NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Electrical and Electronic Engineering

CELL PLANNING AND RADIO INTERFACE IN GSM

Graduation Project
EE- 400

Student: Malik M. Kashif (971277)

Supervisor: Prof. Dr. Fakhreddin Mamedov

Nicosia - 2001

ACKNOWLEDGMENTS

First and Foremost I would like to Thank almighty ALLAH for giving me the strength and sincereness during this Project.

My special Thanks to my Supervisor Prof. Dr. FAKHREDDIN MAMEDOV, for his valuable advice and utmost support in completing this Project.

Second, I would like to thank my family for their continues support and for always encouraging me especially in this Project

Finally, I would like to thank my friends Imran, Bhai, Shabi, Shehzada, Aneel, Umair & KK and all the others, for their utmost support, advice and for guiding me in the making of this Project.

ABSTRACT

Different requirements and the dedication to meet them led to, the development of the GSM standard. An unprecedented effort has been taken by telecommunication authorities, network operators, and industry sectors to establish and maintain a state-of-the-art cellular standard for the benefit of the entire industry and all its customers.

The GSM standard can be regarded as an evolving standard. The whole standardization process could not be completed before the actual launch of the services; a phased approach to rolling out the specifications and the networks was adopted. The reduced features were initially designed to be upwardly compatible *odd-ons* of services and functions, the subset was called GSM *Phase* 1. The additional supplements to full implementation of all the planned services and network features were called GSM *Phase* 2. By this, the GSM platform was created, a platform which is full of hooks, mechanisms and not at least potential to continue to build on and to provide mobile communication in all its possible forms and variations.

Even before the *Phase* 2 standard has been completed, GSM has grown far beyond its original geographical "limitations" and the Global System Of Mobile Communication really starts to deserve its name. With Phase 2, and in particular with Phase 2+, GSM will also expand far beyond its originally intended functional boundaries and open up for new applications, new access methods, new technologies and thus altogether for new categories of markets, needs and users.

It looks Promising.

TABLE OF CONTENTS

INTRODUCTION

GSM stands for "Global System For Mobile Communication". Words cannot easily express the tireless efforts expanded to propel the development of the GSM standard, design a network architecture, test and verify technical parameters, prove functionalities, promote the system itself, and design and manufacture the necessary equipment. What we see today is the result of this work.

The new standard has given new momentum to the economy and has created new markets. A common standard for a market whose customer's number in the tens of millions lead s to minimize costs for the manufacturers of appropriate equipment. They can produce large number of terminals for a large market, which drives down the cost to end-user.

New services and features, especially the roaming and security features, as well as the digital advantages, such as reduced power consumption (state-of-the-art semiconductor devices, TDMA technology) and improved speech quality are the keys that convince network operators and potential subscribers to choose GSM.

This project "Cell Planning and Radio Interface in GSM" consist of an Introduction, Three Chapters and a Conclusion.

Chapter One: Introduction To GSM, contains a brief introduction about GSM, its history, services offered by GSM, the System Architecture of GSM, it's Radio Link Aspects and it's Network Aspects.

Chapter Two: Cell Planning, this chapter confines the focus on different aspects of Cell Planning. Starting from History, it explains the Cellular Structure, Network Planning, Mobile Radio Network Planning Tasks, Radio Wave Propagation, Cellular Network and Frequency allocation and finally Call Handover/Handoff.

Chapter Three: Radio Interface, this chapter gives an introduction about Radio Interface, it also explain the Access to the Trunking System, the Channel Structure, the Burst Structure, Frequency Hopping and Radio Frequency Power Level.

Finally, the Conclusion explains the knowledge gained during the making of this project and the future of GSM.

CHAPTER 1
INTRODUCTION TO GSM

1.1 History of GSM

The development of GSM started in 1982, when the Conference of European Posts and Telegraphs (CEPT) formed a study group called **Groupe Spécial 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.

1.2 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, teleservices 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 is 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 specifications.

1.3 System Architecture

It is difficult for typical wire-line phone users to understand and appreciate the overhead necessary to process a call to another city or country. It is even more difficult for cellular subscribers to understand that there is a little bit more in a cellular network outside their phones. To supply cellular service to subscribers, a network operator has to install a complete and separate network, which, at a certain point, has to interface to the *public switched telephone network* (PSTN). In addition to the standard national roaming feature, which applies to the current analog systems, the new GSM system was also designed to allow international roaming. This means that users can enjoy the option of taking their phone abroad and using it in foreign GSM systems. Furthermore, users can still be reached under their own subscriber number in their home country, independent of their location, as if they had never left town.

A description of the different entities in the GSM system follows. Most of these entities are also used in analog networks. The recommendations and the specifications for GSM networks do not merely specify the air interface and the message flow between mobile stations and the cellular network on that air interface. They also describe the whole infrastructure and all the other parts of the system that are mentioned and described here (Figure 1.1).

