-Interface. Depending on the message type, processing of RR messages is performed by the MS, in the BSS, or even in the MSC. Involvement of the BSS distinguishes RR from MM and CC[1].

n GPRS, the SNDCP is used to transfer data packets between SGSN and MS. It nultiplexes several connections of the network layer onto one virtual logical connection of ne underlying LLC layer. This comprises multiplexing of packets from different protocols, eader compression (e.g. TCP/IP) and data compression (e.g. V42.bis), and segmentation of ackets larger than the maximum LLC packet data size. It also compresses and ecompresses user data and redundant header information.

3.4 Signaling

GSM signaling between the different entities in the fixed part of the network, such as etween the HLR and VLR, is accomplished through the Mobile Application Part (MAP).

AP acts as a communication control between MAP and applications, and is a carrier of gnaling data[1].

AP is built on top of the Transaction Capabilities Application Part (TCAP, the top layer Signaling System Number 7). TCAP is built on top of SCCP. The SCCP analyzes the ta received from the MTP and forwards the data to the addressed subsystem, where the put data is associated with the various active transactions. The Message Transfer Part ITP) of SS7 is used. The Message Transfer Part provides all the functionality of OSI ayer1 to 3 required to provide reliable transport of signaling data to the various SS7 user rts, takes the necessary measures to ensure that the connection can be maintained or events loss of data, like when switching to an alternative route.

PRS uses the same protocols for signaling between the SGSN and the HLR, VLR, and R as used in GSM and extends them to GPRS functionality.

he Gf interface between the SGSN and EIR, the Gr interface between the SGSN and the LR and the Gc interface between the GGSN and the HLR use the the same lower levels as ed in GSM. That is the Physical layer, MTP, SCCP and TCAP. However an enhanced rsion of MAP denoted by MAP+, handles handovers, location updates , routing formation and user profiles.

ke GSM a GGSN just send its information requests to any GSN connected to the SS7. nother interface which is quite similar to GSM's interfaces is the Gs interface between the GSN and the visited MSC with the VLR(see figure 3). In this case, only one protocol anges called BSSAP+ which is a subset of the base station subsystem application part SSAP) protocol used in GSM. BSSAP+ like BSSAP uses existing signaling standards S7 and SCCP). This protocol was implemented to handle combined GSM and GPRS rvices are requested.

he BSS GPRS Application Protocol (BSSGP) has also been derived from BSSMAP used GSM. On the BSS it is used to deliver routing and QoS-related information between SS and SGSN.

nother difference between the GSM Protocol stack is one more new protocol at the Gn terface. The protocol called the GPRS Tunneling Protocol (GTP) tunnels mobile pplication part (MAP), IP, and x.25 messages between the GPRS support nodes (GSNs). he protocol is defined both between GSNs within one PLMN (Gn interface) and between

ls of different PLMNs (Gp interface). GTP employs a tunnel mechanism to transfer data packets specifying a tunnel control and management protocol. The signaling is to create, modify, and delete tunnels. GTP packets carry the IP or X.25 packets which e not supported by GSM. [13].

Chapter 4

MOBILE SWITCHING CENTER

1 Introduction

ne Switching System contains the following components:

