NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Electrical and Electronic Engineering

GSM SYSTEM ARCHITECTURE

Graduation Project
EE-400

Student: Yousef Al-Maqousi

Supervisor: Prof. Dr. Fakhreddin Mamedov

Lefkoşa – 2002

Acknowledgement

I would like to acknowledge the contribution of:

- Dr. Fakhreddin Mamedov: My supervisor and advisor who has paid a great effort and incite me until I finished the project.
- Electrical Engineering Department staff who have not hesitated to help me as well as presenting all tools and advices that I needed in order to go on with the project.
- All my colleagues and friends in faculty, they were always beside me.
- All my family members who encouraged me and stood by my side.

Yousef Maqousi

Abstract

GSM, the Global System for Mobile communications, is a digital cellular communications system which has rapidly gained acceptance and market share worldwide, although it was initially developed in a European context. In addition to digital transmission, GSM incorporates many advanced services and features, including ISDN (Integrated Services Digital Network) compatibility and worldwide roaming in other GSM networks. The advanced services and architecture of GSM have made it a model for future third-generation cellular systems. This paper will give an overview of the services offered by GSM, the system architecture, the radio transmission structure, and the signaling functional architecture.

Table of Contents:

Chapter3: GSM Network Components

Chapter4: GSM Basic Call Sequence and Radio Interface Optimization

Introduction and history of GSM

The development of GSM started in 1982, when the Conference of European Posts and Telegraphs (CEPT) formed a study group called Group Special Mobile (the initial meaning of GSM). The group was to study and develop a pan-European public cellular system in the 900 MHz range, using spectrum that had been previously allocated. At that time, there were many incompatible analog cellular systems in various European countries. Some of the basic criteria for their proposed system were:

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

In 1989, the responsibility for GSM was transferred to the European Telecommunication Standards Institute (ETSI), and the Phase I recommendations were published in 1990. At that time, the United Kingdom requested a specification based on GSM but for higher user densities with low-power mobile stations, and operating at 1.8 GHz. The specifications for this system, called Digital Cellular System (DCS1800) were published 1991. Commercial operation of GSM networks started in mid-1991 in European countries. By the beginning of 1995, there were 60 countries with operational or planned GSM networks in Europe, the Middle East, the Far East, Australia, Africa, and South America, with a total of over 5.4 million subscribers [2].

GSM SYSTEM ARCHITECTURE

Chapter 1
Cellular Telecommunications

1.1 Principles of Cellular Telecommunications

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

Information sent between the MS subscriber and the cellular network uses radio communication. This removes the necessity for the fixed wiring used in the traditional telephone installation.

Due to this, the MS subscriber is able to move around and become fully mobile, perhaps travelling in a vehicle or on foot [1].

1.1.1 Advantages of Cellular Communications

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

1.1.2 Advantages to mobile Subscriber

- Mobility
- Flexibility
- Convenience

1.1.3 Advantages to Network Provider

- Network Expansion Flexibility
- Revenue/Profile Margins
- Efficiency
- Easier Re-Configuration

1.2 Introduction and history of GSM

The development of GSM started in 1982, when the Conference of European Posts and Telegraphs (CEPT) formed a study group called Group Special Mobile (the initial meaning of GSM). The group was to study and develop a pan-European public cellular system in the 900 MHz range, using spectrum that had been previously allocated. At

cellular system in the 900 MHz range, using spectrum that had been previously allocated. At that time, there were many incompatible analog cellular systems in various European countries. Some of the basic criteria for their proposed system were:

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

In 1989, the responsibility for GSM was transferred to the European Telecommunication Standards Institute (ETSI), and the Phase I recommendations were published in 1990. At that time, the United Kingdom requested a specification based on GSM but for higher user densities with low-power mobile stations, and operating at 1.8 GHz. The specifications for this system, called Digital Cellular System (DCS1800) were published 1991. Commercial operation of GSM networks started in mid-1991 in European countries. By the beginning of 1995, there were 60 countries with operational or planned GSM networks in Europe, the Middle East, the Far East, Australia, Africa, and South America, with a total of over 5.4 million subscribers [2].

1.3 Services provided by GSM

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

In addition, various data services are supported, with user bit rates up to 9600 bps. Specially equipped GSM terminals can connect with PSTN, ISDN, Packet Switched and Circuit Switched Public Data Networks, through several possible methods, using synchronous or asynchronous transmission. Also supported are Group 3 facsimile service, videotex, and teletex. Other GSM services include a cell broadcast service, where messages such as traffic reports, are broadcast to users in particular cells.

A service unique to GSM, the Short Message Service, allows users to send and receive point-to-point alphanumeric messages up to a few tens of bytes. It is similar to paging

services, but much more comprehensive, allowing bi-directional messages, store-and-forward delivery, and acknowledgement of successful delivery.

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

1.4 Cell Site

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

1.4.1 Large Cells

The maximum cell size for GSM is approximately 80 Km in diameter, but this is dependent on the terran the cell is covering and the power class of the MS. In GSM the MS can be transmitting anything up to 8 watts, obviously, the higher the power output of the MS the larger the cell size. If the cell site is on top of a hill with no obstruction for miles, then the radio waves will travel much further than if the cell site was in the middle of a city, with many high-rise building blocking the path of the radio waves.

Generally large cells are employed in:

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

1.4.2 Small Cells

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

Typical uses of a small cells:

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

1.4.3 The Trade off – Large v Small

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

1.5 Network Components

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

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

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

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

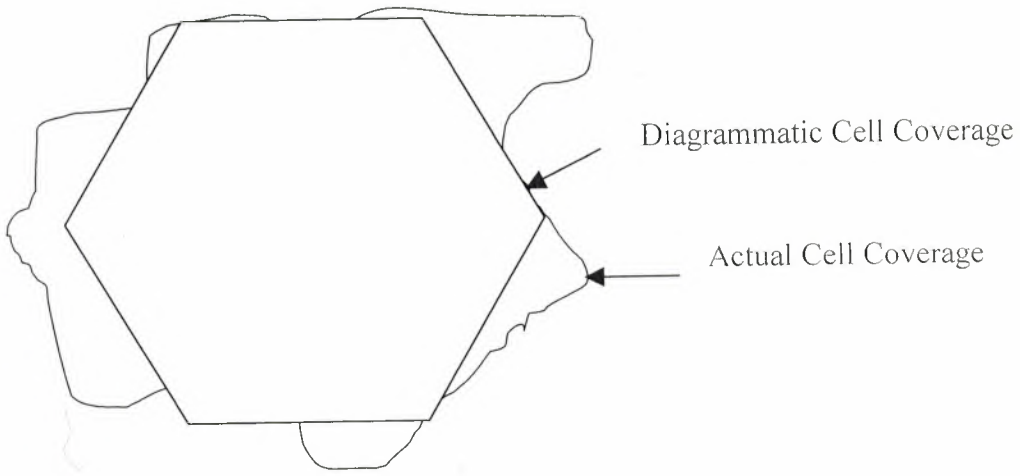
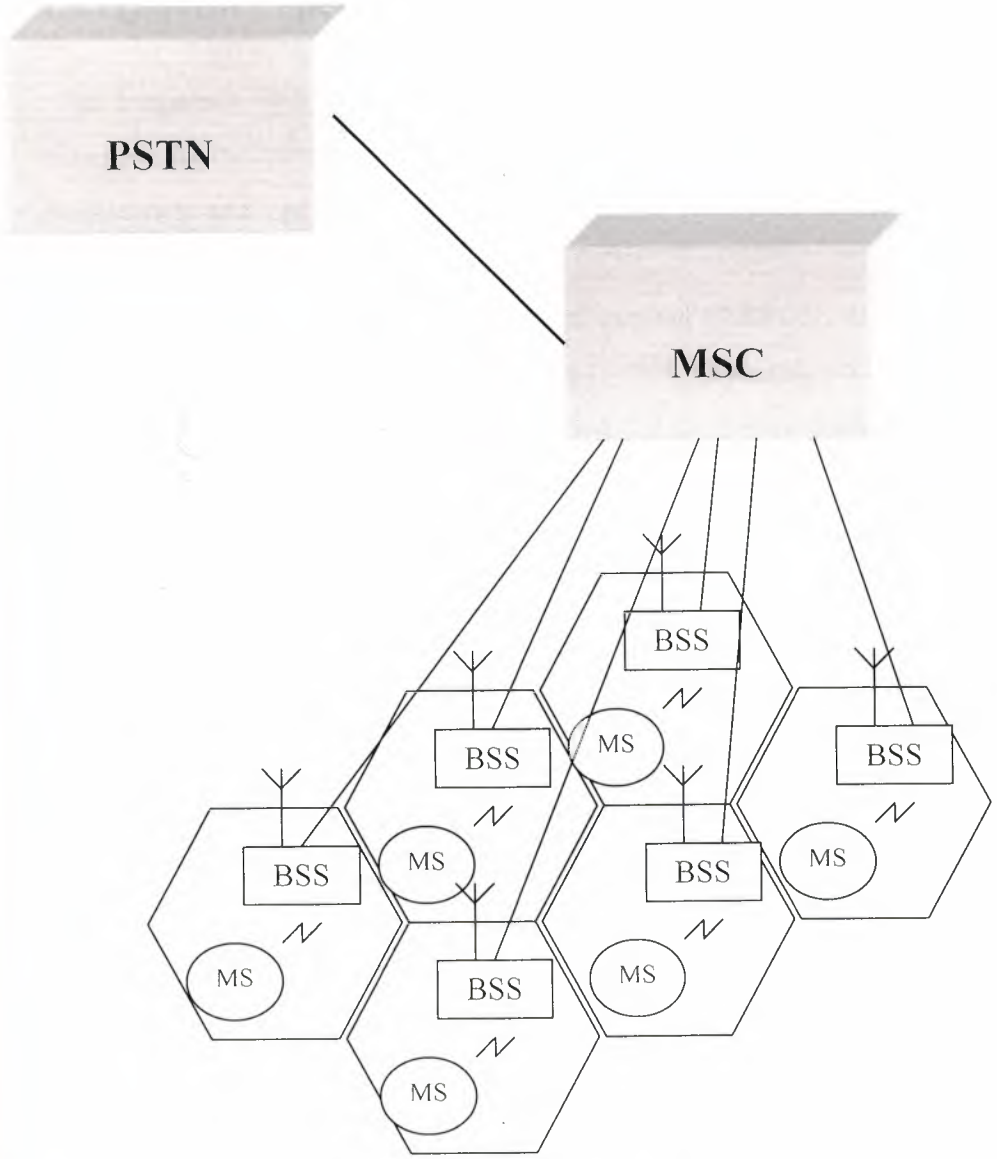


Figure 1.1: Actual and Diagrammatic Cell Coverage

PSTN is connected to the GSM Network through the MSC



PSTN	(Public Switched Telephone Network)
MSC	(Mobile Service Switching Centre)
BSS	(Base Station system)
MS	(Mobile Station)
	(Cell Coverage Area)

Figure 1.2: Network components

1.6 Frequency Spectrum

The frequency spectrum is very congested, with only narrow slots of bandwidth allocated for cellular communication. The list in the next page shows the number of frequencies and spectrum allocated for GSM, Extended GSM (EGSM), GSM1800 (DCS1800) and PCS1900.

A single absolute radio frequency channel number (ARFCN) or RF carrier is actually a pair of frequency, one used in each direction (transmit and receive). This allows information to be passed in both. For GSM900 the paired frequencies are separated by 45MHz, for DCS1800 the separation is 95MHz and for PCS1900 separation is 75MHz.

For each cell in GSM network (GSM, EGSM OR DCS1800) at least one ARFCN must be allocated, and more may be allocated, to provide greater capacity.

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

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

Frequency Range

GSM

- Receive (uplink) 890-915 MHZ
- Transmit (downlink) 935-960 MHZ
- 124 Absolute Radio Frequency Channels (ARFCN)

EGSM

- Receive (uplink) 880-915 MHZ
- Transmit (downlink) 925-960 MHZ
- 175 Absolute Radio Frequency Channels (ARFCN)

DCS1800

- Receive (uplink) 1710-1785 MHZ
- Transmit (downlink) 1805-1880 MHZ
- 374 Absolute Radio Frequency Channels (ARFCN)

ARFCN

- Bandwidth = 200 KHZ
- 8 TDMA timeslots

1.7 Frequency Re-use

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

Example

A network provider has been allocated 48 frequencies to provide coverage over a large area, let us take for example Great Britain.

As we have already seen, the maximum cell size is approximately 70Km in diameter, This our 48 frequencies would not be able to cover the whole Britain. To cover this limitation the network provider must re-use the same frequencies over and over again, in what is termed a "frequency re-use pattern ". When planning the frequency re-use pattern the network planner must take into account how often to use the same frequencies and determine how close together the cells are, otherwise co-channel interference and / or adjacent channel interference may occur. The network provider will also take into account the nature of the area to be covered. This may rang from a densely populated (high frequency re-use, small cells, high capacity) to sparsely populated rural expanse (large omni cells, low re-use, low capacity).

1.7.1 Co-Channel Interference

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

1.7.2 Adjacent Channel Interference

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

1.8 Sectorization

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

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

To gain a further increase in capacity within the geographic area we can employ a technique called " sectorization ". Sectorization splits a single site into a number of cells each cell has transmit and receive antennas and behaves as an independent cell.

Each cell uses special directional antennas to ensure that the radio propagation from one cell is concentrated in a particular direction. This has a number of advantages: Firstly, as we are now concentrating all energy from the cell in a smaller area 60, 120, 180 degrees instead of 360 degrees, we get much stronger signal, which is beneficial in location such as "in-building coverage".

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

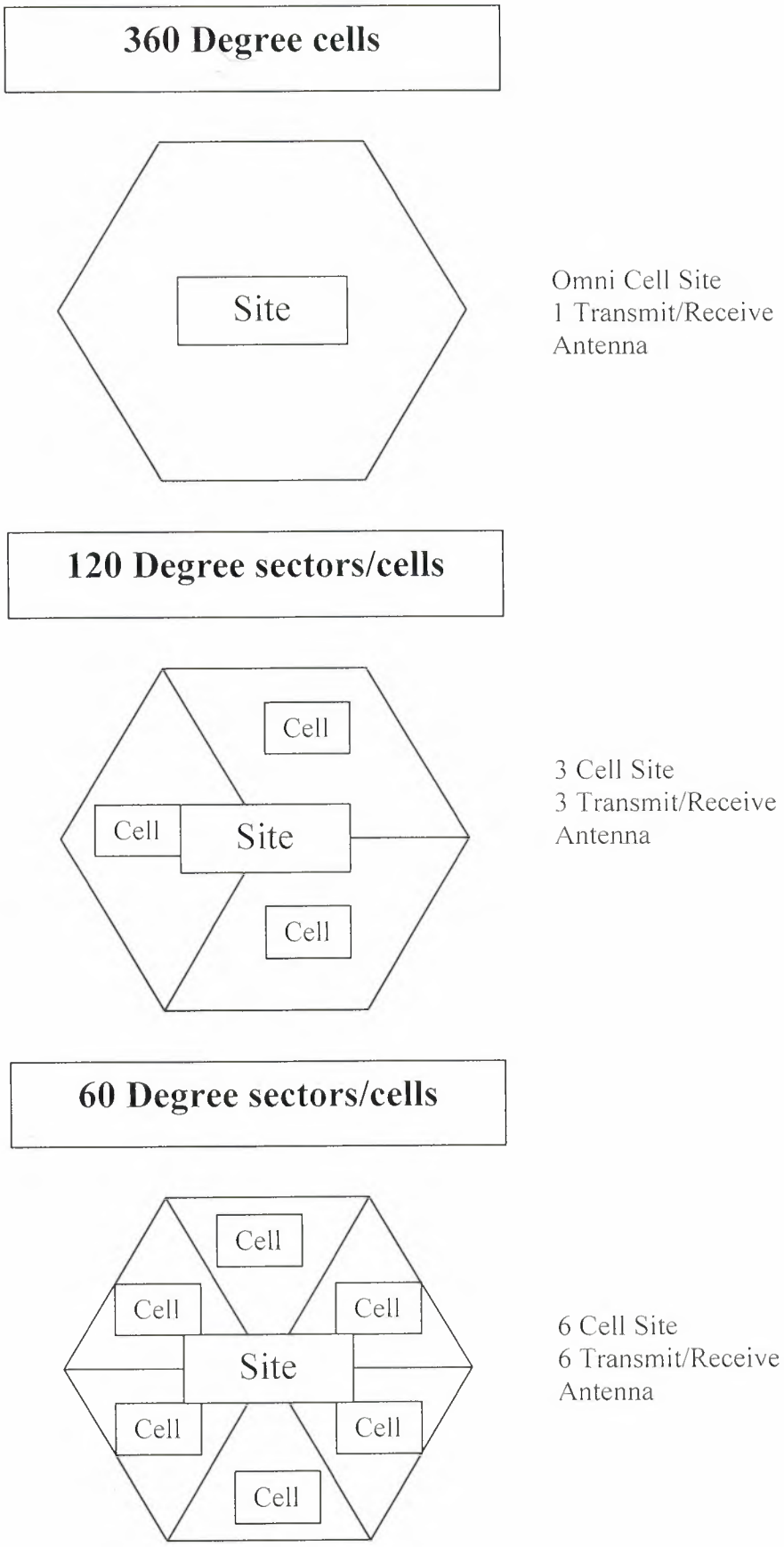


Figure 1.3: Sectorization

1.9 Transmission of Analogue and Digital Signals

The main reasons why GSM uses a digital air interface:

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

1.9.1 Modulation Techniques

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

- **Amplitude Modulation (AM)**

  Amplitude Modulation is very simple to implement for analogue signals but it is prone to noise.