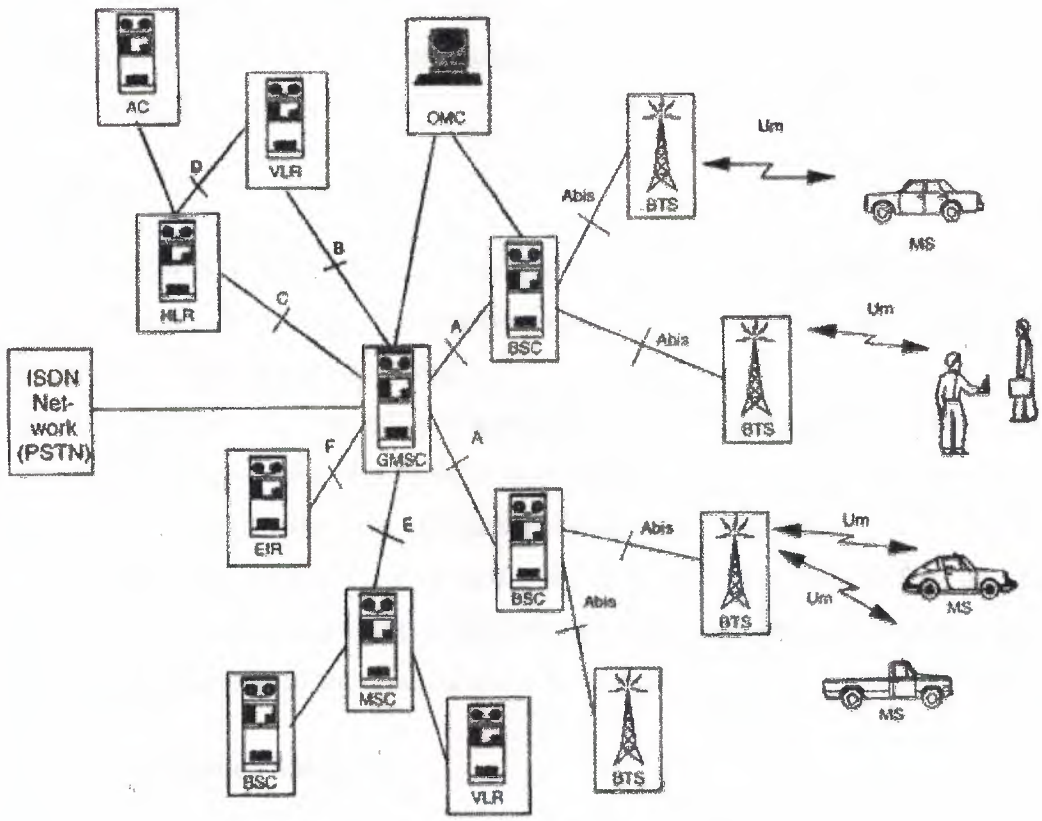


Figure 1.1, GSM System Architecture

1.3.1 Mobile Station

A Mobile Station consists of two main elements:

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

(a) The Terminal

There are different types of terminals distinguished principally by their power and application:

The `fixed' terminals are the ones installed in cars. Their maximum allowed output power is 20 W.

The GSM portable terminals can also be installed in vehicles. Their maximum allowed output power is 8W. The handholds terminals have experienced the biggest success thanks to thei weight and volume, which are continuously decreasing. These terminals can emit up to 2 W. The evolution of technologies allows decreasing the maximum allowed power to 0.8 W.

(b) The SIM

The SIM is a smart card that identifies the terminal. By inserting the SIM card into the terminal, the user can have access to all the subscribed services. Without the SIM card, the terminal is not operational.

The SIM card is protected by a four-digit Personal Identification Number (PIN). In order to identify the subscriber to the system, the SIM card contains some parameters of the user such as its International Mobile Subscriber Identity (IMSI).

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

1.3.2 The Base Station Subsystem

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

- The Base Transceiver Station (BTS) or Base Station.
- The Base Station Controller (BSC).

(a) The Base Transceiver Station

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

(b) The Base Station Controller

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

1.3.3 The Network and Switching Subsystem

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

(a) The Mobile services Switching Center (MSC)

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

(b) The Gateway Mobile services Switching Center (GMSC)

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

(c) Home Location Register (HLR)

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

(d) Visitor Location Register (VLR)

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

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

(e) The Authentication Center (AuC)

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

(f) The Equipment Identity Register (EIR)

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

(g) The GSM Interworking Unit (GIWU)

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

1.3.4 The Operation and Support Subsystem (OSS)

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

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

1.4 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.

1.4.1 Multiple Access And Channel Structure

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

Channels are defined by the number and position of their corresponding burst periods. All these definitions are cyclic, and the entire pattern repeats approximately every 3 hours. Channels can be divided into *dedicated channels*, which are allocated to a mobile station, and *common channels*, which are used by mobile stations in idle mode.

(a) Traffic channels

A traffic channel (TCH) is used to carry speech and data traffic. Traffic channels are defined using a 26-frame multiframe, or group of 26 TDMA frames. The length of a 26-frame multiframe is 120 ms, which is how the length of a burst period is defined (120 ms divided by 26 frames divided by 8 burst periods per frame). Out of the 26 frames, 24 are used for traffic, 1 is used for the Slow Associated Control Channel (SACCH) and 1 is currently unused (Figure 1.2). 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.

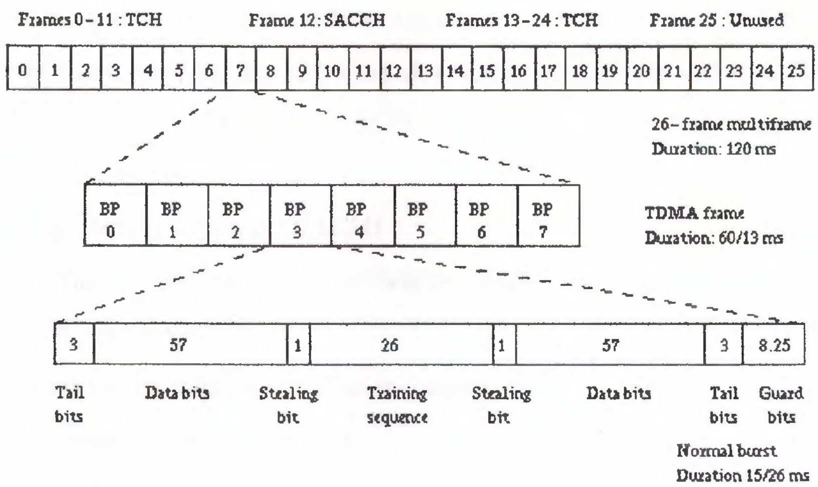


Figure 1.2, Organization of bursts, TDMA frames, and multiframes for speech and data

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 signaling. In the recommendations, they are called Stand-alone Dedicated Control Channels (SDCCH).

(b) Control channels

Common channels can be accessed both by idle mode and dedicated mode mobiles. Idle mode mobiles to exchange the signaling information required changing to dedicated mode use the common channels. 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 synchronies 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.

(c) Burst structure

There are four different types of bursts used for transmission in GSM. The normal burst is used to carry data and most signaling. 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 1.2. 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.

1.4.2 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.

1.4.3 Channel Coding And Modulation

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

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

Class I a 50 bits - most sensitive to bit errors

Class I b 132 bits - moderately sensitive to bit errors

Class II 78 bits - least sensitive to bit errors

Class I a bit 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 I b 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).

1.4.4 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.

1.4.5 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.

1.4.6 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.

1.4.7 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.

1.4.8 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 mill watts).

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 alternating 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.

1.5 Network Aspects

Radio transmission forms the lowest functional layer in GSM. In any telecommunication system, signalling is required to coordinate the necessarily distributed functional entities of the network. The transfer of signaling information in GSM follows the layered OSI model. On top of the physical layer described above is the data link layer providing error-free transmission between adjacent entities based on the ISDN's LAPD protocol for the Um and Abis interfaces, and on SS7's Message Transfer Protocol (MTP) for the other interfaces. The functional layers above the data link layer are responsible for Radio Resource management (RR), Mobility Management (MM) and Call Management (CM).

1.5.1 Radio Resources Management

The RR functional layer is responsible for providing a reliable radio link between the mobile station and the network infrastructure. This includes the establishment and allocation of radio channels on the Um interface, as well as the establishment of A interface links to the MSC. The handover procedures, an essential element of cellular systems, are managed at this layer, which involves the mobile station, the base station subsystem, and, to a lesser degree, the MSC. Several protocols are used between the different network elements to provide RR functionality.