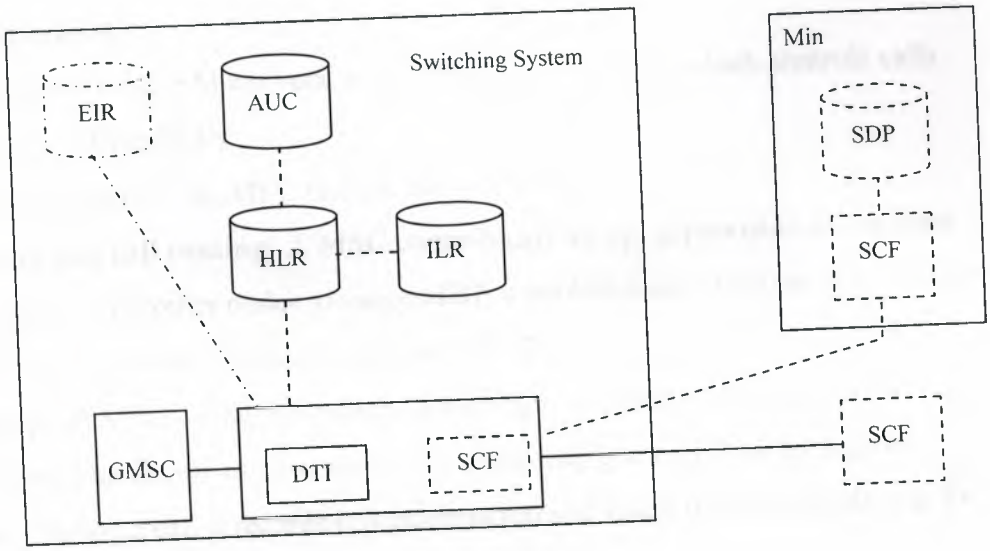


Figure 4.1 Switching Systems

Table 4.1 Switching System components

Type	Abbrev.	Full component name	Platform
Basic	MSC/VLR	Mobile services Switching Center/Visitor Location Register	AXE
	GMSC	Gateway MSC	AXE
	HLR	Home Location Register	AXE
	ILR	Interworking Location Register	AXE
	AUC	Authentication Center	Unix
	ELR	Equipment Identity Register	/AXE
	DTI	Data Transmission Interface	Unix
			AXE
Additional	MC	Message Center	MXE
	SSP	Service Switching Function	AXE
	SCP	Service Control Function	AXE
	SDP	Service Data Point	Unix

ch network component is described in the remainder of this chapter.

2 Mobile Services Switching Center/visitor Location Register (MSC/VLR)

2.1 MSC Function

he primary node in a GSM network is the MSC. It is the node, which controls calls oth to MS's and from MS's.

he primary functions of an MSC include the following:

) **Switching and call routing: A MSC** controls call set-up, supervision and release nd may interact with other nodes to successfully establish a call. This includes routing f calls from MS's to other networks such as a PSTN.

) **Charging:** an MSC contains functions for charging mobile calls and information bout the particular charge rates to apply to a call at any given time or for a given destination. During a call it records this information and stores it after the call, e.g. for output to a billing center.

3) **Service provisioning:** supplementary services are provided and managed by a MSC. In addition, the SMS service is handled by MSC's.

4) **Communication with HLR:** the primary occasion on which an MSC and HLR communicate is during the set-up of a call to an MS, when the HLR requests some routing information from the MSC's.

5) **Communication with the VLR:** associated with each MSC is a VLR, with which it communicates for subscription information, especially during call set-up and release.

6) **Communication with other MSC's:** it may be necessary for two MSC's to communicate with each other during call set-up or handovers between cells belonging to different MSC's.

7) **Control of connected BSC's**: as the BSS acts as the interface between the MS's and the SS, the MSC has the function of controlling the primary BSS node: the BSC. Each MSC may control many BSC's, depending on the volume of traffic in a particular MSC service area. An MSC may communicate with its BSC's during, for example, call set-up and handovers between two BSC's.

rect access to Internet services: traditionally, an MSC accessed the Internet nodes
Internet Service Provider (ISP) via existing networks such as the PSTN.
ver,this function enables an MSC to communicate directly with Internet nodes,
reducing call set-up time. Direct access can be provided by using an access server
d Tigris (from Advanced Computer Communications). This may be integrated in
ISC or stand-alone connected to an MSC.

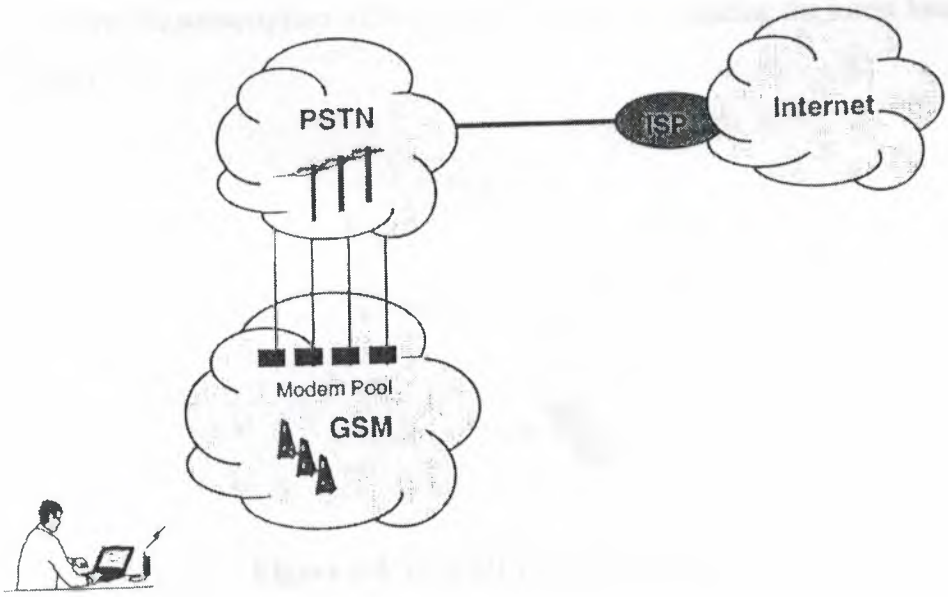


Figure 4.3 Direct access to Internet

ISDN Primary Rate Access (PRA): this function enables an MSC to provide PRA
vices to subscribers. One network operator can offer PABX connection services,
ough the PLMN. In this way the operator can compete directly with PSTN
erators for ISDN business subscribers.