- **Frequency Modulation (FM)**

  Frequency Modulation is more complicated to implement but provides a better tolerance to noise.

- **Phase Modulation (PM)**

  Phase modulation provides the best tolerance to noise but it is very complex to implement for analogue signals and therefore is rarely used.

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

1.10 Transmission of Digital Signals

1.10.1 Phase Shift Keying – PSK

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

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

1.10.2 Gaussian Minimum Shift Keying – GMSK

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

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

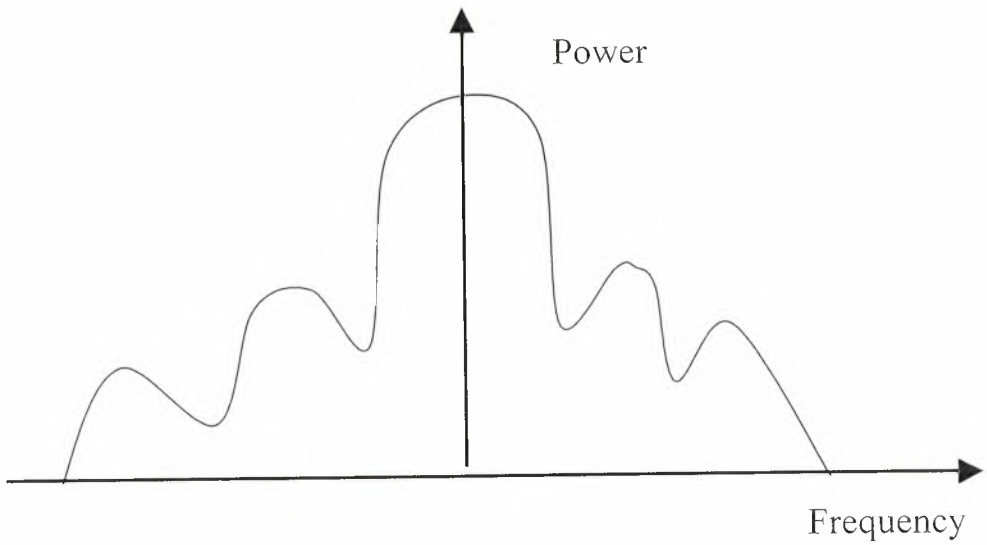


Figure 1.4: Frequency Spectrum

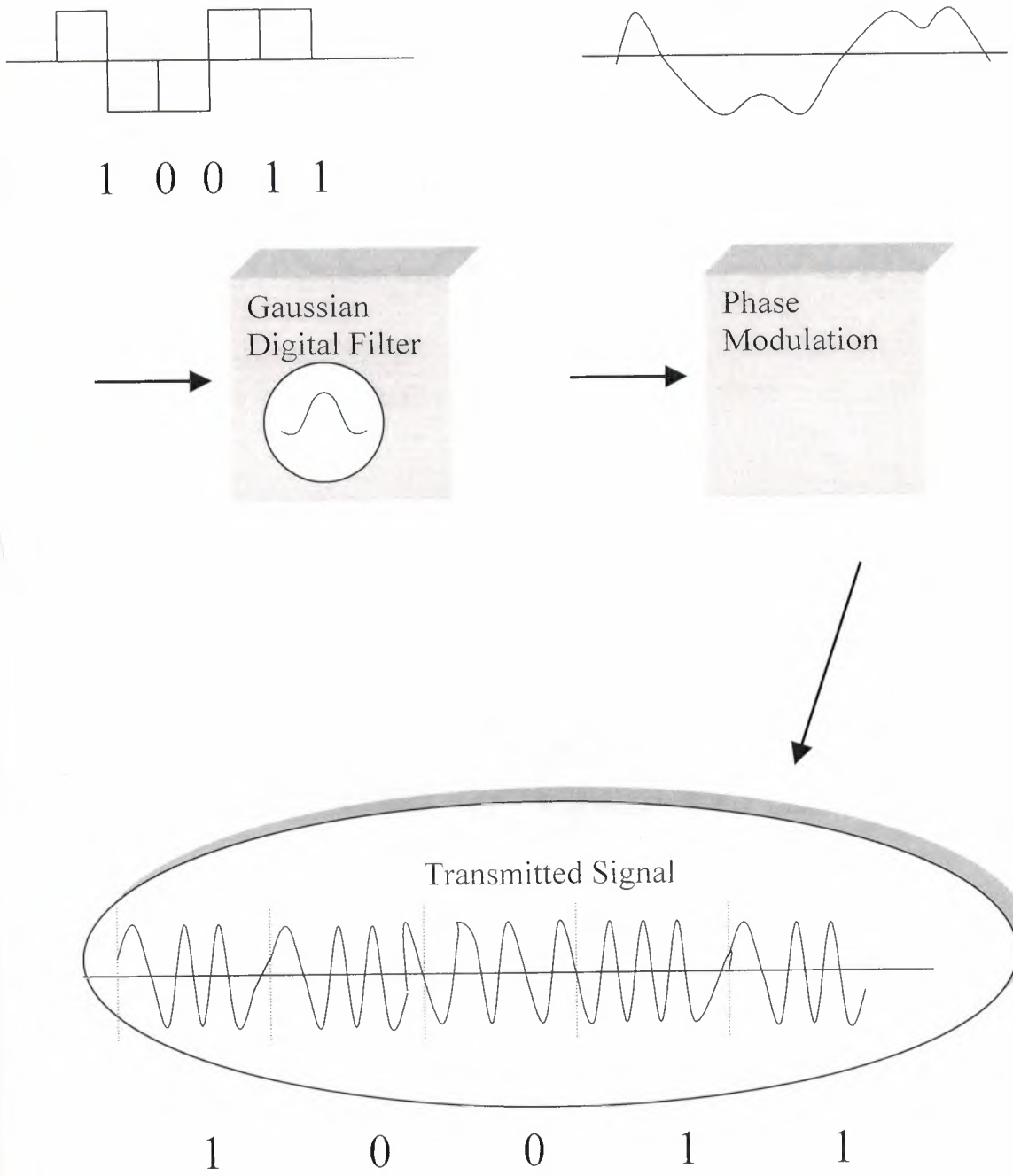


Figure 1.5: Gaussian Minimum Shift Keying (GMSK)

GSM SYSTEM ARCHITECTURE

Chapter 2
Features of GSM System

2. Features of GSM System

Our current cellular telephone systems provide the MS subscriber and network provider with many advantages over a standard telephone network, but there are still many drawbacks.

2.1 Compatibility

Due to the rapid development of cellular, there are many different cellular systems that are incompatible with one another.

The need for a common standard for mobile telecommunications is therefore obvious. An executive body was set up to co-ordinate the complicated task of specifying the new standardized network.

GSM has been specified and developed by many European countries working in co-operation with each other. The result is a cellular system that will be implemented throughout Europe. Eventually you will be able to drive from Germany to Spain without dropping your telephone call.

Due to GSMs standardization and features, it has now been accepted not only in Europe but also throughout the world.

An additional advantage resulting from this is that there will be a large market from GSM equipment. This means that manufacturers will produce equipment in higher quantities and of better quality, and also, due to the number of manufacturers, a competitive and aggressive pricing structure will exist. This will result in lower costs for the MS subscriber [1].

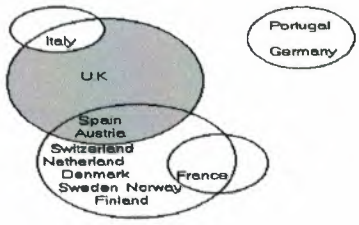


Figure 2.1: Different cellular systems incompatible with one another

2.2 Noise Robust

In the current cellular telephone systems the MS communicates with the cell site by means of analogue radio signals. Although this technique can provide an excellent audio quality (it is widely used for stereo radio broadcasting, for example), it is vulnerable to noise, as anyone who has tried to receive broadcast stereo with poor aerial will testify!

The noise, which interferes with the current system, may be produced by any of the following sources:

- A powerful or nearby external source (a vehicle ignition system or a lightning bolt, perhaps);
- Another transmission on the same frequency (co-channel interference);
- Another transmission "breaking through" from a nearby frequency (adjacent channel interference);
- Background radio noise intruding because the required signal is too weak to exclude it.

In order to combat the problems caused by noise, GSM uses digital technology instead of analogue.

By using digital signals, we can manipulate the data and include sophisticated error protection, detection and correction software. The overall result is that the signals passed across the GSM air interface can withstand more errors (that is, we can locate and correct more errors than current analogue systems). Due to this feature, the GSM air interface in harsh RF environments can produce a usable signal, where analogue systems would be unable [1].

2.3 Flexibility and Increased Capacity

The success of the current analogue cellular systems means that there is a requirement for increased cellular phone capacity and also ease of expansion. Current cellular networks have to some extent become the victims of their own success. So many subscribers have registered on these systems so quickly that it has been difficult to expand their capacity fast enough to satisfy call demand.

With the analogue air interface, every connection between an MS and a cell site requires a separate RF carrier and that, in turn, requires a separate set of RF hardware at the cell site. Therefore, to expand the capacity of a cell site by a given number of channels, an equipment quantity of RF hardware must be added to the cell site equipment. System expansion, therefore, is time-consuming, expensive and labor intensive.

With GSM, the equipment is typically much smaller in size due to the latest technology being implemented in its design. This offers significant cost savings to the network provider as well as allowing quick installation and reconfiguration of existing networks.

A future enhancement of GSM is "half rate speech". This in its simplest terms will reduce the transmission rate over the air interface of a traffic channel by 50%, thus will effectively doubling the number of traffic channels on a signal carrier.

GSM also offers the increased flexibility of international roaming. This allows the MS user to travel from one country to another, use their SIM card in any GSM phone and use the visited country GSM network to make and receive calls. The advantage for the MS user is that no matter where they are (any country with supported GSM network) the GSM network will ensure that they receive all their calls from their home network; not only that, all call billing is done on the home network, so the MS user only receives the one bill.

GSM is highly software dependent. Although this makes it very complex, it also allows a high degree of flexibility when changes need to be implemented. GSM suppliers are constantly revising their software and adding new features to compete in the GSM market [1].

2.4 Use Of Standardized Open Interfaces

The equipment in each of the analogue cellular networks tends to be produced by one manufacturer. This is because the equipment is only designed to communicate with other equipment made by that manufacturer. This situation is very profitable for the manufacturers as they have a great deal of influence over the pricing of their product. Unfortunately for the MS user and the network provider, this means high prices.

The situation is very different with GSM, where standard interfaces such as **C7** and **X.25** are used throughout the network. This means that network planners can select different manufacturers for different pieces of hardware. Competition between manufacturers will therefore increase and prices should fall.

In addition, network planners have a great deal of flexibility in where the network components are situated. This means that they can make the most efficient use of the terrestrial links, which they operate [2].

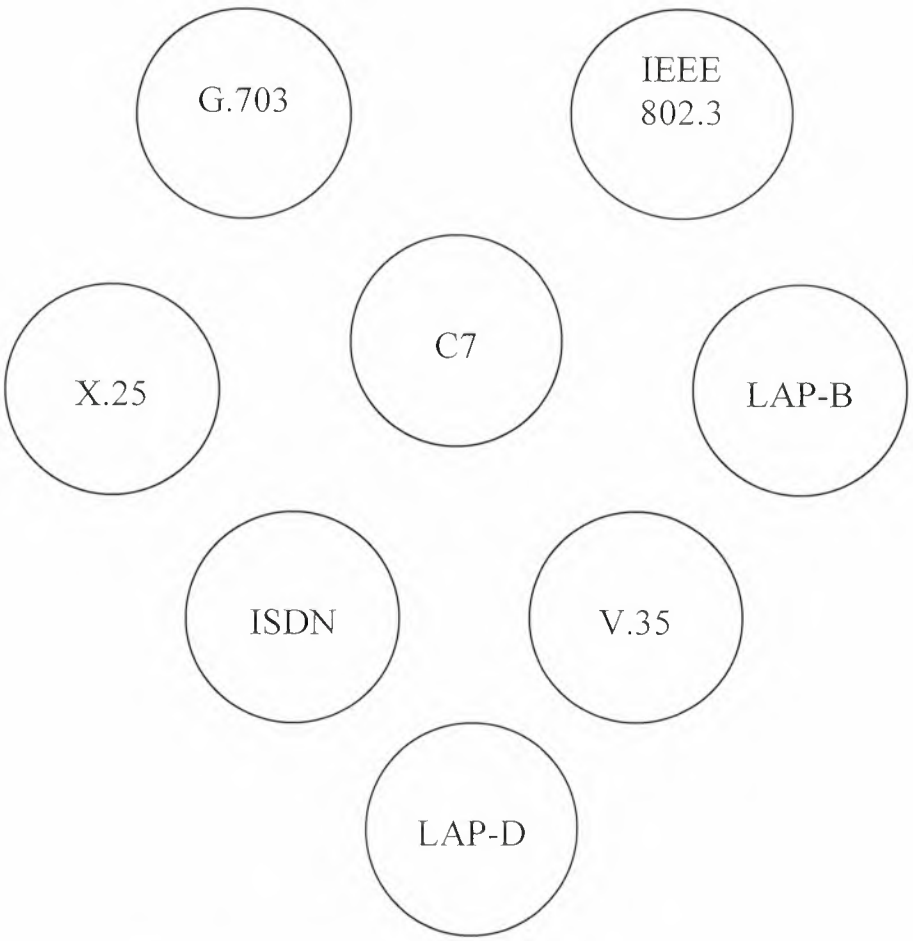


Figure 2.2: Standardized Open Interfaces

2.5 Improved Security and Confidentiality

Security figures high on the list of problems encountered by some operators of analogue systems. In some systems, it is virtually non-existent and the unscrupulous were quick to recognize this. With some of the "first generation" systems, it has been estimated that up to 20% of cellular phone calls are stolen.

Extensive measures have been taken, when specifying the GSM system, to substantially increase security with regard to both call theft and equipment theft.

With GSM, both the Mobile equipment (ME) and Mobile Subscriber are identified. The ME has a unique number coded into it when its is manufactured. This can be checked against a database every time the mobile makes a call to validate the actual equipment. The subscriber is authenticated by use of a smart card known as a Subscriber Identity Module (SIM) again this allows the network to check an MS subscriber against a database for authentication.

GSM also offers the capability to encrypt all signaling over the air interface. Different levels of encryption are available to meet different subscriber/country requirements.

With authentication processes for both the ME and subscriber, together with the encryption and the digital encoding of the air interface signal, it makes it very difficult for the casual "hacker" to listen-in to personal calls.

In addition to this, the GSM air interface supports frequency hopping, this entails each "burst" of information being transmitted to/from the MS/base site on a different frequency again making it very difficult for an observer (hacker) to follow/listen to a specific call [3].

2.6 Flexible Handover Processes

Handovers take place as the MS moves between cells, gradually losing the RF signal of one and gaining that of the other.

The MS switches from channel to channel and cell to cell as it moves to maintain call continuity. With analogue systems, handovers are frequently a problem area and the subscriber is only too well aware that a handover has occurred!

When GSM was specified a great deal of though went into the design and implementation of handovers. Although the GSM system is more complicated than analogue in this area, the flexibility of the GSM handover processes offer significant improvements which provide a much better quality of service to the subscriber.

GSM provides handover processes for the following:

- Quality (uplink/downlink).
- Interference (uplink/downlink).
- RF level (uplink/downlink).
- MS distance.
- Power budget.

More handover algorithms have been developed for specific applications, such as microcellular, and are currently being implemented [1].