The MM functional layer assumes a reliable RR-connection, and is responsible for location management and security. Location management involves the procedures and signalling for location updating, so that the mobile's current location is stored at the HLR, allowing incoming calls to be properly routed. Security involves the authentication of the mobile, to prevent unauthorized access to the network, as well as the encryption of all radio link traffic. The protocols in the MM layer involve the SIM, MSC, VLR, and the HLR, as well as the AuC (which is closely tied with the HLR). The machines in the network subsystem exchange signalling information through the Mobile Application Part (MAP), which is built on top of SS7.

The CM functional layer is divided into three sublayers. The Call Control (CC) sublayer manages call routing, establishment, maintenance, and release, and is closely related to ISDN call control. The idea is for CC to be as independent as possible from the underlying specifics of the mobile network. Another sublayer is Supplementary Services, which manages the implementation of the various supplementary services, and also allows users to access and modify their service subscription. The final sublayer is the Short Message Service layer, which handles the routing and delivery of short messages, both from and to the mobile subscriber.

1.5.2 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.

(a) Location Updating

A powered-on mobile is informed of an incoming call by a paging message sent over the PAGCH channel of a cell. One extreme would be to page every cell in the network for each call, which is obviously a waste of radio bandwidth. The other extreme would be for the mobile to notify the system, via location updating messages, of its current location at the individual cell level. This would require paging messages to be sent to exactly one cell, but would be very wasteful due to the large number of location updating messages. A compromise solution used in GSM is to group cells into *location areas*. Updating messages are required when moving between location areas, and mobile stations are paged in the cells of their current location area.

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

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

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

(b) Authentication And Security

Since the radio medium can be accessed by anyone, authentication of users to prove that they are who they claim to be, is a very important element of a mobile network. Authentication involves two functional entities, the SIM card in the mobile, and the Authentication Center (AuC). Each subscriber is given a secret key, one copy of which is stored in the SIM card and the other in the AuC. During authentication, the AuC generates a random number that it sends to the mobile. Both the mobile and the AuC then use the random number, in conjunction 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.

1.5.3 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 sub layer 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 sub layer include call establishment, selection of the type of service (including alternating between services during a call), and call release.

(a) Call Routing

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

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

The routing information that is returned to the GMSC is the Mobile Station Roaming Number (MSRN), which is also defined by the E.164 numbering plan. MSRNs are related to the geographical numbering plan, and not assigned to subscribers, nor are they visible to subscribers.

The most general routing procedure begins with the GMSC querying the called subscriber's HLR for an MSRN. The HLR typically stores only the SS7 address of the subscriber's current VLR, and does not have the MSRN (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 Figure 1.3).

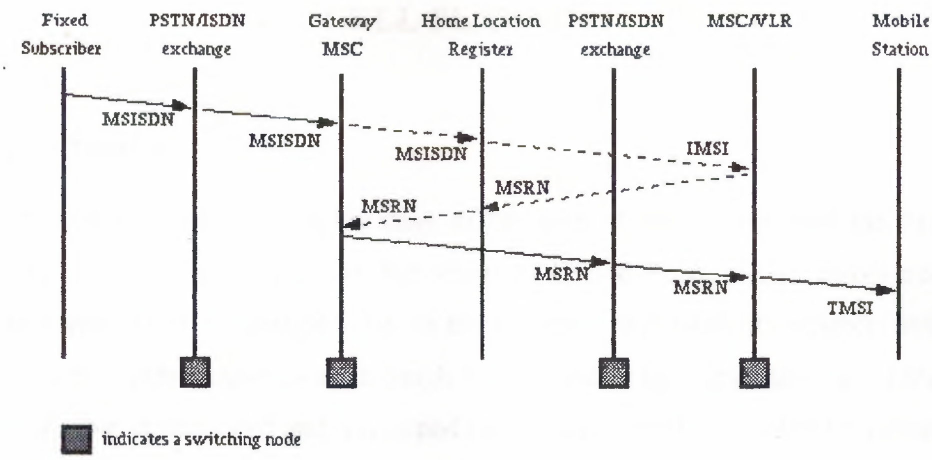


Figure 1.3, Call routing for a mobile terminating call

CHAPTER 2
CELL PLANNING

2.1 Introduction

It was some time since the days of Heinrich Rudolf Hertz until the first real achievements of cellular radio. In the years 1887 and 1888, Hertz discovered that invisible waves which originated from an electric spark were able to transport *influence* or, as we call it today, *information* through the air. Only a few years later, this phenomenon was further investigated and developed until it was possible to actually transmit and receive signals over a distance of several kilometers. Guglieimo Marconi performed a dramatic demonstration of this several years later.

These early experiments formed the basis not only of cellular radio, but also of many types of transmissions. One merely has to think of early radio broadcasting, which was introduced in the early 1920s in the United States and Europe, to see how far these first experiments have taken society. Later applications for radio found quick and numerous paths to mass markets, even though the quality of the early AM transmissions were not very good by today's standards. The introduction of FM by Edwin H. Armstrong in 1929 was a breakthrough for quality of reception, and it became the standard for the remainder of the century. The current analog cellular networks are still based on Armstrong's FM.

Mobile radio applications took a longer and more halting path to their markets. In the days when the first transmitters started broadcasting, people were trying to make use of this technique for mobile applications, but they had a problem in that the transmitters were still very large. In the first applications for mobile radio, only the receiving system was mobile, similar to the paging systems, which are so popular today. There were experiments by police departments, which used only one high-power transmitter to cover a whole city. The called police officer had to get out of his car at the next public telephone to report back to his office for further instructions. This awkward procedure and the limited ability of the receiver to withstand the problems of propagation and road hazards were limiting factors for mobile radio.

When FM was introduced, the quality of received information increased a great deal, but the applications were still limited by transmitter size and the huge amounts of power consumed at the mobile end of the communications links by those early transmitters.

Commercial mobile phone service had to wait for the perfection of the public dispatch systems, such as police and other public safety applications. The breakthroughs were small, low-power transmitters (run from motor generators in the vehicle), and the move to higher operating frequencies (above 30 MHz) to further decrease the size and weight of mobile transmitters. An initial step toward viable mobile phone service appeared with the radio common carrier (RCC) and mobile telephone service (MTS) systems. These were simply conventional land mobile radios fitted with a special control panel, called a *control head,* which were suitable for commercial use by people who were unfamiliar with operating two-way radios. The RCC and MTS systems could direct calls from a single transmitter to a particular mobile, but remained, after all, simple dispatch systems in which the users set up all their calls through a mobile operator. Later, some additional inband tone signaling was added to the MTS system to make the newer improved mobile telephone service (IMTS), which automated to a considerable extent the interface between the mobile customer and the fixed telephone network. The mobile operator almost disappeared from the mobile phone landscape when IMTS was introduced. Cellular radio became popular only when carefully designed, engineered, and thoroughly tested systems like AMPS and TACS started to work.