2.2 VLR Function

he role of a VLR in a GSM network is to act as a temporary storage location for
bscription information for MSs which are within a particular MSC service area. Thus,
ere is one VLR for each MSC service area. This means that the MSC does not have to
ntact the HLR (which may be located in another country) every time the subscriber
ses a service or changes its status.

e following occurs when MS's move into a new service area:

The VLR checks its database to determine whether or not it has a record for the MS ed on the subscriber's IMSI)

When the VLR finds no record for the MS, it sends a request to the Subscriber's R for a copy of the MS's subscription

The HLR passes the information to the VLR and updates its location information for subscriber. The HLR instructs the old VLR to delete the information it has on the

The VLR stores its subscription information for the MS, including the latest location status (idle)

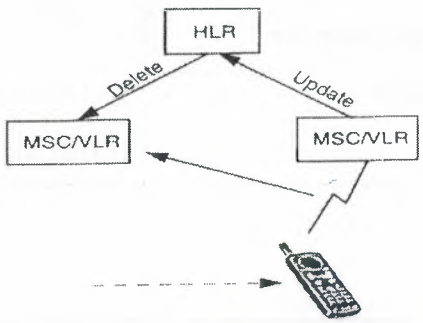


Figure 4.4 VLR-HLR Interaction

the duration when the MS is within one MSC service area, then the VLR contains a nplete copy of the necessary subscription details, including the following ormation:

Identity numbers for the subscriber

Supplementary service information (e.g. whether the subscriber has call forwarding busy activated or not)

Activity of MS (e.g. idle)

Current LA of MS

.3 MSC/VLR Implementation

e MSC and VLR are integrated in the same AXE-based node. The reason for this is t there is an extensive amount of information exchange between the two nodes for ery call, particularly during call set-up. The MSCVLR interface is completely internal thin the AXE, but each is treated as a distinct and separate function.]

ISC/VLR contains the common APZ and APT subsystems described previously, with the subsystems in the following table, each of which is implemented in are only.

Table 4.2 MSC/VLR Subsystems

Subsystem	Functions
Mobile Data Subsystem (MDS)	• VLR functions
Mobile Mobility and radio Subsystem (MMS)	• Control of BSCs • Control of handovers involving the MSC
Mobile Switching Subsystem (MSS)	• Switching and call routing • Communication with HLRs • Communication with other MSCs
Short message Handling Subsystem (SHS)	• Handling of SMS messages

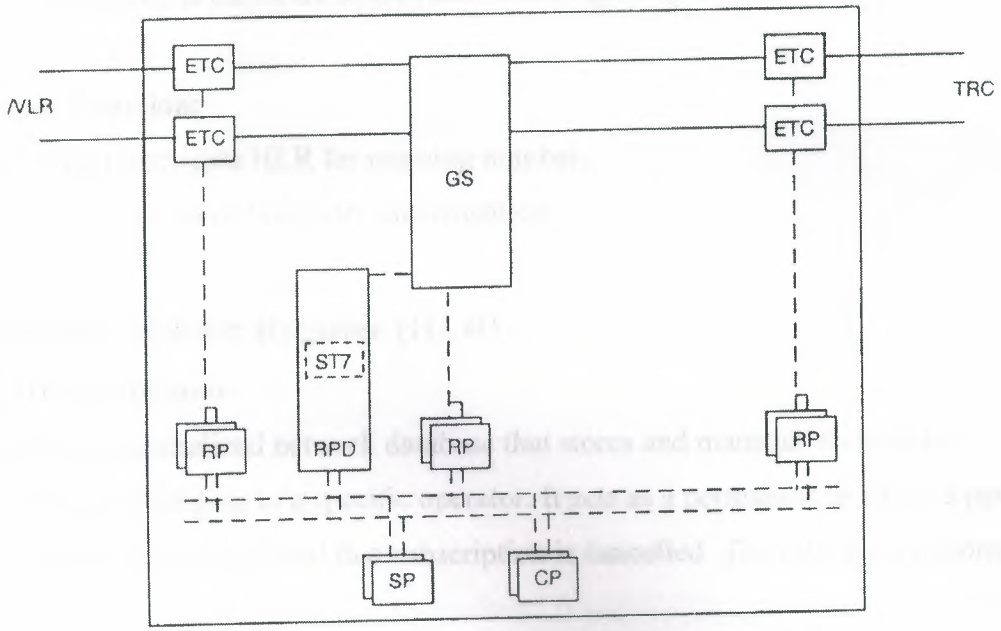


Figure 4.5 MSC/VLR hardware

4.3 Gateway MSC (GMSC)

4.3.1 GMSC Functions

Gateway functionality enables an MSC to interrogate a HLR in order to route a mobile terminating call. It is not used in calls from MS's to any terminal other than another MS. For example, if a person connected to the PSTN wants to make a call to a GSM mobile subscriber, then the PSTN exchange will access the GSM network by first connecting the call to a GMSC. The GMSC requests call routing information from the HLR that provides information about which MSC/VLR to route the call to. The same is true of a call from an MS to another MS.