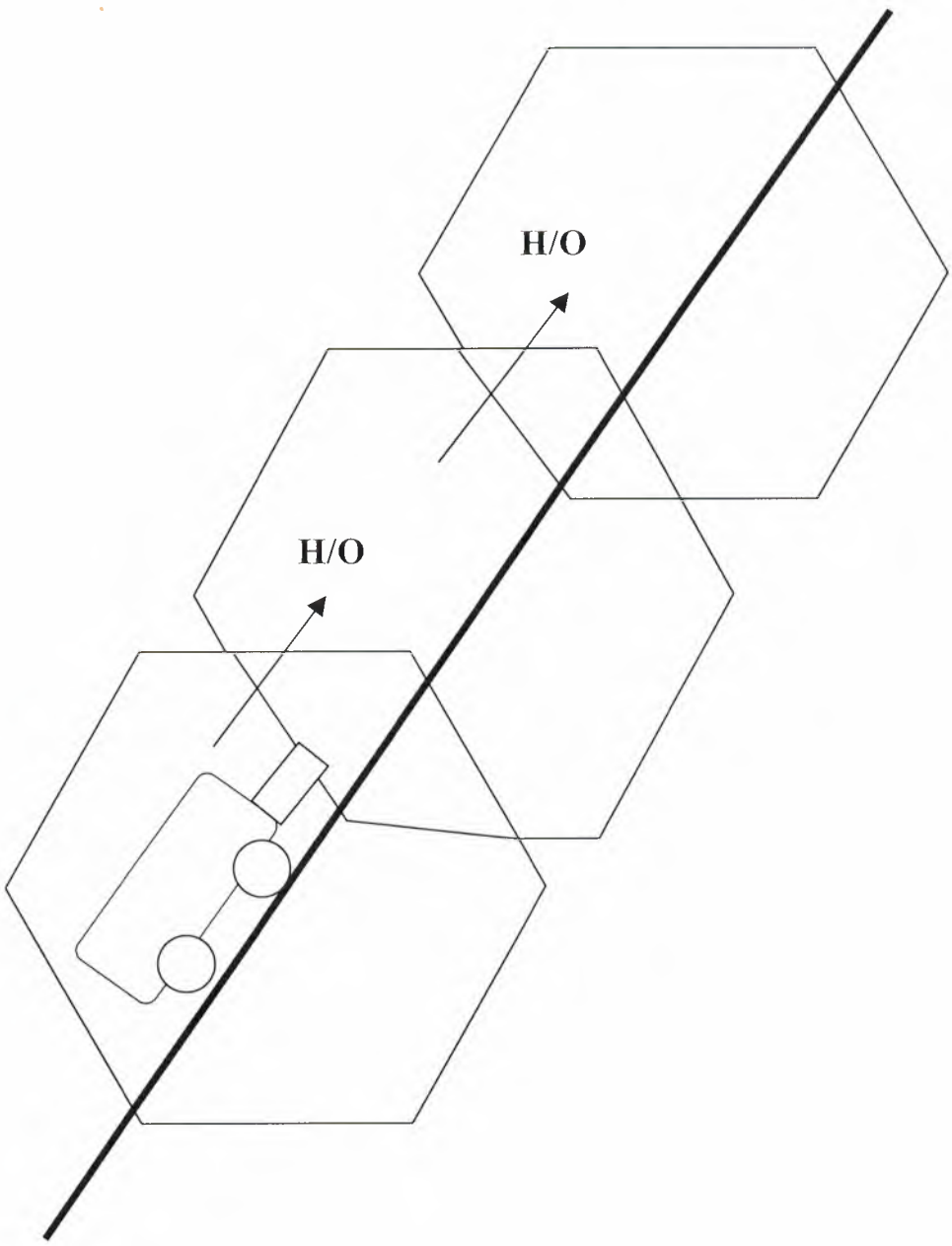


Figure 2.3: Flexible Handover Process

2.7 ISDN Compatibility

Integrated Services Digital Network (ISDN) is a standard that most developed countries are committed to implement. This is a new and advanced telecommunications network designed to carry voice and user data over standard telephone lines.

Major telephone companies in Europe, North America, Hong Kong, Australia and Japan are committed to commercial enterprises using ISDN.

The GSM network has been designed to operate with the ISDN system and provides features, which are compatible with it. GSM can provide a maximum data rate of 9.6 Kbits/s while ISDN provides much higher data rates than this (standard rate 64 Kbits/s, primary rate 2.048 Mbits/s).

2.7.1 2B+D

This refers to the signals and information, which may be carried on an ISDN line. There are effectively three connections, one for signaling ('D') and the other two for data or speech ('2B') [2].

Note:

1.B = 64 Kbits/s

2.D = 16 Kbits/s

2B+D = 144 Kbits/s

2.8 Enhanced Range of Services

GSM has the potential to offer a greatly enhanced range of services compared to existing analogue cellular systems. As well as a full range of data transmission options and fax, there will be a wide range of supplementary services.

The basic call services, which are already provided within analogue systems such as Call Forwarding, Voice Massage Services etc, are already available in some operational systems. Whether these services and others are provided as part of the basic service or at additional cost to the subscriber will depend on the network provider [1].

The services available to a subscriber will be determined by three factors:

- The level of service provided by the network provider.
- The level of service purchased by the subscriber.
- The capabilities of the subscriber's mobile equipment.

2.8.1 Speech Services

The following services listed involve the transmission of speech information and would make up the basic service offered by a network provider:

Telephony

Provides for normal MS originated/terminated voice calls.

Emergency Calls (with/without SIM Card Inserted in MS)

The number "112" has been agreed as the international emergency call number. This should place you in contact with the emergency services (Police, Fire, Ambulance) whichever country you are in.

Short Message Service Point to Point

Provides the transmission of an acknowledged short message (128 bytes maximum) from a service center to a MS. It is also intended that the MS should be able to send short messages to land-based equipment. This will obviously depend upon the equipment owned by the land-based user.

Short Message Cell Broadcast

Provides the transmission of an unacknowledged short message (75 bytes maximum) from a service center in the fixed network to all MSs within one cell. This may carry information from the network provider, for example traffic information or advertising.

Advanced Message Handling Service

Provides message submission and delivery from the storage from a public Message Handling System (MHS) for example, electronic mail.

Duel Personal and Business Numbers

Permits the allocation of duel telephone numbers to a single subscriber. This will allow calls to be made and be billed either "business" or "personal" numbers [1].

2.8.2 Data services

Data can be sent over the air using some of the present systems, but this requires specially designed "add ons" to protect the data content in the harsh environment of the air interface.

Special provision is made in the GSM technical specifications for data transmission. Therefore, like ISDN, GSM is "specially designed" for data transmission. GSM can be considered as an extension of ISDN info the wireless environment.

Text files, images, messages and fax may all be sent over the GSM network. The data rates available are 2.4 kbits/s and 9.6 kbits/s[1].

Below is a list of the various forms of data service that GSM will support.

- **Videotex Access**

  Provides access to computer-based information stored in databases, utilizing public transmission networks, where the requested information is generally in the form of text and/or pictures.

- **Teletex**

  Provides for data transfer in a circuit or packet-switched network (ITU-TSS X.200) (that is, document transmission).

- **Alternate Speech and Facsimile Group 3**

  Allows the connection of ITU-TS group 3 FAX apparatus (send and/or receive) to the MS.

2.8.3 Supplementary Services

A supplementary service is a modification of, or a supplement to, a basic telecommunication service. The network provider will probably charge extra for these services or use them as an incentive to join their network.

Here is a list of some of the optional supplementary subscriber services that could be offered to GSM subscriber.

Number Identification

- Receiving party requests calling number to be shown.
- Calling party requests calling number not to be shown.

Call Barring

- Bar all incoming or all outgoing calls.
- Bar specific incoming or outgoing calls.

Call Forwarding

- Forward all calls.
- Forward calls when subscriber is busy.
- Forward calls if subscriber does not answer.
- Forward calls if subscriber cannot be located.

Call Completion

- Enable incoming call to wait until subscriber completes current call.
- Enable subscriber to place incoming calls on hold.

Charging

- Display current cost of call.

Multi-Party

- Three party service.
- Conference calling [1].

GSM SYSTEM ARCHITECTURE

Chapter 3

GSM Network Components

3.1 GSM Network Overview

The diagram opposite shows and simplified GSM network. Each network component is illustrated only once, however, many of the components will occur several times throughout a network.

Each network component is designed to communicate over an interface specified by the GSM standards. This provides flexibility and enables a network provider to utilize system components from different manufacturers. For example Motorola Base Station System (BSS) equipment may be coupled with an Ericsson Network Switching System.

The principle component groups of a GSM network are:

- **The Mobile Station (MS)**

  This consists of the mobile telephone, fax machine etc. This is the part of the network that the subscriber will see.

- **The Base Station System (BSS)**

  This is the part of the network, which provides the radio interconnection from the MS to land-based switching equipment.

- **The Network Switching System**

  This consists of the Mobile services Switching Center (MSC) and its associated system-control databases and processors together with the required interfaces.

  This is the part which provides for interconnection between the GSM network and the publi9c switched Telephone Network (PSTN).

- **The Operations and Maintenance System**

  This enables the network provider to configure and maintain the network from a central location [1].

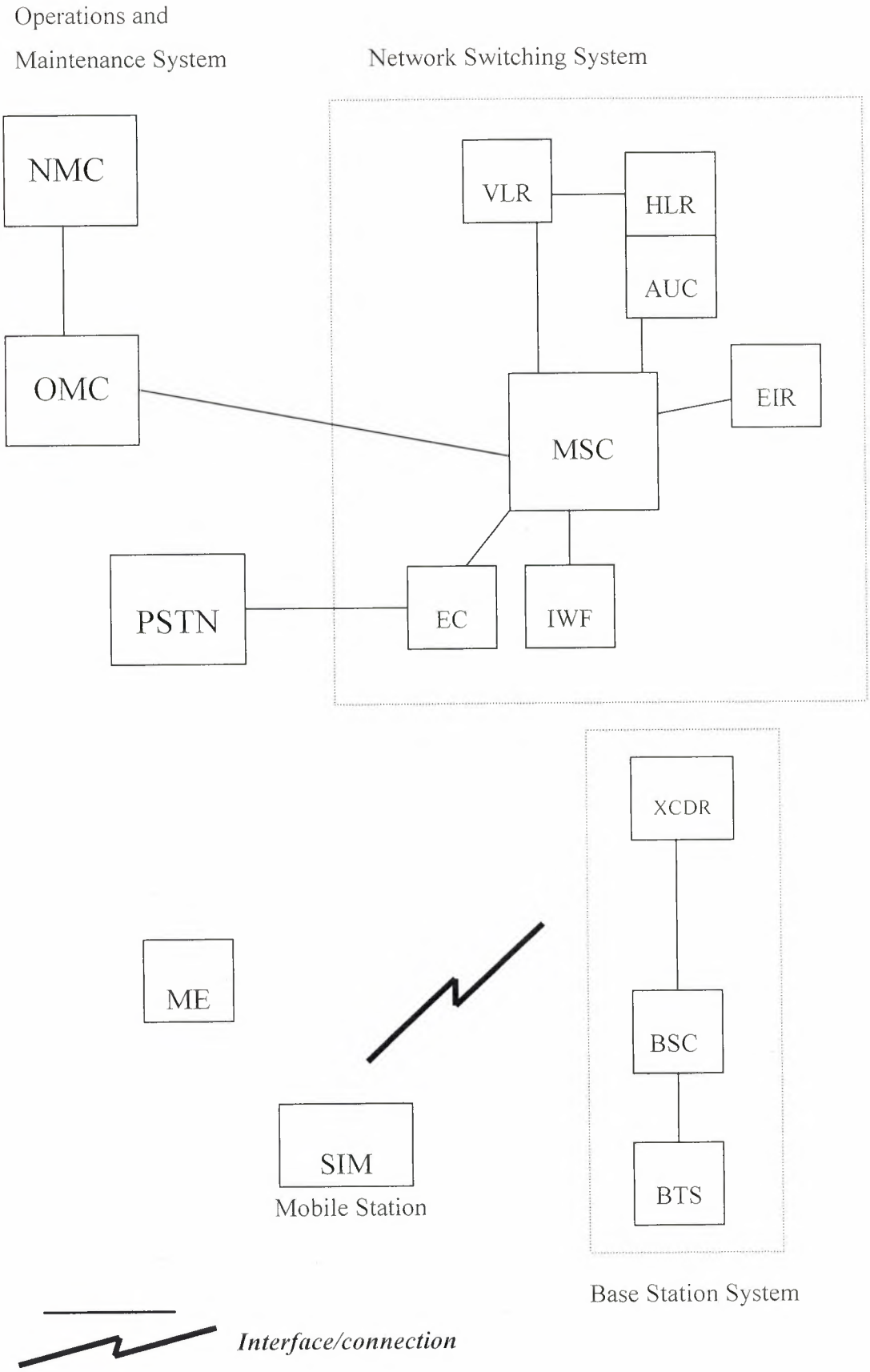


Figure3.1: GSM Network Components

3.2 Mobile Station –MS

The MS consists of two parts, the mobile Equipment (ME) and an electronic 'smart card' called a Subscriber Identity Module (SIM).

The ME is the hardware used by the subscriber to access the network. The hardware has an identity number associated with it, which is unique for that particular device and permanently stored in it. This identity number is called the International Mobile Equipment Identity (IMEI) and enables the network operator to identify mobile equipment which maybe causing problems on the system.

The SIM is a card, which plugs into the mobile equipment. This card identifies the mobile subscriber and also provides other information regarding the service that subscriber should receive. An identity number called the International Mobile Subscriber Identity (IMSI) identifies the subscriber.

Mobile equipment may be purchased from any store but the SIM must obtained from the GSM network provider. Without the SIM inserted, the ME will only be able to make emergency calls.

By making a distance between the subscriber identity and the ME identity, GSM can route calls and perform billing based on the identity of the 'subscriber' rather than equipment or its location [1].

3.3 Mobile Equipment – ME

The ME is the only part of the GSM network, which the subscriber will really see. There are three main types of ME, these are listed below:

- **Vehicle Mounted**

  These devices in a vehicle and the antenna are physically mounted on the outside of the vehicle.

- **Portable Mobile Unit**

  This equipment can be handheld when in operation, but the antenna is not connected to the handset of the unit.

- **Handportable unit**

  This equipment comprises of a small telephone handset not much bigger than a calculator. The antenna is being connected to the handset.

The ME is capable of operating at a certain maximum power output dependent on its type and use.

These mobile types have distinct features, which must be known by the network, for example their maximum transmission power, and the services they support. The ME is therefore identified by means of a class mark. The classmark is sent by the ME in its initial message.

The following pieces of information are held in the classmark:

- **Revision level -**

  Identifies the phase of the GSM specifications that the mobile complies with.

- **RF power Capability**

  The maximum power is able to transmit, used for power control and handover preparation. This information is held in the mobile power class number.

- **Ciphering Algorithm**

Indicates which ciphering algorithm is implemented in MS. There is only one algorithm (A5) in GSM phase 1, but GSM phase 2 specifies different algorithm (A5/0-A5/7).

- **Frequency Capability**

  Indicates the frequency bands the MS can receive and transmit on. Currently all GSM MSs use one frequency band, in the future this band will be extended but not all MSs will be capable of using it.

- **Short Messages Capability**

  Indicates whether the MS is able to receive short messages [3].

Mobile Equipment capabilities

- **RF Power capability**

Power Class	Power Output
1	20 Watt (deleted)
1	8 Watts
3	5 Watts
4	2 Watts
5	0.8 Watts

- **Supports of phase 1 or phase 2 specification**
- **Encryption capability**
- **Frequency capability**
- **Short Messages Services capability**

3.4 Subscriber Identity Module – SIM

The SIM as mentioned previously is a card " smart card " which
Plugs into the ME and contains information about the MS subscriber hence the name Subscriber Identity Module.

The SIM contains several pieces of information:

- **International Mobile Subscriber Identity (IMSI)**
  This number identifies the MS subscriber. It is only transmitted over the air during initialization.

- **Temporary Mobile Subscriber Identity (TMSI)**
  This number identifies the subscriber, it is periodically changed by the system management to protect the subscriber from being identified by someone attempting to monitor the radio interface.

- **Location Area Identity (LAI)**
  Identifies the current location of the subscriber.

- **Subscriber Authentication key (Ki)**
  This is used to authenticate the SIM card.

- **Mobile Station International Services Digital Network (MSISDN)**
  This is the telephone number of the mobile subscriber. It is comprised of a country code, a national code and a subscriber number.

Most of the data contained within the SIM is protected against reading (ki) or alterations (IMSI). Some of the parameters (LAI) will be continuously updated to reflect the current location of the subscriber.
The SIM card, and the high degree of inbuilt system security, provides protection of the subscriber's information and protection of the network against access. SIM cards are designed to be difficult to duplicated. The SIM can be protected by use of Personal

Identity Number (PIN) password, similar to bank/credit charge cards, to prevent unauthorized use of the card.

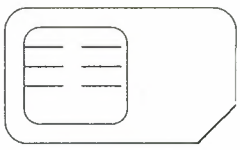
The SIM is capable of storing additional information such as accumulated call charges. This information will be accessible to the customer via handset/keyboard key entry.

The SIM is also executes the Authentication Algorithm [3].

SIM CARD

(Actual size)

Full Size SIM Card



Mini SIM Card

Figure 3.2: Subscriber Identity Module (SIM)

3.5 Base Station System – BSS

The GSM Base Station System is the equipment located at a cell site. It comprises a combination of digital and RF equipment. The BSS provides the link between the Mobile Station (MS) and the Mobile services Switching Centre (MSC).

The BSS communicates with the MS over the digital air interface and with the MSC via 2 Mbit/s links.

The BSS consists of three major hardware components:

- **The Base Transceiver Station – BTS**

  The BTS contains the RF components that provide the air interface for a particular cell. This is the part of the GSM network, which communicates with the MS. The antenna is included as part of the BTS.

- **The Base Station Controller – BSC**

  The BSC as its name implies provides the control for the BSS. The BSC communicates directly with the MSC. The BSC may control single or multiple BTSs.

- **The Transcoder (XCDR)**

  The Transcoder is used to compact the signals from the MS so that they are more efficiently sent over the terrestrial interfaces. Although the Transcoder is considered to be a part of the BSS, it is very often located closer to the MSC.

The transcoder is used to reduce the rate at which the traffic (voice/data) is transmitted over the air interface. Although the transcoder is part of the BSS, it is often found physically closer to the NSS to allow move efficient use of the terrestrial links [1].

BSS

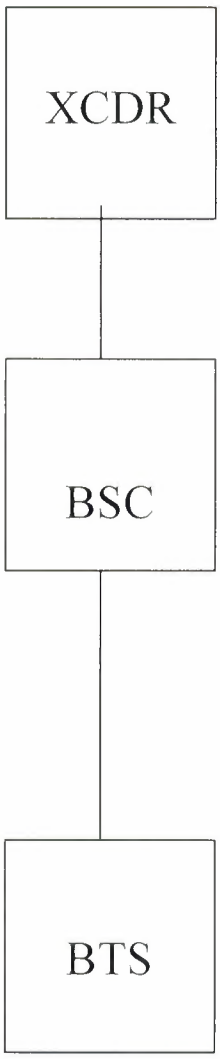


Figure 3.3: Base Station System (BSS)

3.5.1 Base Station Controller—BSC

As previously mentioned, the BSC provides the control for the BSS. The functions of the BSC are shown in the table opposite.