2.2 Cellular Structure

In the beginning of radio, engineers were happy to achieve a simple dedicated link between a transmitter and a receiver. These first links were not even two-way ones, but remained one-way dispatch links; that is, the people who called the mobiles did not get a response right away and did not even get a confirmation that their calls had reached the mobile addressees. The next step was to establish a two-way transmission link that allowed an immediate response. This came with mobile transmitters, but the structure of the network was simplistic and awkward to use. Service was limited to a certain area that could be reached with one transmitter or a small collection of transmitters on different channels at a single base site (Figure 2.1). We call the coverage area a *cell.* The cell or network size was determined by the transmitter's power. It was not possible to have a link between two different cells, or coverage areas, since an orderly means of directing traffic (voice audio) between transmitter sites and moving mobiles was missing. It was important to select the frequency of the transmitter and receiver in the cell carefully so that there was no interference from other systems, perhaps in the next town, which would interfere with the system's local operation.

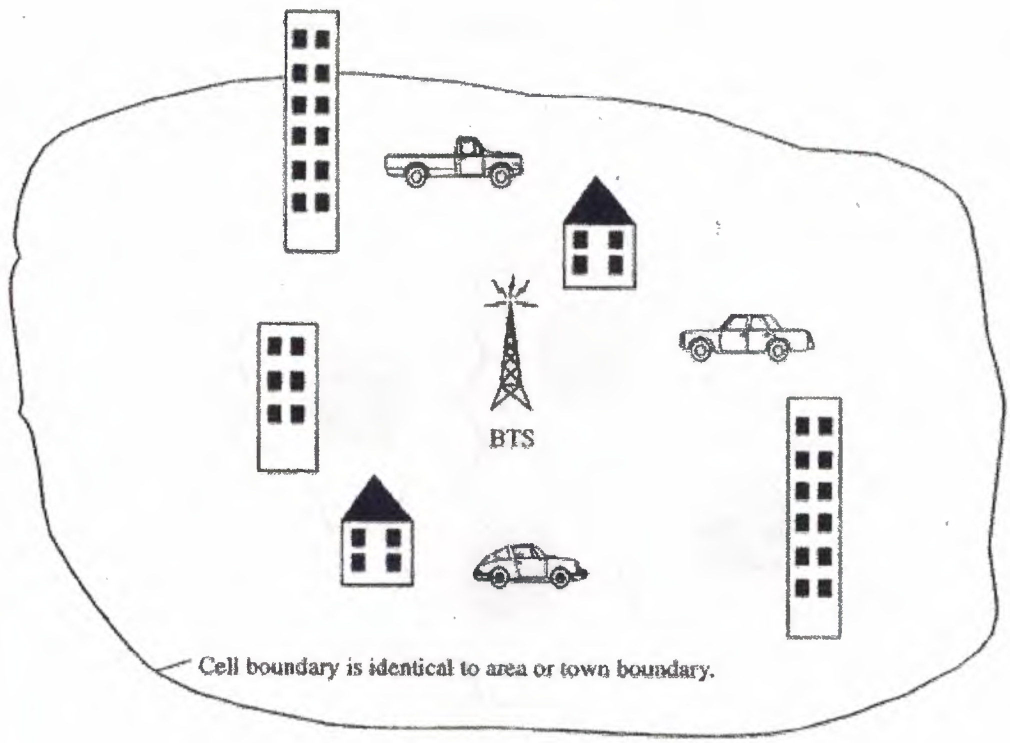


Figure 2.1, Single-Cell Structure

The disadvantage of this is obvious to everyone from today's perspective. A small set of frequencies was used for a huge area. The transmitters were so powerful that their operating frequencies could not be reused for hundreds of kilometers. This was a major limitation to the capacity of the system; once a channel was in use, the channel was tied up over the whole coverage area, even though the need for a mobile communications channel was confined to a small part of the network's service area. One could argue that capacity was not an issue in those days, for the mobile radios were expensive enough to limit the need for capacity below that of the technical limits of the system. Eventually the price of the mobile equipment dropped so low that the artificial capacity threshold was broken, and long waiting lists were common in the 1960s and 1970s for even rudimentary mobile phone service. A search for a solution continued in many countries. The possibility of allocating more frequency space was not a viable one. Other institutions and agencies needed spectrum too.

An idea was proposed to split the frequency band allocated to one cell among many cells, and has several cells coexist next to each other (Figure 2.2). The cellular structure was born. In order for this scheme to work properly, some restrictions had to be applied:

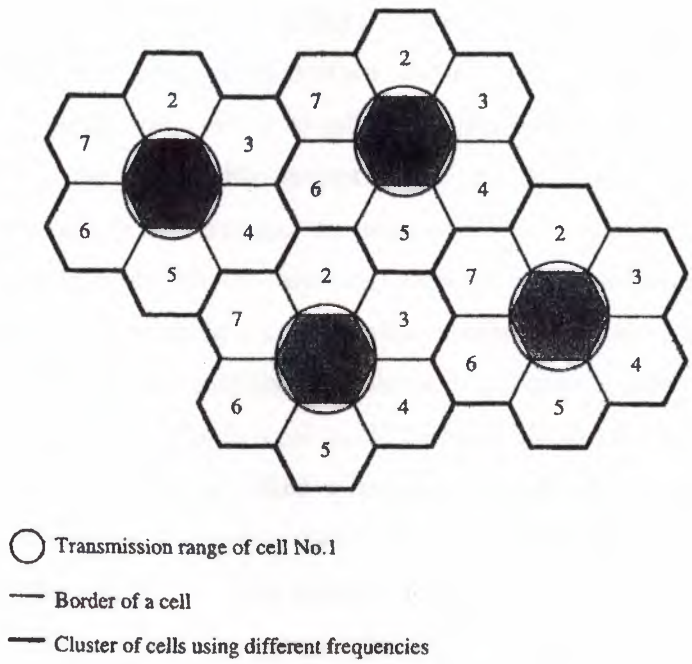


Figure 2.2, Cellular Structure

The frequencies had to be reused only within a certain pattern in order to reduce the interference between two different stations using the same channel. Neighboring cells could not share the same channels.

The power levels used within the single cells had to be carefully limited, again to reduce the interference between the different stations. Receiver filters had to be improved.

The pattern used for early systems was the seven-cell reuse pattern, which was a result of the distance required between cells using the same frequencies, yet again to preclude excessive interference. Interference had to be limited to some level that could be handled by the input filters of all the receivers in all the cells. Typically, a distance of about 2.5 to 3 times the diameter of an average cell had to be reserved between base site transmitters to guarantee that interference would not render the system useless. Calculations and experiments dictated this reuse pattern. If the systems were carefully designed and installed, more users could be accommodated as the same frequencies were used more and more times in the system.