4.3.2 GMSC Implementation

Any MSC in the mobile network can function as a gateway by integration of the appropriate software and definition of HLR interrogation information. In effect it then becomes a GMSC/VLR.

Gateway functions are provided within the subsystem MSS. The only additional hardware required is hardware to interface to the signaling link to the HLR.

Gateway Function:

1) Find and interrogate HLR for roaming number.
2) Route the call according to the interrogation.

4.4 Home Location Register (HLR)

4.4.1 HLR Functions

The HLR is a centralized network database that stores and manages all mobile subscriptions belonging to a specific operator. It acts as a permanent store for a person's subscription information until that subscription is cancelled. The information stored includes:

1) Subscriber identity (i.e. IMSI, MSISDN)
2) Subscriber supplementary services
3) Subscriber location information (i.e. MSC service area)
4) Subscriber authentication information

he primary functions of the HLR include:

) **Subscription database management:** as a database, the HLR must be able to rocess data quickly in response to data retrieval and update requests from other etwork nodes. For this reason it acts as a database management system. Each ubscriber record contains a substantial amount of parameters.

) **Communication with MSC's:** when setting up calls to an MS, it is necessary for the ILR to contact the MSC serving the MS for routing information. By analyzing the MSISDN, MSC knows which HLR to contact worldwide for that MS's subscription.

) **Communication with GMSC's:** during call set-up to an MS, the GMSC requests IS location information from the HLR, which then provides this in the form of outing information. Also, if the subscriber is detached the HLR will inform the GMSC that there is no need to perform further routing of the call.

) **Communication with AUC's:** before any activity involving change or use of ubscription information takes place, the HLR must retrieve new authentication arameters from an AUC.

) **Communication with** VLR's / ILR's: when an MS moves into a new MSC ervice area the VLR for that area requests information about the MS from the HLR of the subscriber.

The HLR provides a copy of the subscription details, updates its MS location information and instructs the old VLR to delete the information it has about that MS. As the ILR acts as a VLR for AMPS subscribers, the HLR communicates with it in a similar way.

4.4.2 HLR Implementation

The HLR can be implemented in the same network node as the MSC/VLR (i.e. MSC/VLR/HLR) or as a stand-alone database. An MSC/VLR/HLR node is a suitable solution for a small startup GSM network as it saves hardware and signaling load on the links between MSC/VLR and HLR.

A stand-alone HLR is a suitable solution for large networks. It has the following advantages:

1) There are no traffic disturbances creating better reliability

2) When the HLR is separate from the MSC/VLR, there is more capacity available for

call handling in the MSC/VLR

If the number of subscribers exceeds the capacity of a HLR, additional HLR's may be added.

HLR Redundancy

In order to provide additional network reliability, an additional "mated" HLR is used to mirror the data in a HLR and can automatically take over if required.

System Structure

The HLR is an AXE-based AM called HLRAM. Along with the standard APZ and APT subsystems the HLR includes the APT subsystem Home location Register Subsystem (HRS) that performs the necessary subscription management.

4.5 Interworking Location Register (ILR)

4.5.1 ILR Functions

ILR offers roaming capabilities between mobile telephony systems complying with different standards. The ILR is specific to the GSM1900 product portfolio and enables AMPS network subscribers to roam to a GSM 1900 network.

In the near future the ILR will make intersystem roaring possible both directions between all GSM, AMPS/TDMA networks.

For AMPS subscribers who wish to avail of this roaming functionality, their AMPS network subscriptions are copied into the HLR side of the ILR. When they roam into the GSM 1900 network, the I-ILR copies this information into the VLR side of the ILR, as occurs for normal GSM roaming subscribers.

From the subscriber's point of view however, there is only one subscription.

In the near future, the ILR will make intersystem roaming possible in both directions between all GSM, AMPS/TDMA networks

4.5.2 ILR Implementation

In Ericsson's GSM systems the ILR is AXE-based. It includes the common APZ and APT subsystems outlined previously and the following additional subsystems:

Table 4.3 ILR subsystems

Subsystem	Functions
Home location Register Subsystem (IIRS)	• AMPS Subscriber database management

Mobile Intersystem roaming Subsystem (MIS)	• Mapping and translation of services and protocols • Communication with other nodes

R hardware is similar to ILR hardware.

6 Authentication Center (AUC) and Equipment Identity Register EIR)

LMN's need a higher level of protection than traditional telecommunication networks. herefore, to protect GSM systems, the following security functions have been defined:

Subscriber authentication: by performing authentication, the network ensures that unauthorized users can access the network, including those that are attempting to npersonate others.