Any operational information required by the BTS will be received via the BSC. Likewise any information required about the BTS (by the OMC for example) will be obtained by the BSC.

The BSC incorporates a digital switching matrix, which it uses to connect the radio channels on the air interface with the terrestrial circuits from the MSC.

The BSC switching matrix also allows the BSC to perform "handover" between radio channels on BTSs, under its control, without involving the MSC.

3.5.2 Base Transceiver Station — BTS

The BTS provides the air interface connection with the MS. It also has a limited amount of control functionality, which reduces the amount of traffic passing between the BTS and BSC. The functions of the BTS are shown opposite. Each BTS will support 1 or more cells 1711.

BSS Functionality	Control
Terrestrial Channel Management	
Channel Allocation	BSC
Transcoding *I* Rate Adaption	BSC
Radio Channel Management	BSC
Channel Configuration Management	BSC
Handover Control	BSC
Frequency Hopping	BSC[BTS
Traffic Channel Management	BSC/BTS
Control Channel Management	BSC/BTS
Encryption	BSC/BTS
Paging	BSC/BTS
Power Control	BSC/BTS
Channel Coding / Decoding	BTS
Timing Advance	BTS
Idle Channel Observation	BTS
Measurement Reporting	BTS

Where the BSC and BTS are both shown to control a function, the control is divided between the two, or may be located wholly at one.

3.5.3 BSS Configurations

As we have mentioned, a BSC may control several BTSs, the maximum number of BTSs, which may be controlled by one BSC, is not specified by GSM.

Individual manufacturer's specifications may very greatly.

The BTSs and BSC may either be located at the same cell site "Colocated", or located at different sites "Remote". In reality most BTSs will be remote, as there are many more BTSs in a network.

Another BSS configuration is the Daisy Chain. A BTS need not communicate directly with the BSC, which controls it, it can be connected to the BS~ via a chain of BTSs.

Daisy chaining reduces the amount of cabling required to set up a network as a BTS can be connected to its nearest BTS rather than all the way to the BSC.

Problems may arise when chaining BTSs, due to the transmission delay through the chain. The length of the chain must, therefore, be kept sufficiently short to prevent the round trip speech delay becoming too long.

Other topologies are also permitted including stars and loops. Loops are used to introduce redundancy into the network, for example if a BTS connection was lost, the BSC may still be able to communicate with the BSC if a second connection is available [1].

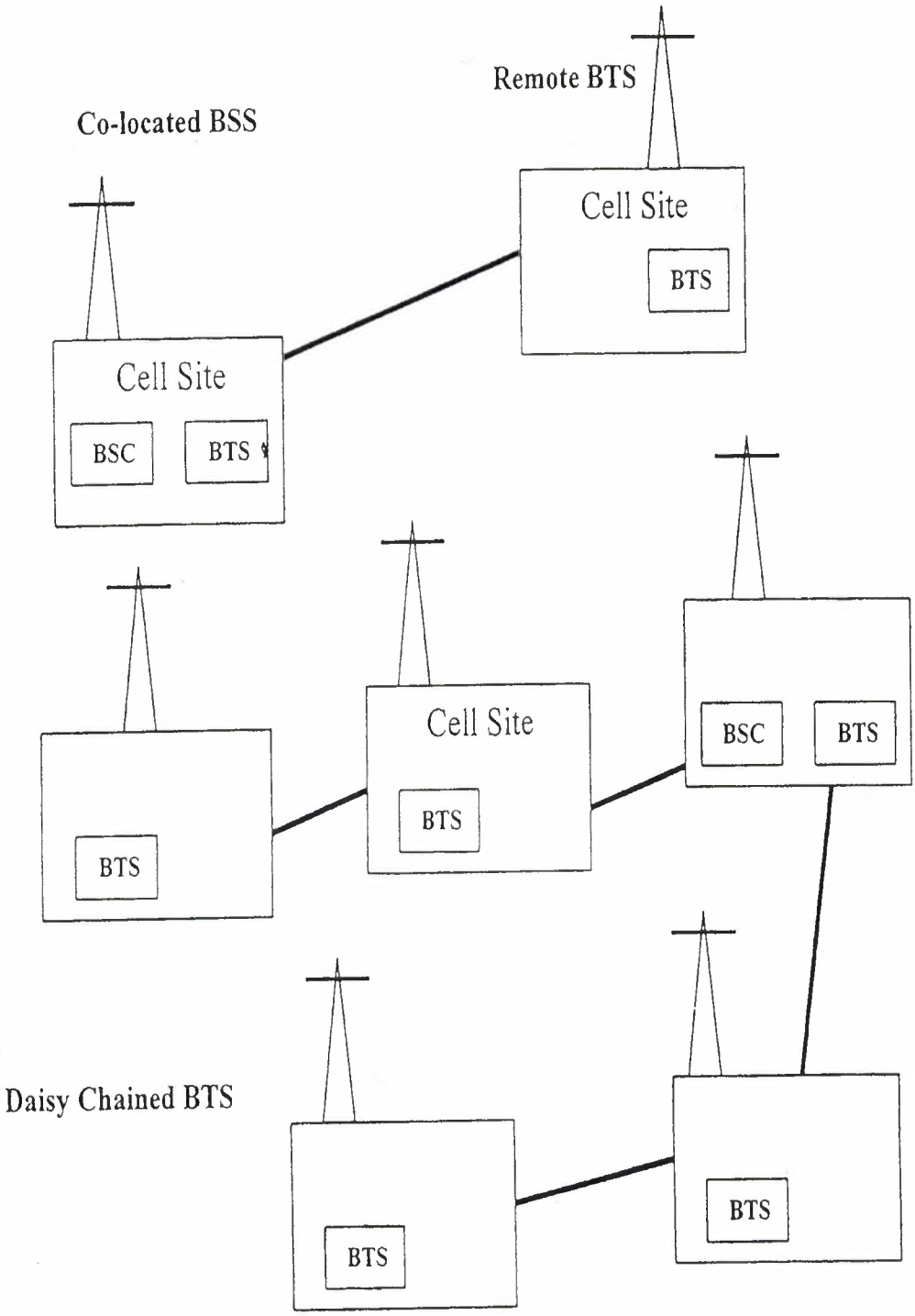


Figure 3.4: BSS Configurations

3.5.4 The Transcoder (XCDR)

The Transcoder is used to compact the signals from the MS so that they are more efficiently sent over the terrestrial interfaces. Although the Transcoder is considered to be a part of the BSS, it is very often located closer to the MSC.

The transcoder is used to reduce the rate at which the traffic (voice/data) is transmitted over the air interface. Although the transcoder is part of the BSS, it is often found physically closer to the NSS to allow move efficient use of the terrestrial links [1].

The Transcoder (XCDR) is required to convert the speech or date output from MSC (64 kbit/s PCM), into the form specified by GSM specifications for transmission over the air interface that is, between the BSS and MS (64 kbit/s to 16 kbit/s and vice versa).

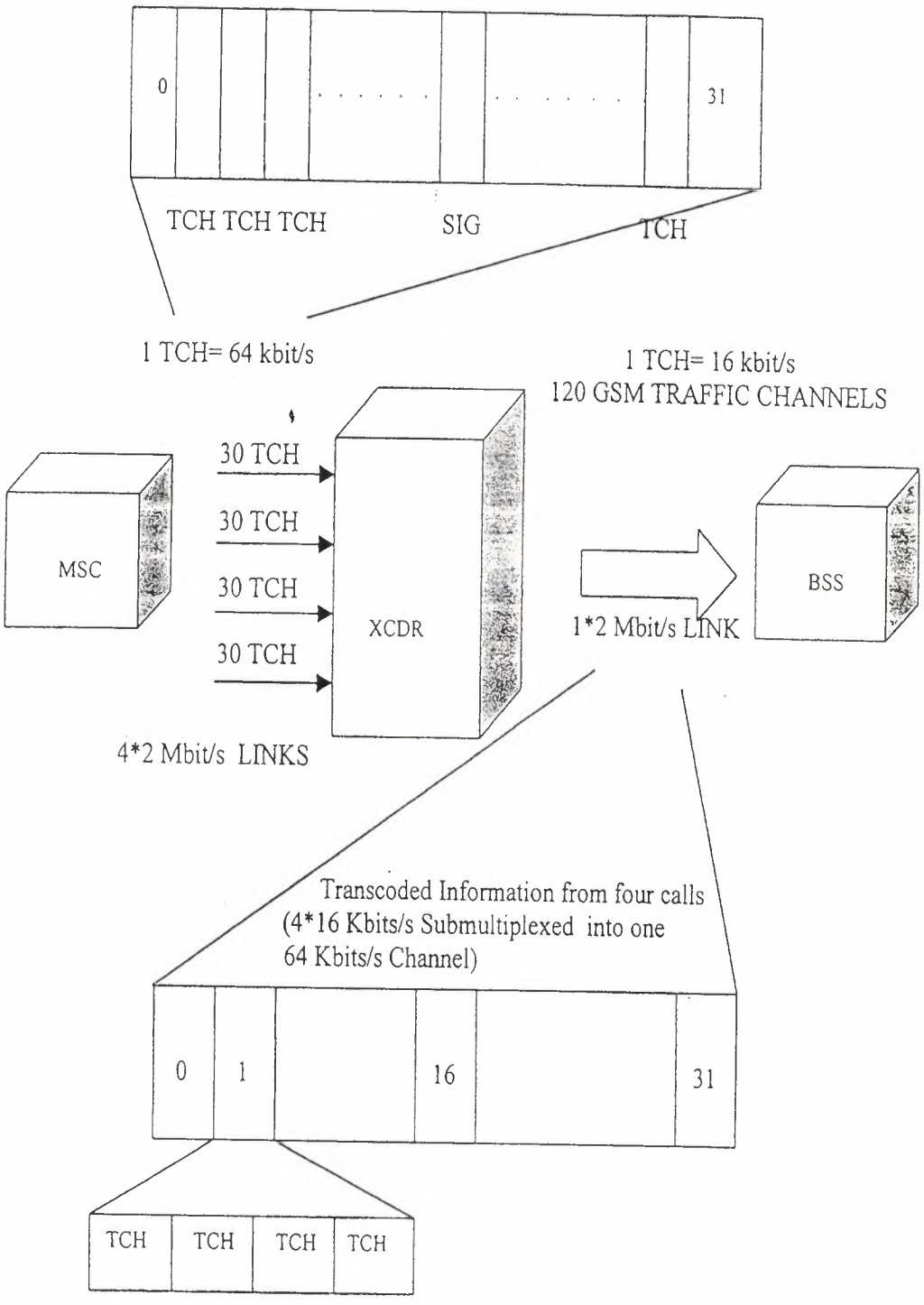
The 64 kbit/s Pulse Code Modulation (PCM) circuits from the MSC, if transmitted on the air interface without modification, would occupy an excessive amount of radio bandwidth. This would use the variable radio spectrum inefficiently. The required bandwidth is therefore reduced by processing the 64 kbit/s circuits that the amount of information required to transmit digitized voice falls 13 kbit/s.

The transcoding function may be located at the MSC, BSC, or BTS.

A Transcoder Rate Adaption Unit (TRAU) of 3 kbit/s is added to the 13 kbit/s channel leaving the tanscoding function to form a gross traffic channel of 16 kbit/s, which is transmitted, over the terrestrial interfaces to the BTS. At the BTS the TRAU is removed and the 13 kbit/s is processed to form a gross rate of 22.8 kbit/s for transmission over the air interface.

For data transmissions the data is not transcoded but data rate adapted from 9.6 kbit/s (4.8 kbit/s or 2.4 kbit/s may also be used) up to a gross rate of 16 kbit/s for transmission over the terrestrial interfaces, again this 16 kbit/s contains a 3 kbit/s TRAU.

As can be seen from the diagram opposite, although the reason for transcoding was to reduce the data rate over the air interface, the number of terrestrial links is also reduced approximately on 4:1 ratio [3].



(C7)
Information Control

Figure 3.5: Transcoder

3.6 Network Switching System

The Network Switching System includes the main switching functions of the GSM network. It also contains the databases required for subscriber data and mobility management. Its main function is to manage communications between the GSM network and other telecommunications network.

The components of the Network Switching System are listed below:

- Mobile Services Switching Centre — MSC
- Home Location Register — HLR
- Visitor Location Register — VLR
- Equipment Identify Register — EIR
- Authentication Centre — AUC
- InterWorking Function — JWF
- Echo Canceller — EC

In addition to the more traditional elements of a cellular telephone system, GSM has Home Location Register entities. These entities are the Home Location Register (HLR), Visitor Location Register (VLR), and the Equipment Identify register (EIR). The location register are databased-oriented processing nodes which address the problems of managing subscriber data and keeping track of a MSs location as it roams around the network.

Functionally, the Interworking Function and Echo Cancellers may be considered as parts of the MSC, since their activities are inextricably liked with those of the switch as it connects speech and data calls to and the MSs [3].

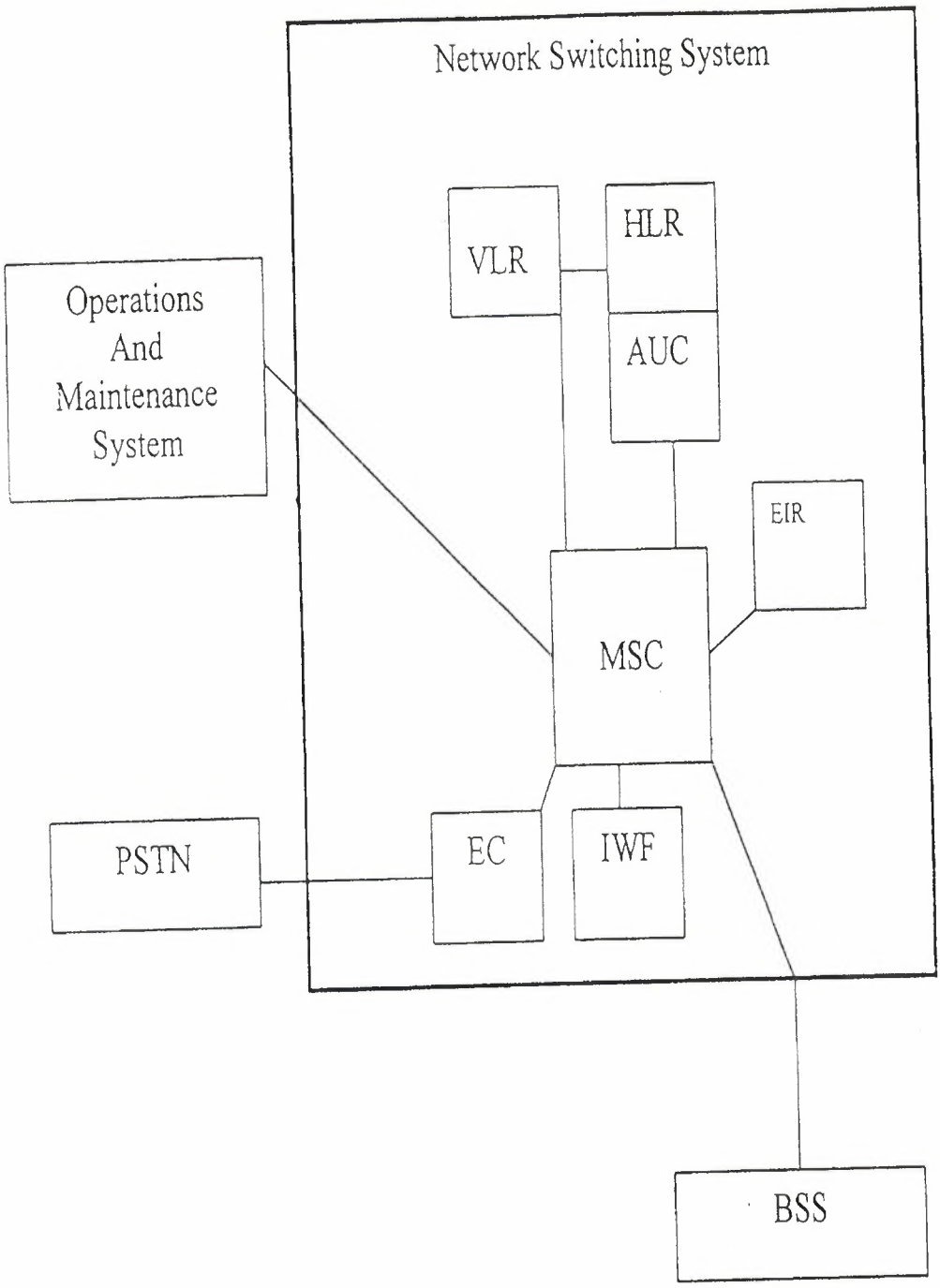


Figure 3.6: The Network Switching System Block diagram

3.6.1 Mobile Services Switching Centre – MS

The MSC is included in the GSM system for call-switching. Its overall purpose is the same as that of any telephone exchanger.

However, because of the additional complications involved in the control and security aspects of the GSM cellular system and the wide range of subscriber facilities that it offers, the MSC has to be capable of fulfilling many additional functions.

The MSC will carry out several different functions depending upon its position in the network. When the MSC provides the interface between the PSTN and the BSSs in the GSM network it will be known as a Gateway MSC. In this position it will provide the switching required for all MS originated or terminated traffic.

Each MSC provides service to MSs located within a defined geographic coverage area, the network typically contains more than one MSC. One MSC is capable of supporting a regional capital with approximately one million in habitants. An MSC of this size will be contained in about half a dozen racks.