In the early systems, it was not possible to roam among the cells. This meant that a user was not able to travel freely between cells while engaged in a single phone call. It was also not possible to place a call from the fixed network to a particular mobile station (MS) without knowing the exact position of the mobile. Each area had its own code, and a mobile station within this area had to be called with this code in a manner similar to the use of area codes in the fixed public network. The only difference is that in the fixed public network, the phones are fixed and the area codes do not change. The introduction of much more intelligence into the network, together with additional audio routing equipment, made roaming possible. Registers were installed in the network, which traced all the mobiles and stored their positions in order to route calls to them. These registers could be queried so that the audio in a call could be passed from cell to cell as needed. A single incidence of this process is called a handoff or handover, and a host of details within both the network and the mobile station itself need to be carefully coordinated for this process to happen reliably. Mobile stations, for example, have to be equipped with synthesized transmitters, which can change operating frequencies quickly. The network has to have sufficient equipment and signaling to make sure the handover or handoff is directed to the correct cell site

2.2.1 Types Of Cells

The density of population in a country is so varied that different types of cells are used:

- Macrocells
- Microcells
- Selective cells
- Umbrella cells

(a) Macrocells

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

(b) Microcells

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

(c) Selective Cells

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

(d) Umbrella Cells

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

A too important number of handover demands and the propagation characteristics of a mobile can help to detect its high speed.

2.3 Network Planning

If one thinks of a country as varied in population density as the United States, it is easy to understand that it does not make sense to apply the same size to each cell. It makes a difference if an operator has to supply a big and densely populated city, such as

New York, with a network, or a remote and sparsely populated area, such as the island of Hawaii. Different possibilities of network planning and cell planning have been developed:

Cell-splitting or microcell applications. As the number of subscribers grew larger, the density within these networks also became higher. The operators and radio engineers had to look for new capacity funds. A rather basic idea was to split the existing space into smaller portions, thus multiplying the number of channels available (Figure 2.3). Along with this simple scheme, the power levels used in these cells decreased, making it possible to reduce the size of batteries required for mobile stations. With the decreased power required for mobiles came decreased size and weight. This made the networks more attractive to new users.

Selective cells. It does not always make sense to have circular cells. Radio engineers designed cells with a wide variety of shapes, together with the required antennas, which are able to confine transmitted power within a particular area and exclude power from adjacent areas.

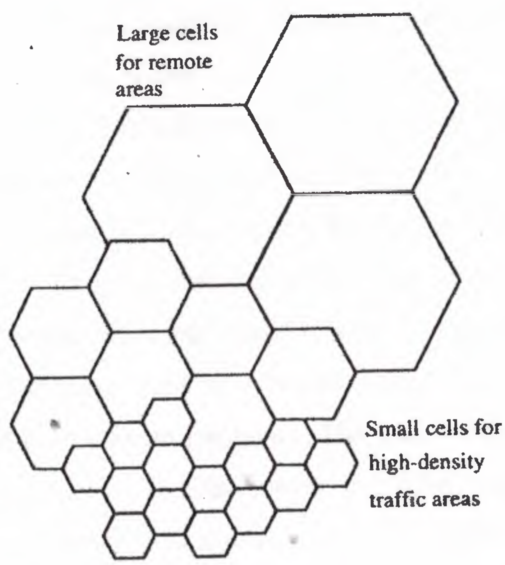
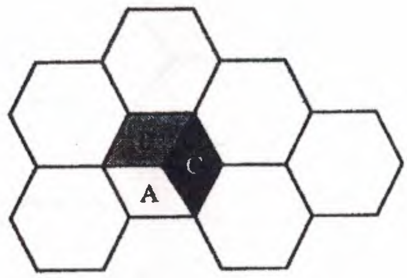


Figure 2.3, Cell Splitting And Microcells

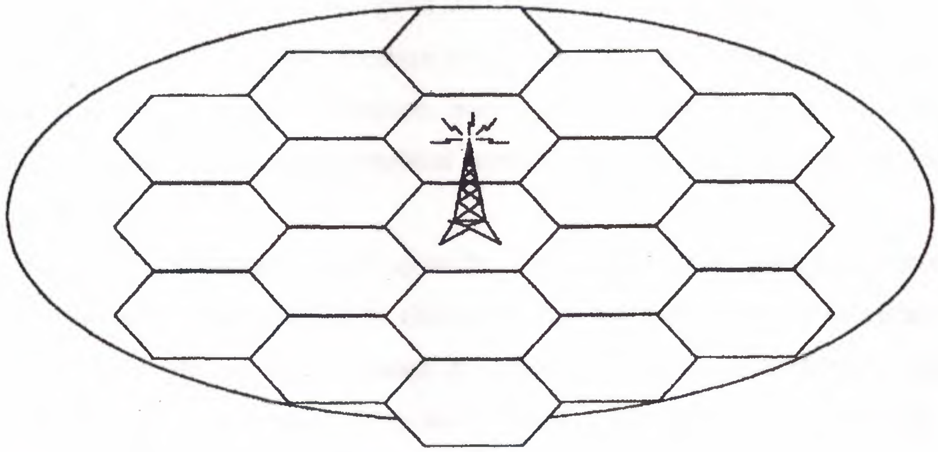
The most common of these selective coverage schemes is the sectored cell, where coverage is confined to individual 120-deg sectors rather than the typical full 360-deg coverage (Figure 2.4). Such antennas may be located at the entrances of tunnels, on the edge of a valley, or at the ends of streets among skyscrapers.



Three direction location

Figure 2.4, Selective Cells

Umbrella cells. When the cell-splitting technique was first applied, the operators realized that a freeway crossing within very small cells caused a large number of handovers among the different small cells. Since each handover requires additional work by the network, it is not particularly desirable to increase the number of such events. This is particularly true on European freeways, where the average speed is very high. The time a mobile on such a European freeway would stay in one cell decreases with increasing speed. Umbrella cells were introduced (Figure 2.5) to address this problem. In an umbrella cell, power is transmitted at a higher power level than it is within the underlying microcells and at a different frequency. This means that when a mobile that is traveling at a high speed is detected as a fast mover, it can be handed off to the umbrella cell rather than tie up the network with a fast series of handoffs. Such a mobile can be detected from its propagation characteristics or distinguished by its excessive handoff demands. In this cell, the mobile can stay for a longer period of time, thus reducing the workload for the network.



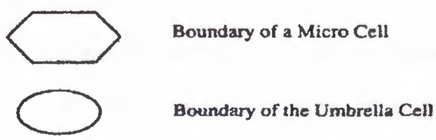


Figure 2.5, Umbrella Cells

2.4 Mobile Radio Network Planning Tasks

The mobile radio network is the connecting element between the mobile telephone users and the fixed network.