Radio information ciphering: the information sent between the network and an MS ciphered. An MS can only decipher information intended for it.

Mobile equipment identification: because the subscriber and equipment are eparate in **GSM,** it is necessary to have **a** separate authentication process for the MS quipment. This ensures, e.g. that a mobile terminal, which has been stolen, is not able access the network.

Subscriber identity confidentiality: during communication with an MS over a radio nk, it is desirable that the real identity (IMSI) of the MS is not always transmitted. nstead a temporary identity (TMSI) can be used. This helps to avoid subscription fraud. he AUC and EIR are involved in the first three of the above features, while the last is andled by MSC/VLRs.

.6.1 AUC Functions

The primary function of an AUC is to provide information, which is then used by an MSC/VLR to perform subscriber authentication and to, establish ciphering procedures on the radio link between the network and MS's.

The information provided is called a triplet and consists of:

1) A non predictable RANDom number (RAND)

2) A Signed RESponse (SRES)

ciphering Key (Kc)

ision of Triplets

bscription time, each subscriber is assigned a subscriber authentication Key (Ki). stored in the AUC along with the subscriber's IMSI. Both are used in the process oviding a triplet. The same Ki and IMSI are also stored in the SIM. In an AUC the ving steps are carried out to produce one triplet:

non-predictable random number, RAND, is generated

AND and Ki are used to calculate SRES and Kc, using two different algorithms, nd A8 respectively

AND, SRES and Kc are delivered together to the HLR as a tripletLR as a triplet.

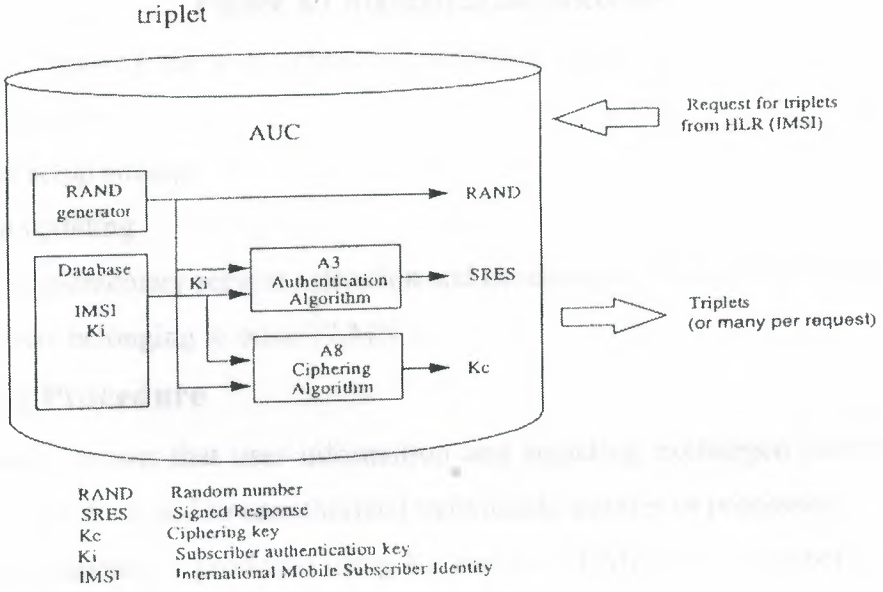


Figure 4.6 Provision of triplet

thentication Procedure

The MSC/VLR transmits the RAND to the MS.

The MS computes the signature SRES using RAND and the subscriber authentication (Ki_1) through the A3 algorithm.

The MS computes the Kc by using Ku and RAND through A8 algorithm. Kc will reafter be used for ciphering and deciphering in MS.

The signature SRES is sent back to MSC/VLR, which performs authentication, by cking whether, the SRES from the MS and the SRES from the AUC match. If so, the bscriber is permitted to use the network. If not, the subscriber is barred from network

ess.

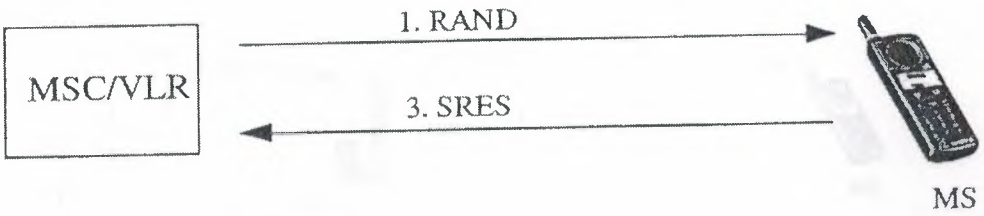


Figure 4.7 Authentication procedure

ıthentication can by operator's choice be performed during:

Each registration

Each call setup attempt

Location updating

Before supplementary service activation and deactivation There can be exceptions

r subscribers belonging to other PLMN's.

iphering Procedure

ɔnfidentiality means that user information and signaling exchanged between BTS's

d MS's is not disclosed to unauthorized individuals, entities or processes.

ciphering sequence is produced using Kc and the TDMA frame number as inputs in

e encryption algorithm A5. The purpose of this is to ensure privacy concerning user

formation (speech and data) as well as user related signaling elements.

order to test the ciphering procedure some sample of information must be

sed. For this purpose the actual ciphering mode command (M) is used.