The functions carried out by the MSC are listed below:

- **Call Processing**

  Includes control of data/voice call setup, inter-BSS and inter-MSC handovers and control of mobility management (subscriber validation and location).

- **Operations and Maintenance Support**

  Includes database management, traffic metering and measurement, and a man-machine interface.

- **Internetwork and Interworking**

  Manages the interface between the GSM network and the PSTN.

- **Billing**

  Collects call billing data [1].

3.6.2. Home Location Register – HLR

The HLR is the reference database for subscriber parameter.

Various identification numbers and addresses are stored, as well authentication parameters. This information is entered into the database by the network provider when a new subscriber is added to the system.

The parameters stored in the HLR are listed below:

The HLR database contains the master database of all the subscribers to a GSM PLMN. The data it contains is remotely accessed by all the MSCs and VLRs in the network and, although the network may contain more than one HLR, there is only one database record per subscriber – each HLR is therefore handling a portion of the total subscriber database. The subscriber data may accessed by either the IMSI or MSISDN number. The data can also be accessed by an MSC or a VLR in a different PLMN, to allow inter-system and inter-country roaming [1].

Home Location Register

(HLR)

- **Subscriber ID (IMSI and MSISDN)**
- **Current subscriber VLR (current location)**
- **Supplementary services subscriber to**
- **Supplementary services information (e.g. current forwarding number)**
- **Subscriber status (registered/deregistered)**
- **Authentication key and AUC functionality**
- **Mobile Subscriber Roaming Number (MSRN)**

3.6.3 Visitor Location Register – VLR

The VLR contains a copy of most of the data stored at the HLR. It is, however, temporary data which exists for only as the subscriber is "active" in the particular area covered by the VLR. The VLR database will therefore contain some duplicate data as well as more precise data relevant to the subscriber remaining within the VLR coverage. The VLR provides a local database for the subscribers wherever they are physically located within a PLMN, this may not be the "home" system. This function eliminates the need for excessive and time-consuming references to the "home" HLR database. The additional data stored in the VLR is listed below:

- Mobile status (busy/free/answer etc.).
- Location Area Identity (LAI).
- Temporary Mobile Subscriber Identity.
- Mobile Station Roaming Number.

3.6.3.1 Location Area Identity

Cells within the Public Land Mobile Network (PLMN) are grouped together into geographical areas. Each area is assigned a Location Area Identity (LAI), a location area may typically contain 30 cells. Each VLR controls several LAIs and as a subscriber moves from one LAI to another, the LAI is updated in the VLR. As the subscriber moves from one VLR to another, the VLR address is updated at the HLR.

3.6.3.2 Temporary Mobile Subscriber Identity

The VLR controls the allocation of new Temporary Mobile Subscriber Identity (TMSI) numbers and notifies them to the HLR. The TMSI will be updated frequently, this makes it very difficult for the call to be traced and therefore provides a high degree of security for the subscriber. The TMSI may be updated in any of the following situations:

- Call setup.
- On entry to a new LAI.
- On entry to a new VLR.

3.6.3.3 Mobile Subscriber Roaming Number

As a subscriber may wish to operate outside its "home" system at some time, the VLR can also allocate a Mobile Station Roaming Number (MSRN). This number is assigned from a list of number held at the VLR (MSC). The MSRN is then used to route the call to the MSC, which controls the base station in the MSs current location.

The database in the VLR can be accessed by the IMSI, the TMSI or the MSRN.

Typically there will be one VLR per MSC [1].

3.6.4 Equipment Identity Register –EIR

The EIR contains a centralized database for validating the International Mobile Equipment Identity (IMEI).

This database is concerned solely with MS equipment and not with the subscriber who is using it to make or receive a call.

The EIR database consists of lists of IMEIs (or ranges of IMEIs) organized as follows:

- **White List**

  Contains those IMEIs, which are known to have been assigned to valid MS equipment.

- **Black List**

  Contains IMEIs of MS, which have been reported stolen, or which are to be denied service for some other reason.

- **Grey List**

  Contains IMEIs of MS, which have problems (for example, faulty software). These are not, however, sufficiently significant to warrant a "black listing".

The EIR database is remotely accessed by the MSCs in the network and can also be accessed by an MSC in a different PLMN.

As in the case of the HLR, a network may well contain more than one EIR with each EIR controlling certain blocks of IMEI number. The MSC contains a translation facility, which when given an IMEI, returns the address of the EIR controlling the appropriate section of the equipment database [3].

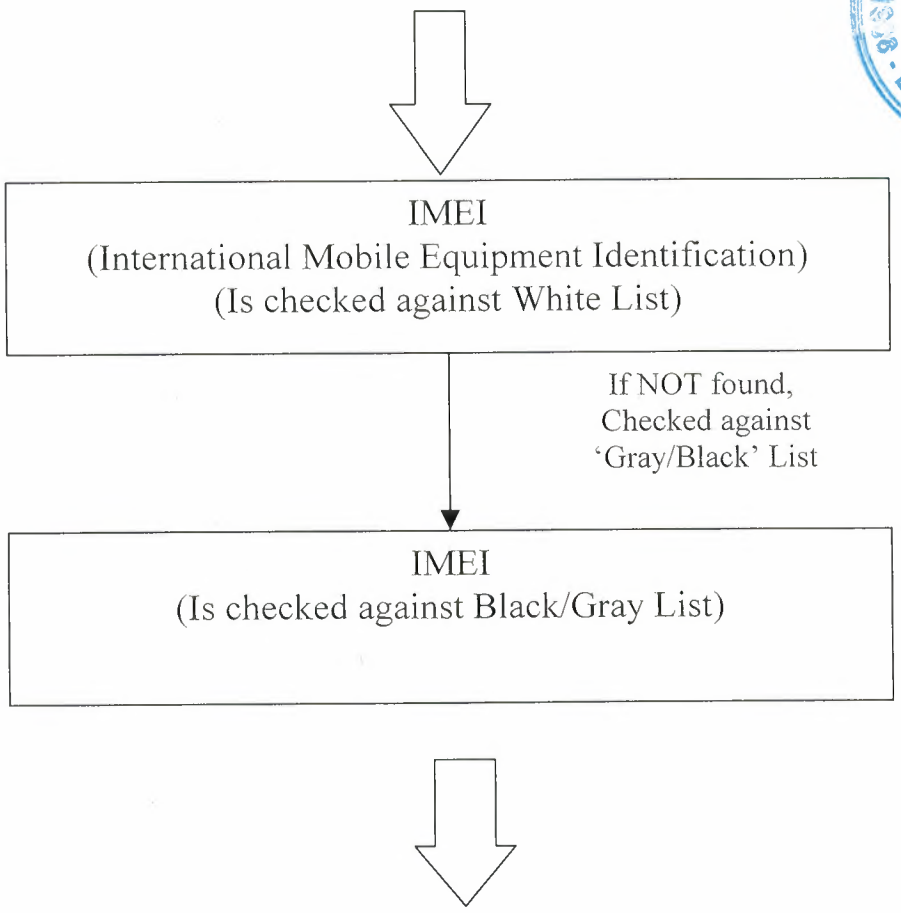


Figure 3.7: Call Processing Functions (EIR)

3.6.5 Authentication Centre – AUC

The AUC is a processor system, it performs the "authentication" function.

It will normally be co-located with the Home Location Register (HLR) as it will be required to continuously access and update, as necessary, the system subscriber records. The AUC/HLR centre can be co-located with the MSC or located remote from the MSC.

The authentication process will usually take place each time the subscriber "initializes" on the system.

3.6.5.1 Authentication Process

To discuss the authentication process we will assume that the VLR has all the information required to perform that authentication process (Kc, SRES and RAND). If this information is unavailable, then VLR would request it from the HLR/AUC.

1. Triples (Kc, SRES and RAND) are stored at the VLR, each triple is allocated a Cipher Key Sequence Number (CKSN).
2. The VLR sends RAND and CKSN of a triple, via the MSC and BSS, to the MS (unencrypted).
3. The MS, using the A3 and A8 algorithms and the parameter Ki stored on the MS SIM card, together with the received RAND from the VLR, calculates the values of SRES and Kc.
4. The MS sends SRES and CKSN unencrypted to the VLR.
5. Within the VLR the value of SRES is compared with the SRES of the triple for the specified CKSN. If the two values match, the authentication is successful.
6. Kc from the assigned triple is now passed to the BSS.
7. The mobile calculates Kc from the RAND and A8 and Ki on the SIM.
8. Using KC, A5 and the GSM hyperframe number, encryption between the MS and the BSS can now occur over the air interface [1].

Note: The triples are generated at the AUC by:

RAND = Randomly generated number.

SRES = Derived from A3 (RAND, Ki).

Kc = Derived from A8 (RAND, Ki).

A3 = From 1 of 16 possible algorithms defined on allocation of IMSI and creation of SIM card.

A8 = From 1 of 16 possible algorithms defined on allocation of IMSI and creation of SIM card.

Ki = Authentication key, assigned at random together with the versions of A3 and A8.

The first time a subscriber attempts to make a call, the full authentication process takes place.

However, for subsequent calls attempted within a given system control time period, or within a single system provider's network, authentication may necessary, as the data generated during the first authentication will still be available [1].

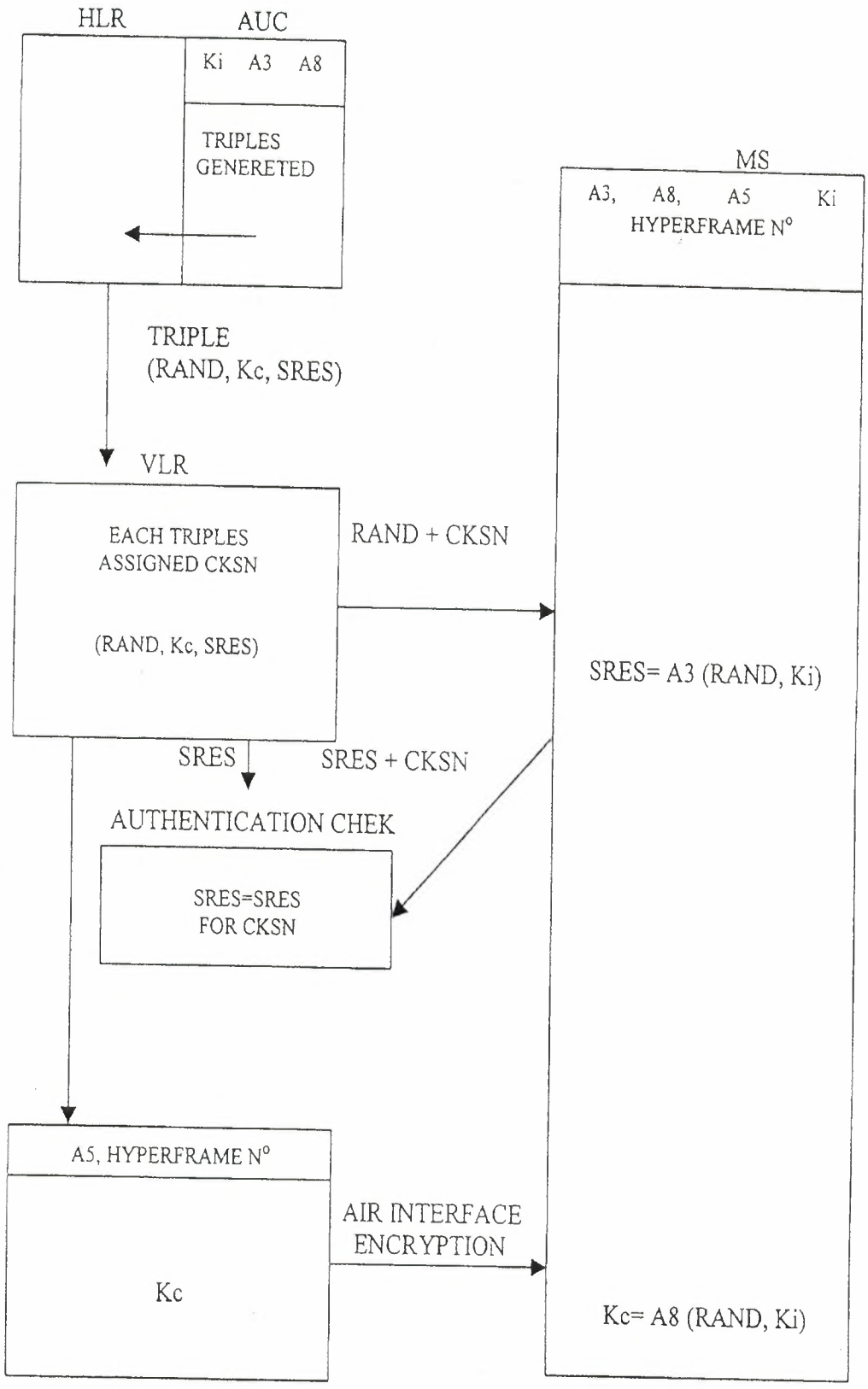


Figure 3.8: Authentication Process

3.6.6 InterWorking Function – IWF

The IWF provides the function to enable the GSM system to interface with the various forms of public and private data networks currently available.

The basic features of the IWF are listed below:

- Data rate adaption.
- Protocol conversion.

Some systems require more IWF capability than others, this depends upon the network to which it is being connected.

The IWF also incorporates a "modem bank", which may be used when, for example, the GSM **Data Terminal Equipment (DTE)** exchanges data with a land DTE connected via an analogue modem [3].

3.6.7 Echo Canceller – EC

An Echo Canceller is used on the PSTN side of the MSC for all voice circuits. Echo control is required at the switch because the inherent GSM system delay can cause an unacceptable echo condition, even on short distance PSTN circuit connections.

The total round trip delay introduced by the GSM system (the cumulative delay caused by call processing, speech encoding and decoding etc) is approximately 180 ms. This would not be apparent to the MS subscriber, but for the inclusion of a 2-wire to 4-wire hybrid transformer in the circuit. This is required at the land party's local switch because the standard telephone connection is 2-wire. The transformer causes the echo. This does not affect the land subscriber.

During a normal PSTN land to land call, no echo is apparent because the delay is too short and the user is unable to distinguish between the echo and the normal telephone "side tone". However, without the EC and the GSM round trip delay added, the effect would be very irritating to the MS subscriber, disrupting speech and concentration.

The standard EC will provide cancellation of up to 68 milliseconds on the "tail circuit" (the tail circuit is the connection between the output of the EC and the land telephone) [3].

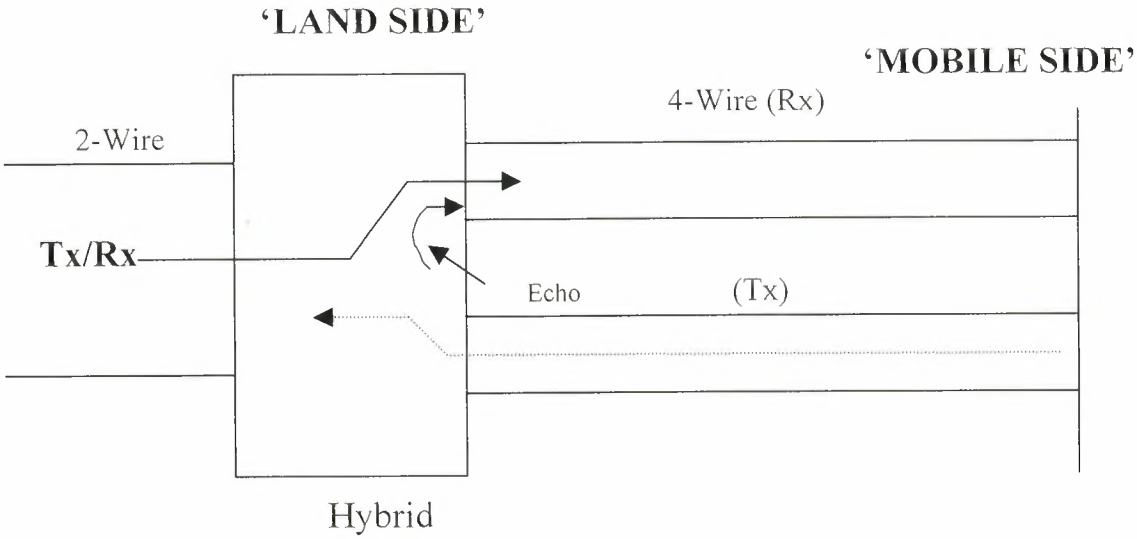


Figure 3.9: Generation of Echoes at 2-Wire to 4-Wire interface

3.7 Operations and Maintenance System

The operations and maintenance system provides the capability to manage the GSM network remotely.

This area of the GSM network is not currently tightly specified by the GSM specification, it is left to the network provider to decide what capabilities they wish it to have. The Operations and Maintenance System comprises of two parts:

3.7.1 Network Management Centre –NMC

The network management centre (NMC) has a view of the entire PLMN and is responsible fort the management of the network as a whole.

The NMC resides at the hierarchy and provides global network management.

3.7.2 Operation and Maintenance Centre – OMC

The operations and Maintenance Centre (OMC) is a centralized facility that supports the day management of a cellular network as well as providing a database for long term network engineering and planing tools. An OMC manages a certain area of the PLMN thus giving regionalized network management [1].

Operations & Maintenance System

OMC (REGIONAL)	NMC (GLOBAL)
Multiple OMCs per network	Single NMC per network
Regionalized network management	Global network management
Employed in daily operations	Employed in long term planning
Used by network operators	Used by network management and planners
	24 hours supervision

3.8 Network Management Centre – NMC

The NMC offers the ability provider hierarchical regionalized network management of a complete GSM system.