In this network the base transceiver station equipment (BTSE) is the direct interface to the subscriber. It has to make radio communication channels available to the users and to care for a satisfactory signal quality within a certain area around the base station. This area may be split into different sectors (cells), which belong to one BTSE.

Planning a mobile radio network is a complex task. Because radio propagation along the earth surface is submitted to many influences due to the local environment. Furthermore the performance requirements to a radio network cover a wide field of applications, which depend on the operator's potentialities and goals. To respond to all these subjects, it is necessary to observe a certain sequence of tasks.

The first step is to get knowledge about the customers/operators objectives and resources (basic planning data). On this basis it is possible to estimate the size of the project and to establish a coarse nominal cell plan.

Then it is necessary to install a digital terrain database into a planning tool, which contains topographical and morphological information about the planning region. This digital map permits to make more accurate predictions about the radio signal propagation as compared to the first rough estimation, and to create a more realistic cell structure, including the recommendable geographical positions of the base stations equipment (coarse coverage prediction).

The network elements defined up to this moment have been found on a more or less theoretical basis. Now it has to be checked if the envisaged radio site locations may realty be kept A site survey campaign in accordance with the customer, who is responsible for the site acquisition, must clarify all Problems concerning the infrastructure and technical as well as financial issues of the BTSE implementation. Inside a tolerable search area the optimum site meeting all these issues has to be selected.

This site selection should also take into account particular properties of the area, e.g. big obstacles that are not recognizable in the digital maps.

Field measurements, to be carried out in typical and in complex areas must give detailed information about the radio characteristics of the planning region. The measurement results will then help to align the radio prediction tool for the actual type of land usage (tool tuning).

Now, fixed site positions and an area-adapted tool being available, it is possible to start the detailed radio planning. The final network design has to care for both sufficient coverage and proper radio frequency assignment In respecting the traffic load and the interference requirements.

The last planning step is the generation of a set of control parameters, necessary to maintain a communication while a subscriber is moving around. These parameters have to comply with the existing cell structure and the needs to handle the traffic load expected in each cell.

After commissioning of the network, the performance must be checked by the network operator by evaluation of statistical data collected in the operation and maintenance center. Situations of congestion or frequent call rejections may be treated by modification of the pertinent control parameters and lead to an optimized network.

The individual planning steps are considered more closely in the following sections.

2.4.1 Collection of Basic Planning Data

The requirements of the network operator concerning traffic load and service area extension are basic data for the design of a mobile network. A coarse network structure complying with these requirements can be created on this basis.

Two fundamental cell types are possible; their properties may be determined
a) By the maximum radio range of the involved transceiver stations and mobile terminals; the range is limited by the available transmit power and the noise figure of the receivers. This type is called a noise-limited cell; it is typical for rural regions.
b) Or it may be determined by the limited traffic capacity of a cell in the case of high subscriber concentration. This leads to the implementation of small cells, mainly in urban areas where interference will become the major problem.

The result of this first planning step is a rough estimate of the network structure, called a nominal cell plan, which gives knowledge about the number of radio stations, their required technical equipment and their approximate geographical positions. Thus allowing assessing the monetary volume of the project.

2.4.2 Terrain Data Acquisition

Mobile communication occurs in a natural environment. The radio signal propagation is highly affected by the existing terrain properties like hills, forests, towns etc. Therefore the real mapping data must be taken into account by the planning tool.

Absorbing, screening, reflecting and diffracting effects of the surrounding objects and along the radio path influence the signal level encountered by a subscriber in the street.

To make realistic signal level predictions, the propagation models implemented in the prediction tool must be fed with the relevant terrain data.

A very important factor for correct modeling is the morph graphic classification of an area:

- Building heights and density of built up areas (metropolitan, urban, suburban, village, industrial. residential) or forest, parks, open areas, water etc.

The screening by hills, which may affect the coverage of a service area, must be made evident by consideration of the terrain profile (height contour lines).

The procurement of digital maps with this information may be rather expensive. The prediction accuracy is directly related to the size of area elements (resolution) and to the reliability of these information (obsolescence of maps!)

2.4.3 Coarse Coverage Prediction

On the basis of the digital terrain database and by using standard propagation models, which have been preselected to fit for special terrain types, it is possible to make field strength predictions without having a very detailed knowledge of the particular local conditions.

By variation and modification of the site positions and antenna orientations, coverage predictions of rather good quality may be attained.

Yet the definitive site locations are subject to an Eater scheduled site selection process in accordance and by cooperation with the customer.

The particular local characteristics must be introduced later by comprehensive survey measurement. These measurements will be used to upgrade the propagation models.

2.4.4 Network Configuration

The results of the "coarse prediction" steps will allow defining the radio network configuration and the layout of individual base stations.

A first frequency allocation plan may also be derived from these predictions. The result might already be a well functioning network. But it is still based on assumptions. The actual impact of the natural environment must be considered in the following steps. Nevertheless, the "coarse planning" results will help to better assess the special details brought in by the real situation.

In designing the radio network one has to keep in mind the requirements emerging from an increasing subscriber number. A multiple phase implementation plan has to govern the network configuration concepts.

In the initial phase a relatively low number of users has to be carried. On the other hand complete coverage of the service area has to be provided from the beginning. Existing sites of the first implementation phase must be useable in later phases. Increasing subscriber numbers (synonymous with increasing interference tendency!) should be responded by completion of the existing TRX-equipment and by addition of new sites. This means reconfiguration of the existing cell patterns and frequency reassignment. The planner should anticipate the future subscriber repartitions and concentrations from the beginning, in creating cell structures capable to respond to future needs,, increasing interference problems arising with higher site density may be overcome by down tilting of directional antennas initially mounted for maximum signal range, as now the radio cell areas will be smaller.

2.4.5 Site Selection

The site positions found in the coarse planning process on a theoretical basis, must now be verified in a joint campaign, called site survey, between the customer and the radio network planner. All site candidates within a tolerable search area around the theoretical site positions must be checked.

This check includes the availability of electric power and of data transmission lines.

The most important topic is the possibility to install the antennas in a suitable height above the roofs or above ground.

Environmental influences (screening obstacles, reflectors) have also to be regarded. The best fitting site should be selected.

Another important task of this campaign is to declare a certain number of the radio sites be suitable to serve as „ survey sites". This means that radio field measurements shall be done with these stations as transmitters. The resulting measurements will be used for the alignment of radio propagation models.

The environment of the survey sites should be typical for a considerable number of other radio sites.

2.4.6 Field Measurements

Digital terrain databases (DTDB) as derived from topographical maps or satellite pictures do not contain all details and particularities of the existing environment. Especially in fast developing urban areas maps cannot keep pace with reality and thus reflect an obsolete status. Keeping maps on this quality level would be very expensive.