) M and Kc are sent from the MSC/VLR to the BTS.

) M is forwarded to the MS.

) M is encrypted using Kc (calculated earlier with SRES in the authentication

rocedure) and the TDMA frame number, which are fed through the encryption

gorithm, A5.

) The encrypted message is sent to the BTS.

) Encrypted M is decrypted in the BTS using Kc, the TDMA frame number and the

ecryption algorithm, A5.

e decryption of M was successful, the ciphering mode completed message is sent to
ISC. All information over the air interface is ciphered from this point on

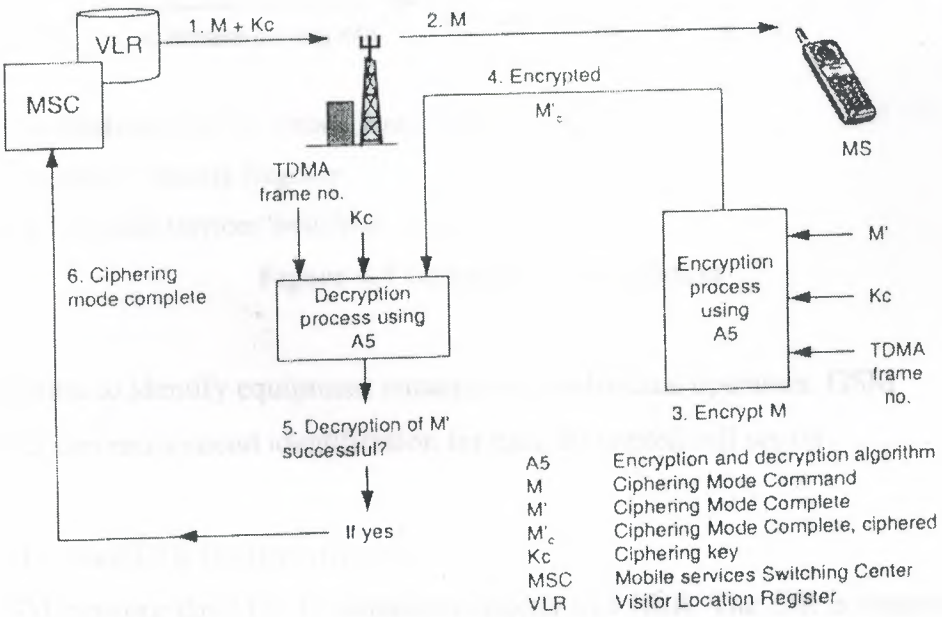


Figure 4.8 ciphering procedure

2 EIR Functions

ipment Identification Procedure

equipment identification procedure uses the identity of the equipment itself
EI) to ensure that the MS terminal equipment is valid.

he MSC/VLR requests the IMEI from the MS.

IS sends IMEI to MSC.

ISC/VLR sends IMEI to EIR.

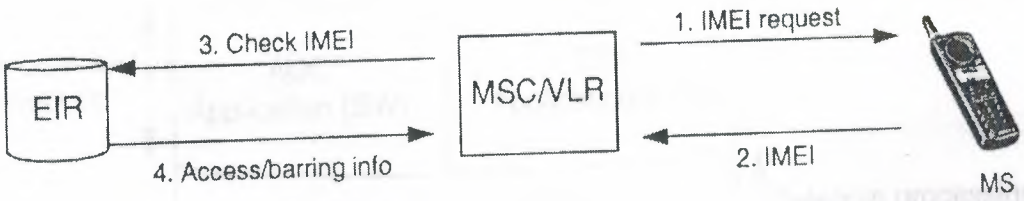
n reception of IMEI, the EIR examines three lists:

hite list containing all number series of all equipment identities that have
n allocated in the different participating GSM countries.

lack list containing all equipment identities that has been barred.

ray list (on operator level) containing faulty or non -approved mobile equipment.

he result is sent to MSC/VLR, which then decides whether or not allow network
ess for the terminal equipment.



IEI International Mobile station Equipment Identity

R Equipment Identity Register

SCNLR Mobile services Switching Center

Figure 4.9 Equipment identification

he decision to identify equipment remains with individual operators. GSM pecifications recommend identification for each attempted call set-up.