It is responsible for operations and maintenance at the network level, supported by the OMC, which are responsible for regional network management.

The NMC is therefore a single logical facility at the top of the network management hierarchy.

The NMC has a high level view of the network, as a series of network nodes and interconnecting communication facility. The OMC, on the other hand, is used to filter information from the network equipment for forwarding to the NMC, thus allowing it to focus on issues requiring national co-ordination. The NMC can also co-ordinate issues regarding interconnection to other networks, for example the PSTN.

The NMC can take regional responsibility when an OMC is not manned, with the OMC acting as a transit point between the NMC and the network

equipment. The NMC provides operators with functions equivalent to those available at the OMC [3].

Functionality of the NMC
Monitors nodes on the network
Monitors GSM Network Element Statistics
Monitors OMC regions & provides information to OMC staff
Passes on statistical information from one OMC region to another to improve problem solving strategies
Enable long term planning for the entire network

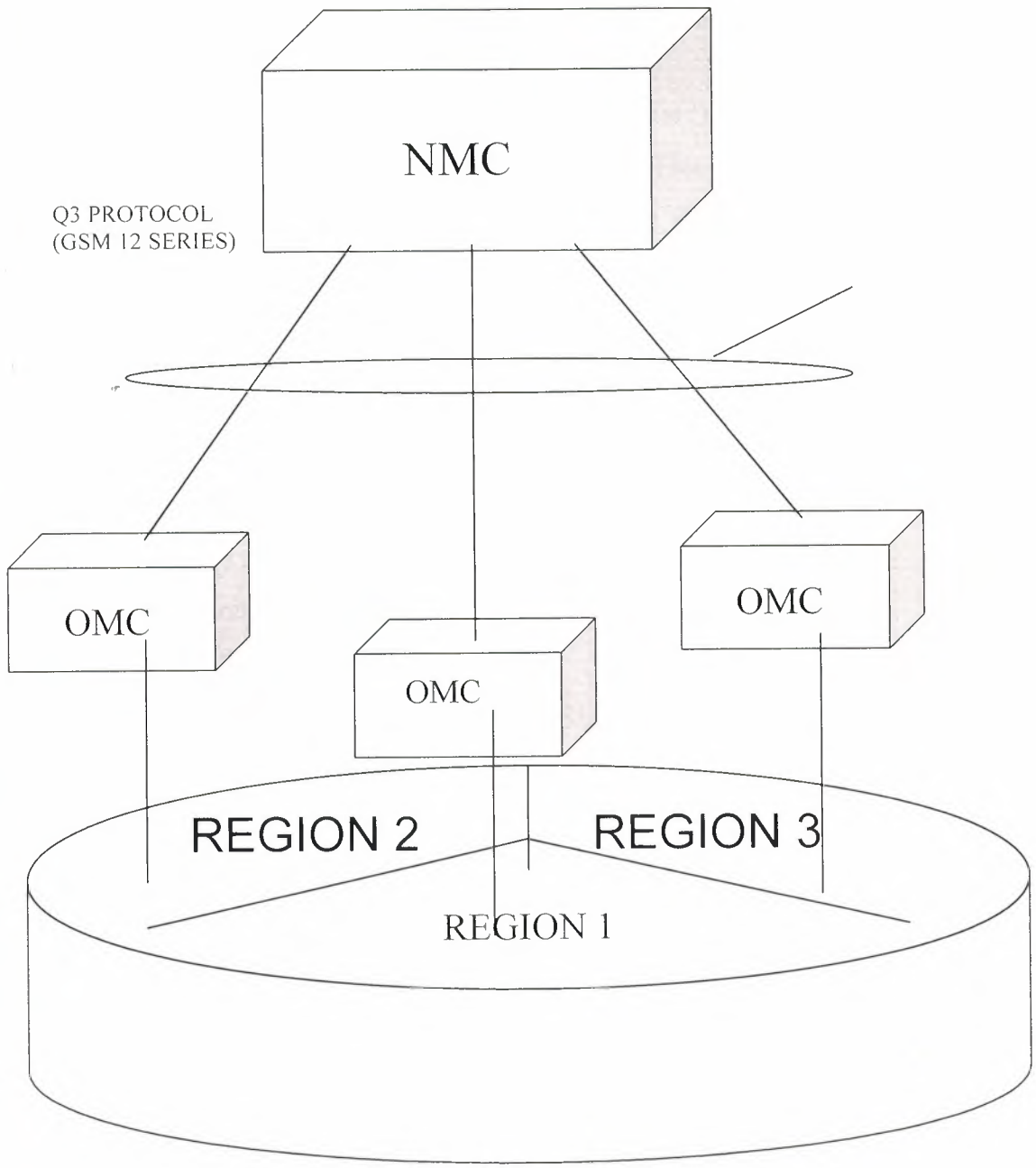


Figure 3.10: Network Management Centre

3.9 Operations and Maintenance Centre - OMC

The OMC provides a central point from which to control and monitor the other network entities (i.e. Base Stations, switches, database, etc) as well as monitor the quality of service provider by the network.

At present, equipment manufactures have their own OMCs, which are not compatible in every aspect with those of other manufactures. This is particularly the case between Radio Base Station equipment suppliers, where in some cases the OMC is a separate item and Digital Switching equipment suppliers, where the OMC is an integral, but functionally separate, part of the hardware.

There are two types of OMC these are:

- **OMC (R)**

  OMC controls specifically the Base Station System.

- **OMC (S)**

  OMC controls specifically the Network Switching System.

The OMC should support the following functions as per ITS-TS recommendations:

- Event/Alarm Management.
- Fault Management.
- Performance Management.
- Configuration Management.
- Security Management [3].

3.10 The Network in Reality

In reality a GSM network is much more complicated than we have seen. The diagram opposite illustrates how multiple BSS and Network Switching System components will be connected within a network. A typical for example, London will have approximately the following number of network components:

Network Component	Quantity
Opersations and maintenance Centre (Base Station Equipment) – OMC (R)	1
Opersations and maintenance Centre (Switiching) _ OMC(S)	1
Mobile Services Switching Centre -MSC/VLR	1-2
Base Station Controller – BSC	5-15
Base Tansceiver Station –BTS	200 - 400

A typical network (for example, UK) will have following number of network components [1].

Network Component	Quantity
Opersations and maintenance Centre (Base Station Equipment) – OMC (R)	6
Opersations and maintenance Centre (Switiching) _ OMC(S)	6
Mobile Services Switching Centre -MSC/VLR	6
Base Station Controller – BSC	40+
Base Tansceiver Station –BTS	1200+

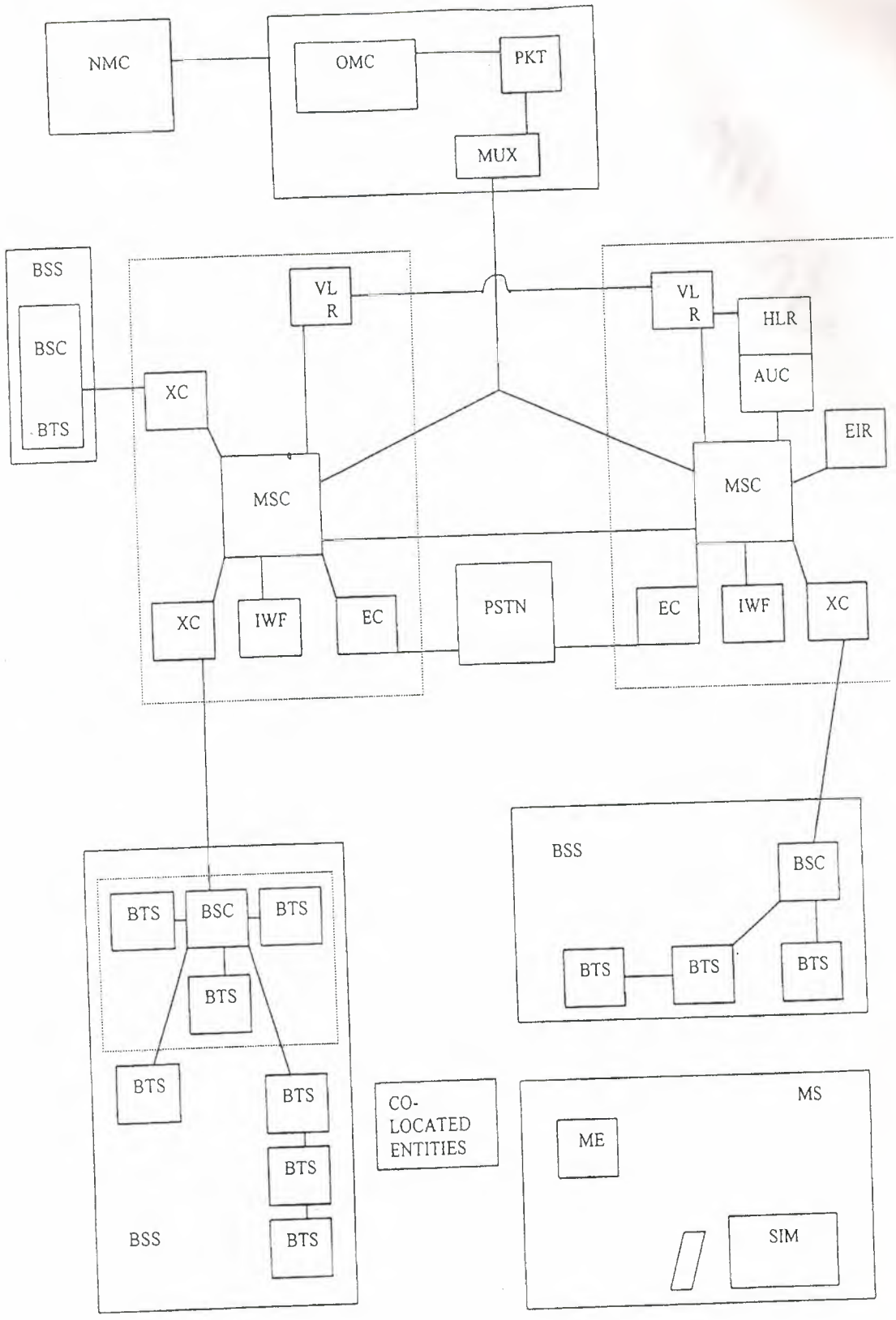


Figure 3.11: GSM Network Components

GSM SYSTEM ARCHITECTURE

Chapter 4

GSM Basic Call Sequence and Radio Interface Optimization

4.1 GSM Basic Call Sequence

The diagram opposite reminds us of the basic components and processes involved in setting up a call between a GSM MS and an ordinary "land" telephone.

- **In the MS to Land Direction**

  The BTS receives a data message from the MS, which it passes it to the BSC. The BSC relays the message to the MSC via C7 signalling links, and the MSC then sets up the call to the land subscriber via the PSTN. The MSC connects the PSTN to the GSM network, and allocates a terrestrial circuit to the BSS serving the MS's location. The BSC of that BSS sets up the air interface channel to the MS and then connects that channel to the allocated terrestrial circuit, completing the connection between the two subscribers.

- **In the Land to MS direction**

  The MSC receives its initial data message from the PSTN (via C7) and then establishes the location of the MS by referencing the HLR. It then knows which other MSC to contact to establish the call and that MSC then sets up the call via the BSS serving the MS's location.

The actual processes are, of course, considerably more complex than described above. Also, there are many different GSM call sequence and handover scenarios enough to form the subject of their own training program! In this course we consider in detail just the MS to Land and Land to MS call sequences and the intra-MSC (inter-BSS) handover sequence. This will give you a good appreciation of the messaging that occurs in the GSM system, and how the PLMN interacts with the PSTN [1].

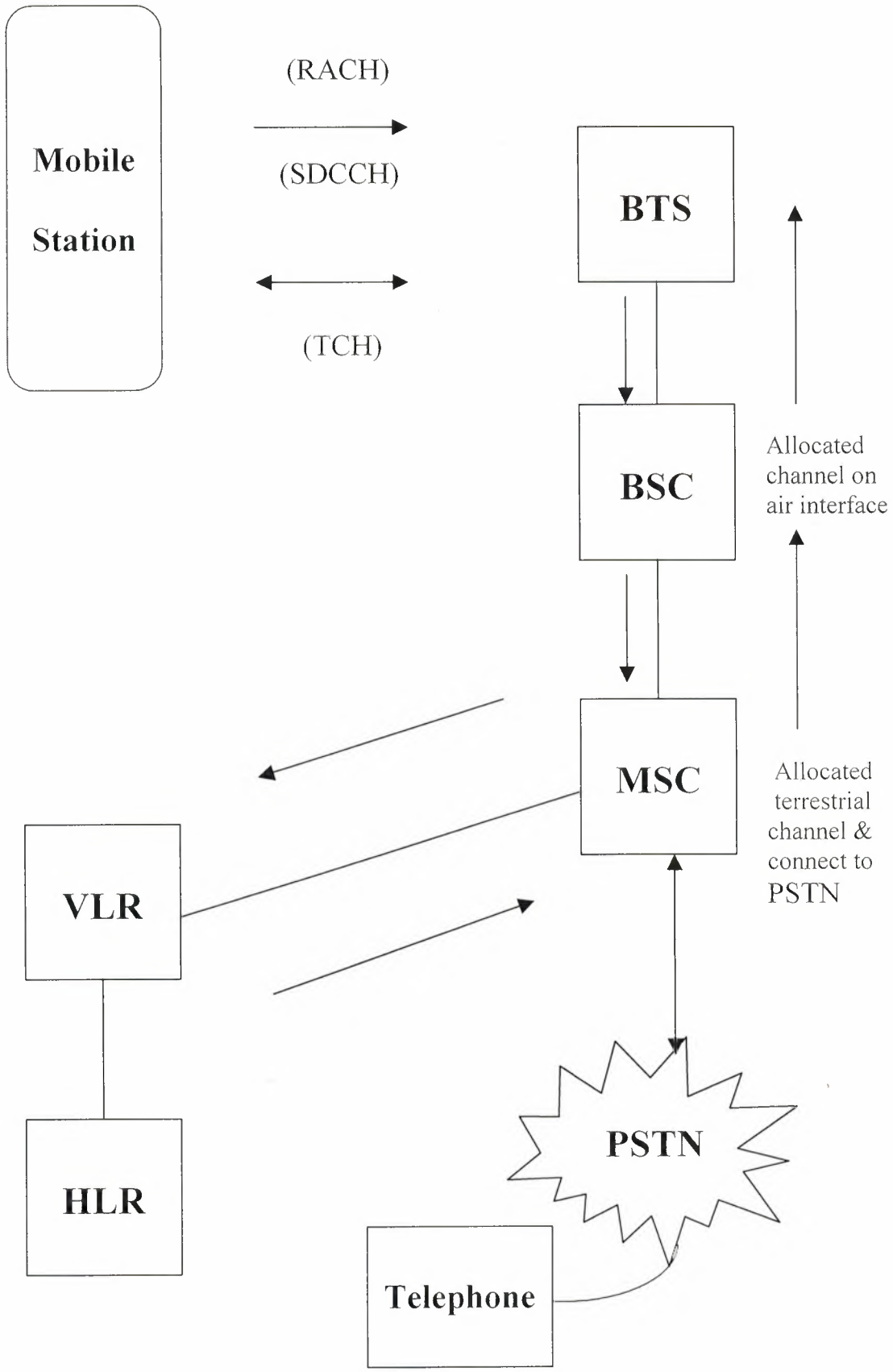


Figure 4.1: GSM Basic Call Sequence

4.2 Radio Interface Optimization

4.2.1 Transmission Timing

To simplify the design of the MS, the GSM specifications specify an offset of three timeslots between the BSS and MS timing, thus avoiding the necessity for the MS to transmit and receive simultaneously. The diagram opposite illustrates this.

The synchronization of TDMA system is critical because bursts have to be transmitted and received within the "real time "timeslots allotted to them. The further the MS is from the base station then, obviously, the longer it will take for the burst to travels the distance between them. The GSM BTS caters for this problem by instructing the MS to advance its timing (that is, transmit earlier) to compensate for the increased propagation delay.

This advance is then superimposed upon the three timeslots nominal offset.

The timing advanced information is sent to the MS twice every second using the SACCH.

The maximum timing advanced is approximately 233Ms. This caters for a maximum cell radius of approximately *35* Km [2].