The characteristics of built up zones and vegetation areas with respect to radio propagation differ in a wide range if we regard different countries. Even climatic conditions may influence the signal level. Knowledge about this specific behavior must be acquired by measurements.

The survey measurements have to be carried out in typical areas. Evaluation of these measurements will result in models that can be applied in comparable areas as well.

Special measurements must be carried out in very complex topographical regions where standardized propagation models will fail. The resulting models are valid exclusively for this measurement Zone.

2.4.7 Tool Tuning

The measurement results have to be compared with the predictions of proven standard models. The standard parameters will be slightly modified to achieve minimum discrepancies with the measurements, i.e. to keep the mean error and rms-error as low as possible. As the signal level is subject to statistical variations, which cannot be predicted, the rms-error will never be zero.

The reliability of the created models increases with the number of measurement runs that can be exploited.

The new specific model may also be applied in other base stations located in similar environment.

2.4.8 Network Design

The area-specific models are the basis for the final planning steps. The detailed network design has to care for

- A suitable signal level throughout the planning area
- Sufficient traffic capacity according to the operators requirements
- Assignment of the pertinent number of RF-carriers to all cells

Sufficient decoupling of frequency reuse cells to respect the interference requirements for co-channels and adjacent channels.

Moreover, attention has to be payed to an optimized handover scenario in heavy traffic zones.

The detailed planning process commits the final structure of the radio network and the configuration of the base stations.

The capacity of digital data links connecting the radio stations to the fixed network elements may now be defined.

2.4.9 Data Base Engineering

A cellular network is a living system with moving subscribers. The service must be maintained while mobiles change radio cells and superior organization units, called location areas. Ail control parameters, necessary to support this task, have to be administered and supervised in central databases.

There is a permanent signaling information exchange between mobiles base stations and control centers.

This signaling communication occurs on predefined time slots, called control channels, which are assigned to one of the RF-carriers of each radio cell.

Important control information's for each radio cell are:

- Cell identification within the network
- Control carrier frequency
- Potential neighbor cells
- Minimum received signal level
- Maximum transmit power of a mobile
- Power reduction factor to perform power control
- Power margin for handover to neighbor cells

2.4.10 Performance Evaluation and Optimization

Regular performance checks must be carried out after commissioning of the network. These checks comprise the evaluation of statistical data collected in the "operations and maintenance center" (OMC) as well as measurements by means of test mobile stations to explore e.g. handover events under realistic conditions; unwanted handover may lead to traffic congestions in certain cells, or may drain off traffic from other cells.

Detection of murtipath propagation problems-caused by big reflecting objects is also subject to measurements.

Another goal of these checks is to investigate the real traffic load and its distribution, as subscriber behavior in a living system will not necessarily reflect the original assumptions of the operator; assumed hot traffic spots may have been changed or shifted after a couple of years.

Careful evaluation of the measurement data will help to optimize the network performance by modification of the system parameters. As the number of subscribers will normally increase in course of time, supervision and control of these parameters should become a permanent maintenance procedure.

2.5 Radio Wave Propagation

There are three main components of radio propagation:

- Mean path loss (loss due to distance between MS – BS),
- Shadowing (long term fading),
- Multi path propagation (short term fading).

2.5.1 Path Loss

Standard path models are of the form:

$$L_m[dB] = A + B\log d[km]$$

Where L_m is the mean propagation path loss between the base station (BS) and the mobile station (MS) at a distance d.

A: unit loss at 1 km.

B: propagation index or loss per decade.

The propagation coefficients A and B depend upon :

- Transmit frequency,
- The MS and BS antenna height,
- The topography and morphology of the propagation area.

2.5.2 Shadowing – Long Term Fading

In larger cells where the BS antenna is installed above the roof top level, details of the environment near the MS is responsible for a variation of the received level around the mean level calculated.

Usually this variation of level – caused by obstacles near the MS (e.g. building or trees)- is described by the statistical model, i.e. the total path loss L_{tot} is given by the mean "distance" path loss plus a random shadowing:

$$L_{tot}\,[\mathrm{dB}] = L_m + \mathrm{S}$$

S < 0: free line of sight,

S > 0: strong shadowing by e.g. a high building near the MS.

S has a Gaussian distribution (fig 2.6) with mean value 0and a standard deviation s which typically lies in the range s = 4... 10dB.

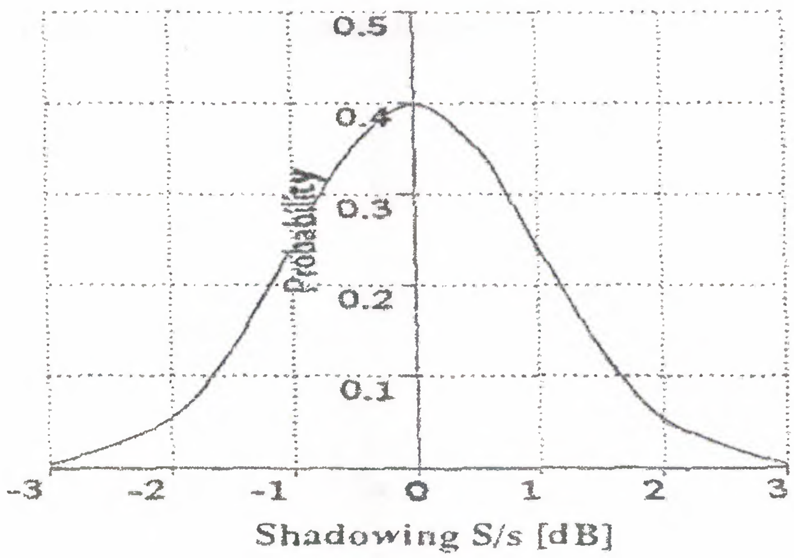


Figure 2.6, Gaussian distribution of Shadowing S

The length scale for variation of the long-term fading is in the 5... 100m, i.e. the typical size of the shadowing obstacles.

2.5.3 Multi Path Propagation – Short Term fading

The superposition of several reflected waves arriving at the receivers on different paths are therefore with different amplitudes and phases cause peaks (constructive superposition) and deep fading dips (destructive supervision) of the received level.

The length scale of variation (e.g. peak to peak) is given by the half of the transmission wavelength, i.e. about 15 cm for GSM 900 or 7.5 cm for DCS 1800.

The statistics of the Rayleigh is described in the following way:

Consider the received level due the path loss and long term fading, which is called local mean: $L_{loc}[dB]$.

2.6 Cellular Networks and Frequency Allocation

One important characteristic of cellular networks is the re-use of frequencies m different cel(s. *By* re-using frequencies, a high capacity can be achieved. However, the re-use distance has to be high enough, so that the interference caused by subscribers using the same frequency (or an adjacent frequency) in another cell (fig 2.7 and 2.8) is sufficientty low.