.6.3 AUC and EIR Implementation

n a GSM network the AUC is connected directly to a HLR. The EIR is connected to an MSC/VLR.

AUC may be implemented on either AXE or Unix (from Sema Group). The EIR is mplemented on a Unix platform from Sema Group.

f implemented on AXE, the most common configuration for an AUC is integrated with HLR as an AUC/HLR node. This reduces the signal processing requirements of both. The AUG is implemented using the AUG Application Module (AUCAM).

The most common implementation is a Unix-based AUC/EIR node, which provides the following benefits to the operator:

1) AUC and EIR processing is physically separated from the switching function in the MSC. This provides better network planning flexibility when the network needs to be expanded.

2) The common platform is based on standard industry computer hardware (HW) and software (SW).

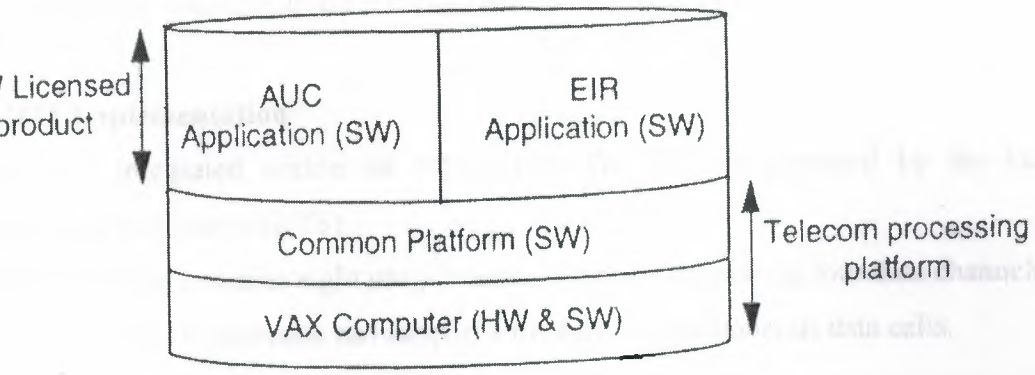


Figure 4.10 AUC / EIR product structure

Data Transmission Interface (DTI)

section gives a brief introduction to the data handling capabilities of GSM systems. a more detailed survey of such functions, please refer to the appendix titled "Data ices".

DTI Functions

DTI implements the GSM Inter-Working Function (IWF). It performs data lling functions such as data rate conversion and provides the functions necessary for interworking between GSM networks and other networks, including:

ata Traffic to/from PSTN: this involves modem and fax calls. For connections he PSTN a modem is selected by the DTI to perform the necessary rate and format versions.

Data Traffic to/from ISDN: the whole set of data communications towards ISD is available, since the MSC/DTI is capable of signaling and mapping basic service ormation between the ISDN and the GSM network.

3) Data Traffic to/from PDNs: the DTI handles data traffic to and from Public Data Networks (PDNs) such as the Packet Switched PDN (PSPDN) and Circuit Switched N (CSPDN).

Data Traffic between mobiles: the data traffic inside the PLMN must pass through DTI to handle the protocol used for rate adaptation in the radio path.

HSCSD: this version of High Speed Circuit Switched Data (HSCSD) allows the nnection of 2, 3, or 4 time slots on one radio channel each carrying 9.6 k bits/s. The

TI handles rate conversion to PSTN or ISDN as appropriate.

.2 DTI Implementation

e DTI is integrated within an MSC/VLR. The DTI is managed by the Data ansmission Subsystem (DTS).

ne DTI sub-rack contains eight plug-in units, each one supporting four data channels. nerefore, each DTI sub-rack can support a total of 32 simultaneous data calls.

8 Message Center (MC)

3.1 MC Function

n MC may be added to a GSM network to provide one or more of the following essaging services:

- Voice mail
- Fax mail
- Short Message Service (SMS) text messages
- SMS Cell Broadcast (SMSCB) text messages

nese services can generate considerable revenue for a network operator, as they are ecoming increasingly popular.

oice Mail

oice mail ensures that all calls to a person can be completed, even when a person does ot answer calls. A calling party can record a voice message for the subscriber they are alling.

A subscriber can use their MS to select diversion to voice mail based on a articular event or status (e.g. busy, unreachable).

The subscriber is informed that they have voice messages in their mailbox by means of ither a short text message or phone call from the network at regular intervals. If their MS is detached, this indication is sent when the subscriber next attaches to the network. The subscriber can then retrieve their voice mail messages at a later stage. Functions for storing voice messages over a long period also exist.