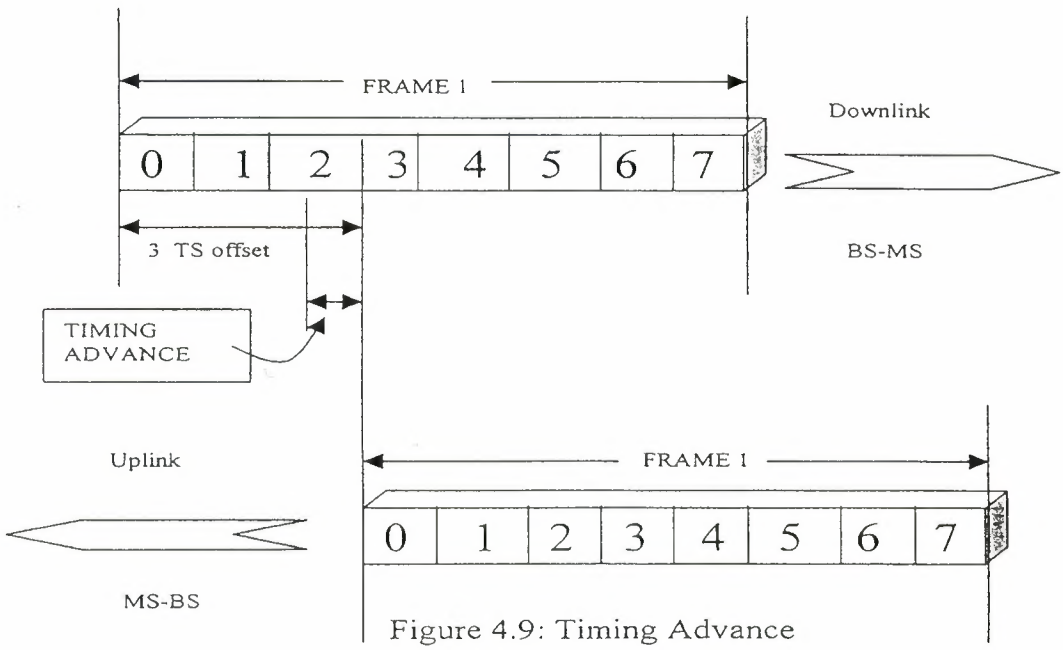


Figure 4.9: Timing Advance

4.2.2 Battery Life

One of the main factors, which restrict reducing the size of a MS, is the battety.

A battery life must be large enough to maintain a telephone call for an acceptable amount of time without needing to be recharged. Since there is demand for MSs to become smaller and lighter the battery must be smaller and lighter

Four features which enable the life of a GSM MS battery to be extended.

- Power Control
- Voice Activity Detection — VAD
- Discontinuous Transmission — DTX
- Discontinuous Reception - DRX

4.2.2.1 Power control

This is a features of the GSM air interface which allows the network provider to not only compensate for the distance from MS to BTS as regards timing, but can also cause the BTS and MS to adjust their power output to take account of that distance also. The closer the MS is to the BTS, the less power it and the BTS will be required to transmit. This feature saves radio battery power at the MS, and helps to reduce co-channel and adjacent channel interference.

Both up link and downlink power setting can be controlled independently and individually at the discretion of the network provider. Initial power setting for the MS is set by the information provided on the broadcast Control Channel (BCCH) for a particular Cell.

The B 85 controls the transmit power of both the MS and the receive BTS power is monitored by the MS and then reported to the BSS. Using these measurements the power of both MS and BTS can be adjusted accordingly [2].

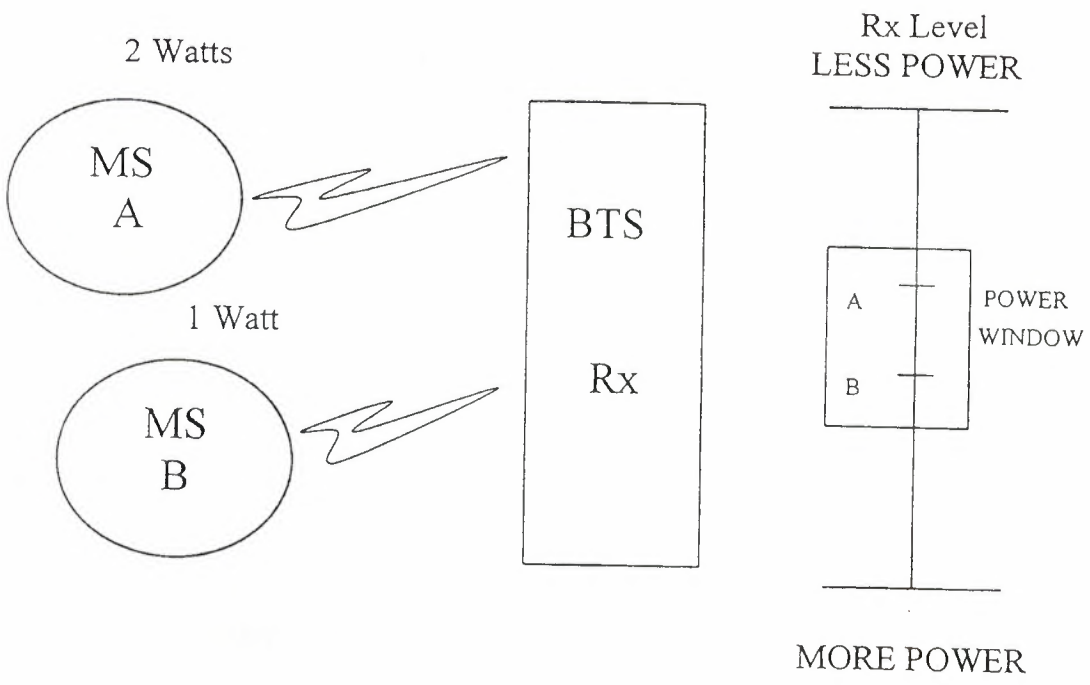


Figure 4.10: Power Control

Note:

The BTS will adjust the Tx power of each MS to ensure that the Rx signal at the BTS is maintained within the defined power window.

4.2.2.2 **Voice Activity Detection** - VAD

VAD is a mechanism whereby the source transmitter equipment identifies the presence or absence of speech.

VAD implementation is effected in speech pattern silences at a rate of 500 bit/s rather than the full 13 kbit/s. this results in a data transmission rate for background noise, known as "comfort" noise, which is regenerated in the receiver.

Without "comfort" noise the total silence between the speech would be considered to be distributing by the listener.

4.2.2.3 Discontinuous Transmission - DTX

DTX increases the efficiency of the system through a decrease in the possible radio transmission interference level. It does this by ensuring that the MS does not transmit unnecessary message data.

DTX can be implemented, as necessary, on a call by a call basis. The effect will be most noticeable in communications between two MS. DTX in its most extreme form, when implemented at the MS can also result in considerable power saving. If the MS does not transmit during "silence" there is a reduction in the overall power output requirement. The implementation of DTX is very much at the distraction of the network provider and there are different specifications applied for different types of channel usage.

DTX is implemented over a SACCH multi-frame (480ms). During this time, of the possible 104 frames, only the 4 SACCH frames and 8 Silence Descriptor (SJD) frames are transmitted [1].

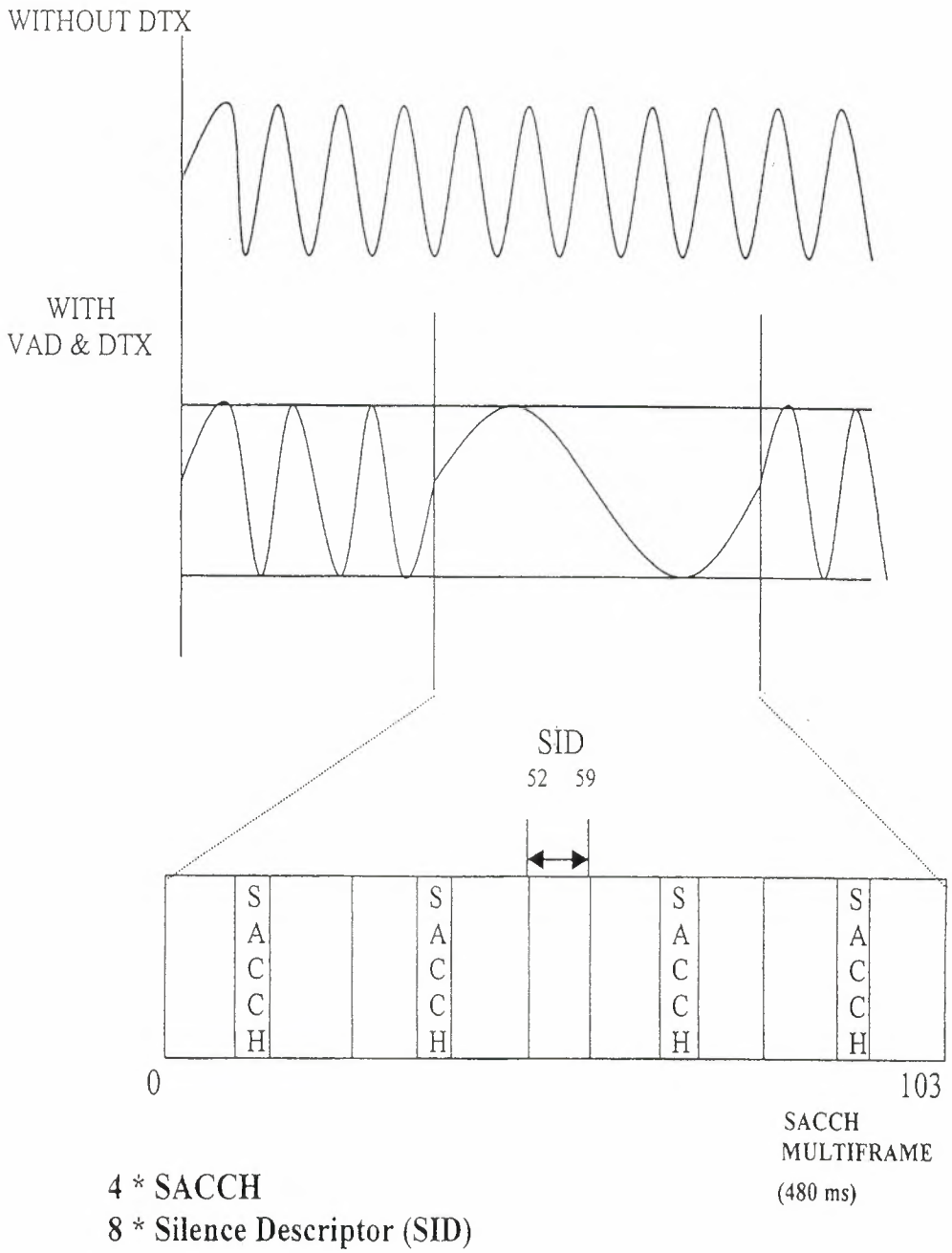


Figure 4.11: VAD & DTX

4.2.2.4 Discontinuous Reception - DRX

DRX allows the MS to effectively "switch off" during times when reception is deemed unnecessary.

By monitoring the Broadcast Control Channel (BCCH), the Frequency Correction Control Channel (FCCH) the MS is aware of the frame Number and repetition format for Frame Synchronization it can therefore, after initially locking on to a BCCH, determine when the next relevant information is to be transmitted. This allows the MS 'go to sleep' and listen-in only when necessary, with the effective saving in power usage. DRX may only be used when a MS is not in a call.

When DRX is employed, the MS using information broadcast on the BCCH determines its paging group . The paging group may appear once during a control channel multi-frame, or may only be scheduled to appear once over several multi-frames —the rate of repetition is determined by the network provider and it is this information which is broadcast over the BCCH, which allows the MS to determine its paging group [1].

4.2.3 Multipath Fading

Multipath Fading results from a signal traveling from a transmitter to a receiver by a number of routes this is caused by the signal being reflected from objects, or being influenced by atmospheric effects as it passes, for example, through layers of air of varying temperatures and humidity.

Received signals will therefore arrive at different times and not be in phase with each other, they will have experienced time description. On arrival at the receiver, the signals combine either constructively destructively, the over all effect being to add together or to cancel each other out, if the latter applies, there may be hardly any usable signal at all. The frequency band used GSM transmission means that a 'good' location may be only 15 cm from a "bad" location.

When the receive antenna is moving, the exact phase of each path changes and consequently the combined signal-strength is also continually changing. When the antenna is moving rapidly, this loss is recovered by inter leaving and channel coding. When it is slow moving or stationary however, the receiver may be in a "null" (point of minimum signal) for several consecutive frames.

The diagram opposite shows a few routes by which a pulse of a radio energy might be propagated from a base station to a mobile.

Each has suffered varying losses in transmission (path attenuation), hence the variety of amplitudes. A typical urban profile would cause dispersion of up to 5 microseconds, whereas, a hilly terrain would cause dispersion up to 20 microseconds.

GSM offers five techniques which combat multipath fading effects:

- Equalization.
- Diversity.
- Frequency Hopping.
- Interleaving.
- Channel coding.

The equalizer must be able to cope with a dispersion of up to 17 microseconds [1].

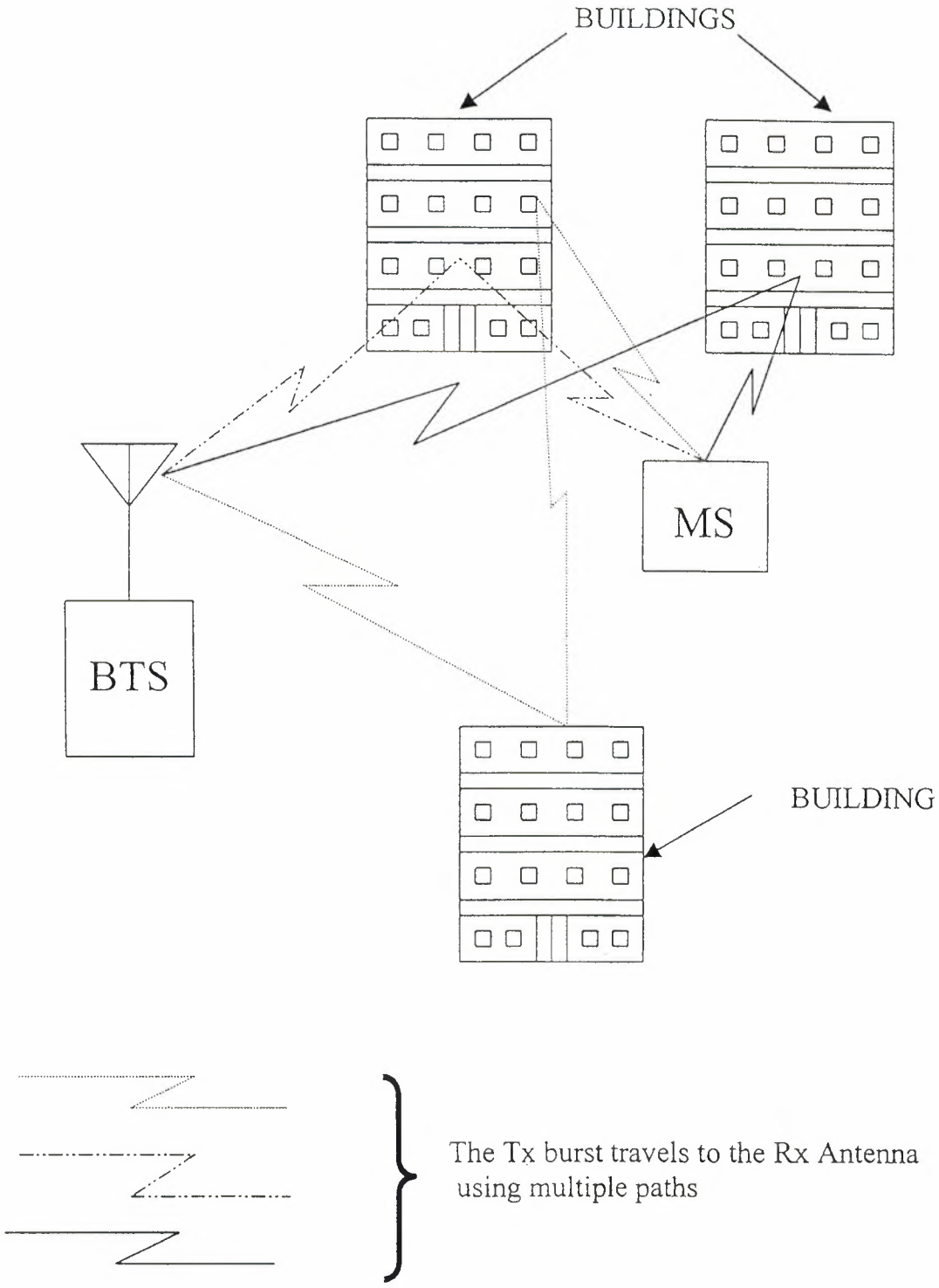


Figure 4.13: Multipath Fading

4.2.3.1 Equalization

Due to the signal dispersion caused by multipath signals the receiver cannot be sure exactly when a burst will arrive and how distorted it will be. To help the receiver identify and synchronize to the burst, a training sequence is sent at the center of the burst. This is a set sequence of bits, which is known by both the transmitter and receiver.

When a burst of information is received, the equalizer searches for the training sequence code. When it has been found, the equalizer measures and then mimics the distortion, which the signal has been subjected to. The equalizer then compares the received data with the distorted possible transmitted sequence and chose the most likely one.

There are eight different training sequence codes numbered (0-7). Nearby cells operating with the same RF carrier frequency will use different Training Sequence Codes to enable the receiver the discern the correct signal [1].

4.2.3.2 Diversity

Signal arrive at the receive antenna from multiple paths. The signals are therefore received by the antenna at different phases, some at a peak and some at a trough. This means that some signals will add together to form a strong signal, while others will subtract causing a weak signal. When diversity is implemented, two antennas are situated at the receiver. These antennas are placed several wavelength apart to ensure minimum correlation between the two receive paths. The two signals are then combined and the signal strength improved [2].

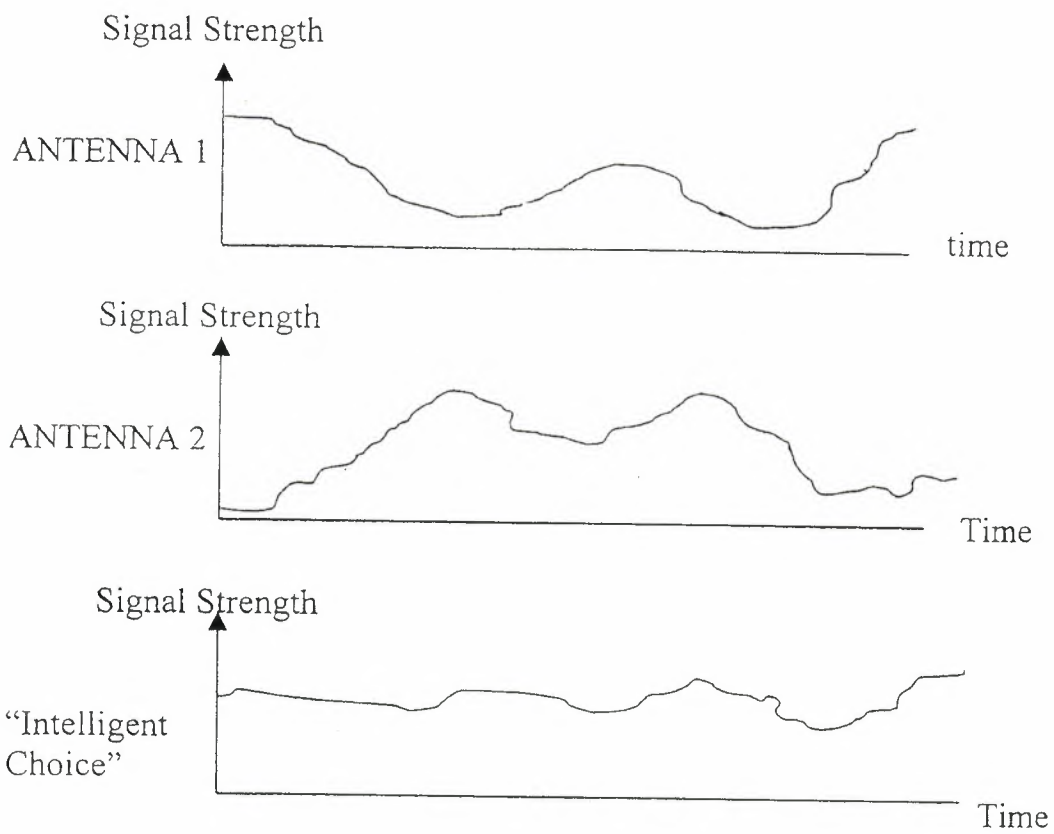


Figure 4.15: Signal Strength vs. Time when Diversity is implemented

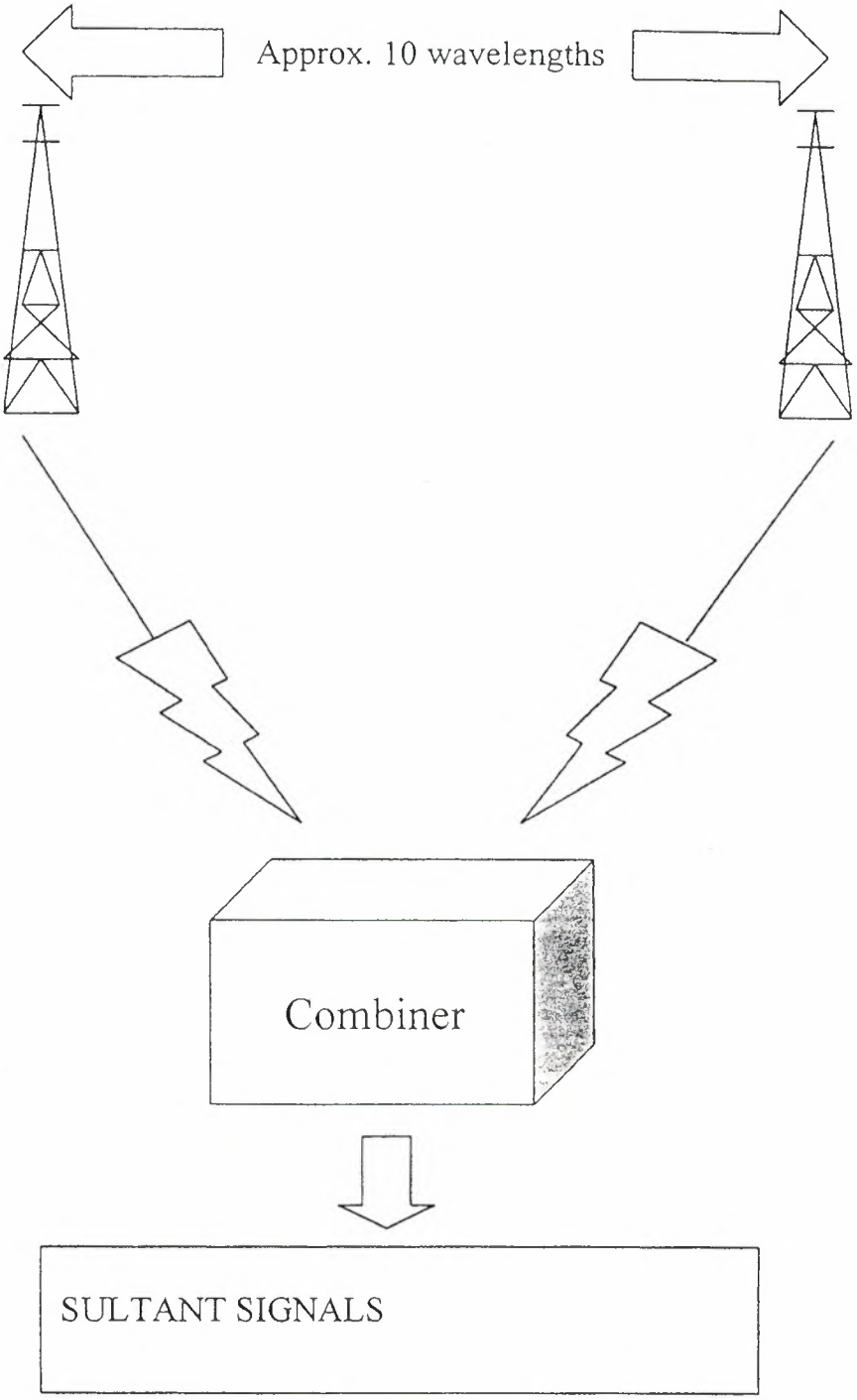


Figure 4.16: Diversity

4.2.3.3 Radio Frequency Channels and Bands For D900

According to the GSM standards the Urn interface is used between the BTS antenna and the MS. The D900 provides the GSM primary band (890-915 MHz for uplink, 935-960 MHz for downlink) as well as the GSM extended band (880-915 MHz for uplink, 925-960 MHz for downlink). With FDMA 124 (174 for extended band) discrete duplex radio frequency channels are available: 124 (174) downlink channels for transmission from the MS to the BSS and 124 (174) downlink channels for transmission from the BSS to the MS. With TDMA the number of channels is increased by a factor of 8 to 992 (1392 for GSM extended band) physical duplex traffic channels in the case of full rate channels [9]. With pure half rate operation, twice the number of physical duplex traffic channels available for a TDMA system. With dual rate operation (full rate and half rate), a value which is practically between a pure full rate and a pure half rate operation is produced for a TDMA system. The specifications of the radio frequency bands are as follows:

GSM primary band (P-GSM 900)

- Carrier frequencies of the BSS receivers (uplink): fup(n) = (890+ 0,2xn) MHz
  (with Absolute Radio Frequency Channel, ARFCN l<=n<=124)

- Carrier frequencies of the BSS transmitters (downlink): Fdown (n)=fup(n)+45MHz
  Radio frequency channel spacing: 200 kHz
  Duplex spacing: 45 MHz

- GSM extended band (E-GSM 900)
  Carrier frequencies of the BSS receivers (uplink):
  Fup(n)(890+0.2 x n) MHz+
  (with ARFCN 0<=n< 124)
  [890+0.2 x (n-1024)] MHz

(with ARFCN 975<=n<=1023)

- Carrier frequencies of the BSS transmitters (downlink):

fdown (n) = fup (n)+45 MHz

Radio frequency channel spacing: 200 kHz

Duplex spacing: 45 MHz

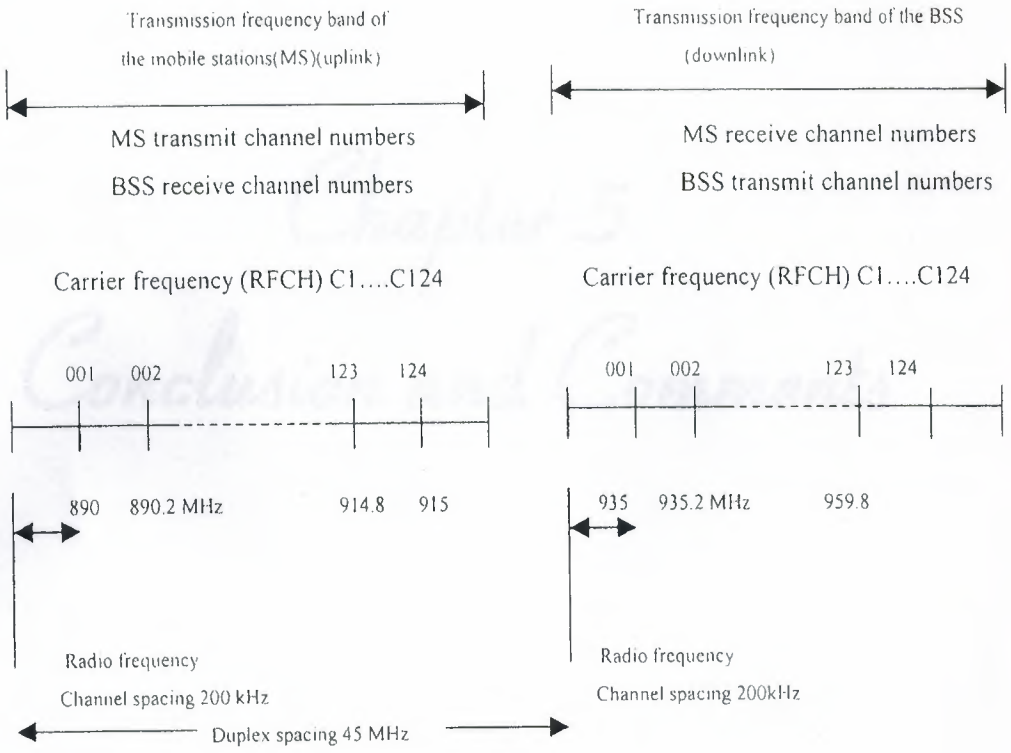
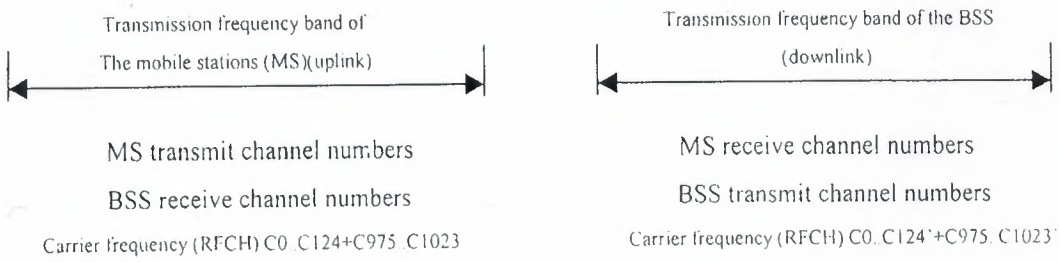


Figure 3.4 Radio Frequency Channel Distribution For D900 BSS (GSM Primary Band)



GSM SYSTEM ARCHITECTURE

Chapter 5

Conclusion and Comments

5.1 Conclusion and Comments

In this paper we have tried to give an overview of the GSM system. As with any overview there are many details missing. We believe, however, that we gave the general flavor of GSM and the philosophy behind its design. It was a monumental task that the original GSM committee undertook, and one that has proven a success, showing that international cooperation on such projects between academia, industry, and government can succeed. It is a standard that ensures interoperability without stifling competition and innovation among suppliers, to the benefit of the public both in terms of cost and service quality. For example, by using Very Large Scale Integration (VLSI) microprocessor technology, many functions of the mobile station can be built on one chipset, resulting in lighter, more compact, and more energy-efficient terminals.

Telecommunications are evolving towards personal communication networks, whose objective can be stated as the availability of all communication services anytime, anywhere, to anyone, by a single identity number and a pocketable communication terminal. Having a multitude of incompatible systems throughout the world moves us farther away from this ideal. The economies of scale created by a unified system are enough to justify its implementation, not to mention the convenience to people of carrying just one communication terminal anywhere they go, regardless of national boundaries.

The GSM system, and its sibling systems operating at 1.8 GHz (called DCS1800) and 1.9 GHz (called GSM1900 or PCS1900, and operating in North America), are a first approach at a true personal communication system. The SIM card is a novel approach that implements personal mobility in addition to terminal mobility. Together with international roaming, and support for a variety of services such as telephony, data transfer, fax, Short Message Service, and supplementary services, GSM comes close to fulfilling the requirements for a personal communication system: close enough that it is being used as a basis for the next generation of mobile communication technology in Europe, the Universal Mobile Telecommunication System (UMTS).

Another point where GSM has shown its commitment to openness, standards and interoperability is the compatibility with the Integrated Services Digital Network (ISDN) that is evolving in most industrialized countries, and Europe in particular (the so-called Euro-ISDN). GSM is also the first system to make extensive use of the

Intelligent Networking concept, in which services like 800 numbers are concentrated and handled from a few centralized service centers, instead of being distributed over every switch in the country. This is the concept behind the use of the various registers such as the HLR. In addition, the signalling between these functional entities uses Signalling System Number 7, an international standard already deployed in many countries and specified as the backbone signalling network for ISDN.

GSM is a very complex standard, but that is probably the price that must be paid to achieve the level of integrated service and quality offered while subject to the rather severe restrictions imposed by the radio environment.

Glossary of Terms:

A interface	Interface between MSC and BSS
A3	Authentication Algorithm
A5	Stream cipher algorithm
A8	Ciphering key generating algorithm
ACK	Acknowledgement
ACM	Address Complete Message
AGCH	Access Grant Channel
AM	Amplitude Modulation
ARFCN	Absolute Radio Frequency Channel Number
AUC	Authentication Centre
AUT(H)	Authentication
BCCH	Broadcast Control Channel
BSC	Base Station Controller
BSS	Base Station System
BTS	Base Transceiver Station
C7	CCITT Signalling System #7 (SS7)
CC	Country Code
CC	Call Control
CCCH	Common Control Channels
CKSN	Ciphering Key Sequence Number
CR	Carriage Return (RETURN)
DCCH	Dedicated Control Channels
DCS	Digital Communication/Cellular System
DISC	Disconnect

DRX, DRx	Discontinuous Reception
DTX, DTx	Discontinuous Transmission
EC	Echo Canceller
EGSM	Extended Global System for Mobile Communications
EIR	Equipment Identity Register
ETSI	European Telecommunications Standards Institute
FACCH	Fast Associated Control Channel
FDMA	Frequency Division Multiple Access
FM	Fault Management (at OMC)
FM	Frequency Modulation
GMSC	Gateway Mobile services Switching Centre
GMSK	Gaussian Minimum Shift Keying
GSM	Groupe Special Mobile (the committee)
GSM	Global System for Mobile communications
HLR	Home Location Register
HO	Handover
IC	Integrated Circuit
IC	Interlock Code (closed user group supplementary service)
ID, id	Identification/Identity
IEEE	Institute of Electrical and Electronic Engineers
IFAM	Initial and Final Address Message
IMEI	International Mobile station Equipment Identity
IMSI	International Mobile Subscriber Identity
I/O	Input/Output
ISDN	Integrated Services Digital Network
ITU	International Telecommunication Union
IWF	InterWorking Function

Kc	Ciphering key
Ki	Individual subscriber authentication key
LAI	Location Area Identification (identity)
ME	Mobile Equipment
MF	MultiFrame
MF	Multi-Frequency (tone signalling type)
MF	MultiFunction block
MRN	Mobile Roaming Number
MS	Mobile Station
MSC	Mobile services Switching Centre
MSISDN	Mobile Station International ISDN Number
MSRN	Mobile Station Roaming Number
NMC	Network Management Centre
OMC	Operations and Maintenance Centre
PCH	Paging Channel
PCM	Pulse Code Modulation
PCS	Personal Communications System
PLMN	Public Land Mobile Network
PM	Performance Management. An OMC application
PSK	Phase Shift Keying
PSTN	Public Switched Telephone Network
RACH	Random Access Channel
RAND	Random Number
RF	Radio Frequency
RSSI	Received Signal Strength Indication

Rx	Receive(r)
SABM	Set Asynchronous Balanced Mode
SACCH	Slow Associated Control Channel
SDCCH	Stand-alone Dedicated Control Channel
SID	Silence Descriptor
SIM	Subscriber Identity Module
SRES	Signed Response (authentication)
TCH	Traffic Channel
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TMSI	Temporary Mobile Subscriber Identity
TRAU	Transcoder Rate Adaption Unit
TRX	Transceiver(s)
TS	Timeslot
Tx	Transmit(ter)
UA	Unnumbered Acknowledgement
VAD	Voice Activity Detection
VLR	Visitor Location Register
X.25	CCITT specification and protocols for public packet-switched networks
XCDR	full-rate Transcoder

References:

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

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

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

Internet Sites:

1. http://www.telecom.no/mobil/?id=1284397
2. http://www.alanta.demon.co.uk/GSMPaper
3. http://www.gsmsystem.cjb.net
4. http://kbs.cs.tu-berlin.de/~jutta/gsm/js-intro.html
5. http://www.gsmag.com/useful.html
6. http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html