Fax Mail

Fax mail operates similarly to voice mail. For MS's that support fax, a subscriber can set diversion for all or some fax calls to a fax mailbox. When the MS is next attached to the network, the network will deliver the fax message to a fax machine identified by the MS.

text message consists of up 160 alphanumeric characters, entered at a
lessage Entity (SME) such as an MS (using the keypad) or computer terminal.
message always originates or terminates in a GSM network, meaning that a
essage can not be sent between two SMEs residing outside a GSM network.
ort message originator knows if the message delivery is successful or
essful via notification. When a message is submitted, the deferred delivery option
requested. This option makes it possible to specify the time the message is to be
ed. An MC, which handles SMS messages is often referred to as an SMS Center
C). When a message is to be forwarded to an MS, the system must first determine
the MS is situated. As in ordinary voice traffic, a gateway requests the routing
ation. The gateway is called the SMS GMSC.
hort message is time stamped by the SMS-Center when it is submitted. A
ge is deleted once the delivery is successful or once the time specified in deferred
ry expires.
a message is buffered, the SMS-C regularly attempts to deliver the
ge, at intervals defined by the operator.

CB

MSCB service enables a message of up to 93 alphanumeric characters to
ivered to all attached MS's in one cell. This may be useful for identifying key
numbers in the cell's area such as that of a hospital or police station.
natively, it may be used for advertising services within the cell (e.g. "Superfood
urant in this area at the junction of M8 and 133").

MC Implementation

MC node may handle one or more messaging service. For example,
nding on the amount of SMS traffic, it may be more efficient to have one MC
g as an SMS-C only, with other messaging services handled by another separate
It is also possible to integrate SMS-C functions on an MSC, leading to the term
Interworking MSC (SMS-IWMSC). Additionally, the SMS GMSC functions may
e in the same node as the GMSC functions used for voice calls.
most important component of MXE is the message kernel. The message kernel is
entral message store and forward nucleus responsible for safe storage of messages,

and retry attempts.

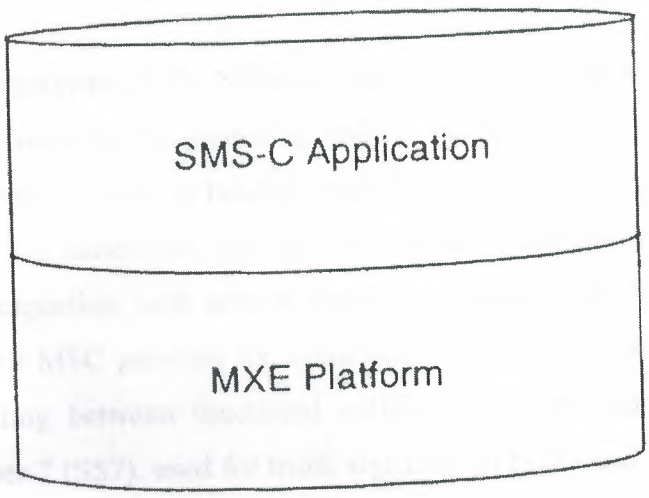


Figure 4.11 SMS-C on MXE

ervice Switching Function (SSF), Service Control Function (SCF) Service Data Point (SDP)

section gives a brief introduction to the Mobile Intelligent Network (MIN) ng capabilities of Ericsson's GSM systems. For a more detailed survey of such ons, please refer to the appendix titled "Mobile Intelligent Network Services".

le Intelligent Network (MIN) nodes can be added to a basic GSM network to de value-added services such as Free phone and Personal Number to subscribers. nodes include

rvice Switching Function (SSF): an SSF acts as an interface between the call control ions of the mobile network and the service control functions of a Service Control (SCP). SSF is an AXE-based AM (SSFAM) and may be integrated within an

rvice Control Function (SCF): a MSC/VLR (recommended) or stand-alone. contains the intelligence of a MIN service or services. This intelligence is realized ftware programs and data. SCP is also an AXE-based AM (SCFAM) and the nmended configuration is as a stand-alone node, accessible by all MSC/SSPs.

ervice Data Point (SDP): an SDP manages the data, which is used by a MIN ce.

CONCLUSION

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

REFERENCES

Vineet Sachdev, System Engineer

Trueposition Inc. 1111 West DeKalb Pike Wayne, PA 19087

Asha Mehrotra, "GSM System Engineering"

MOBILE COMMUNICATIONS SERIES, Artech House Publishers.

Brian McIntosh "Telecommunications"

p://telecomindustry.about.com/business/telecomindustry/library/weekly/aa1115999.ht

Dick Tracy "The Applications We Promote…." http://www.comm-nav.com/commnav.htr

GRAYSON WIRELESS, a division of Allen Telecom. "Geometrix Wireless Location nsor" http://java.grayson.com/geodatasheet.htrr

Louis A. Stilp "Examining the Coming Revolution in Location Services" p://www.trueposition.com

Paul J, Bouchard "AccuCom Wireless Service Inc." http://www.Global-Images.com

9] Tutorial "How GPS works?" http://www.trimble.com