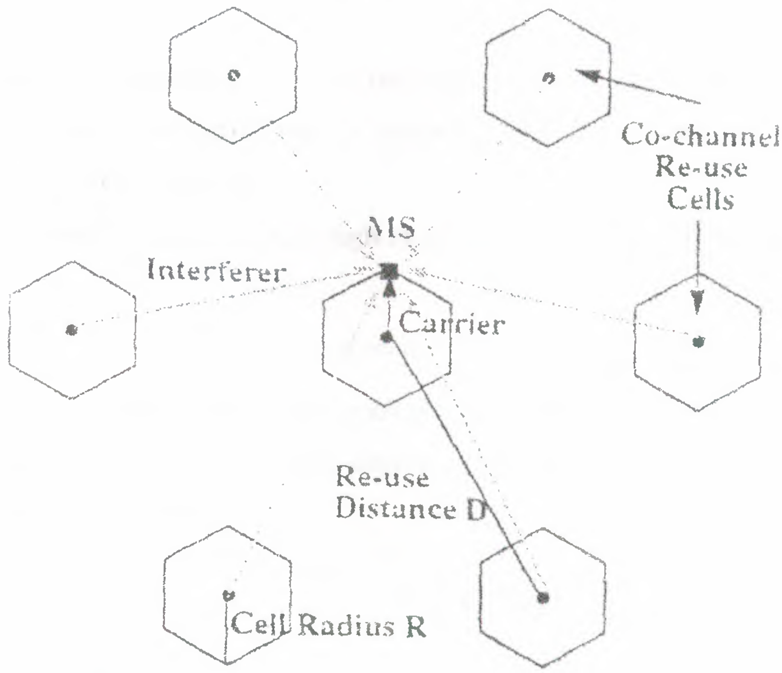


Figure 2.7, Cellular Network and Frequency Allocation

To guarantee an appropriate speech quality, the carrier-to-interference-power-ratio CIR has to exceed a certafn threshold CIR_{min} that is 9 dB for the GSM System.

For homogeneous hexagonal networks frequencies can J3e allocated to ceîls in a symmetric way. Defining the ciuster size K as gcoup of celis in which each frequency is used exactty önce, the fo!iow-ing reiatîons between Ciuster Size, Ceįl Radius and Re-use Distance are obtained.

Inserung ine Tormula tor the ciuster size into the formula tor the minimum CIR one obtains:

$$0.5 \times B \log 3K > CIR_{min} + LTFM(\times\%) + 10 \log N_1$$

which gives a lower bound for the cluster size which can be used.

For a gıven cluster size K and total number of frequencies N_{tot}, the number of frequencies per cell N_{cell} is gıven by:

$$N_{cell} = N_{tot}/K$$

i.e. the capacity of a cell can be increased by reducing the cluster size.

A reduction of **cluster** size can be achieved by

- Reducing the number of interferers → Sectorisation.
- Reducing the interference from co-channel cells → Power Control, Discontinued Transmission. ...

Obviousiy a real netvvork does not have such a regular hexagonal structure and frequency allocation is performed by planning tools using comptex algorithms for optimizing the CIR in each cell.

The objective is to achieve a high mean value of frequencies per cell $<N_{cell}>$. The ratio:

$$<K>= N_{tot}/N_{cell}$$

can viewed as the mean cluster size in such an inhomogeneous envjronment.

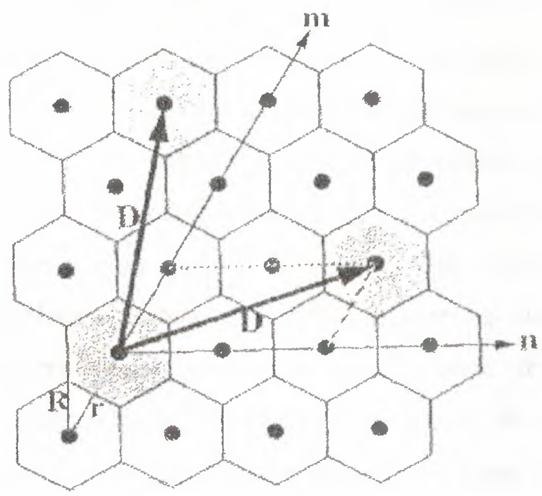
The capacity of the radio netvvork depends upon the available number N of radio channels per area F (e.g. F= 1 km^2).

$$\frac{N}{F} = N_{cell} \times \frac{N_{BTS}}{F} = CPF \times \frac{N_{tot}}{K} \times \frac{1}{F/N_{BTS}} = CPF \times \frac{N_{tot}}{K} \times \frac{i}{CA}$$

N_{BTS} : number of BTS

CA: ceil area

CPF: channel per frequencies



Outer Cell Radius R

Inner Cell Radius $r = 0.5 \times \sqrt{3} \times R$

Re-use Distance

$$D = R \times \sqrt{3 \times (n^2 + m^2 + nm)}$$

Cluster Size

$$K = \sqrt{(n^2 + m^2 + nm)}$$

$n, m = 0, 1, 2, 3, \ldots$

$K = 1, 3, 4, 7, 9, 12, 16, 19, \ldots$

Figure 2.8, Frequency re-Use and Cluster Size.

2.7 Handover / Handoff

The *handover* or *handoff* procedure is a means to continue a call even when a mobile station crosses the border of one cell into another. As mentioned earlier, the handover or handoff technique, from one cell to another, finally made the mobile station really mobile. Before the introduction of this feature, a call was simply dropped when the cell border was crossed or when the distance between the mobile station and one particular base station became too large.

In a cellular network, one cell has a set of neighboring cells. The system, therefore, has to determine which cell the mobile station should be passed to. The method used to determine the next cell to use differs in analog and digital systems. The difference in the procedure can be determined from the different names. The handoff comes from the analog world, whereas handover was introduced by GSM. The term *handover* will be used when talking about the GSM system, and the term *handoff will* be used when talking about analog systems.

In analog systems, the base station monitors the quality of the link between a mobile station and itself. When the base station realizes that the quality of the link has degraded and the distance to the mobile station has become too large, it requests the adjacent cells to report the power level they see for the mobile back to the network. It is reasonable that the strongest reported power level for the mobile comes from the closest cell to the mobile station. The network then decides which frequency channel the base station should use in the new cell and which corresponding frequency the mobile should tune to. Eventually, the mobile station is commanded to perform a channel change.

The mobile station is the passive participant in the handoff process. All the measurements and subsequent work are done in the base stations and the network. Cell sites are equipped with a *measuring receiver* used to measure the power level of the different mobile stations on the various frequency channels in use. For those readers interested in analog cellular systems, the distance measurements within cells is sometimes determined from the relative phase of the *supervisory audio tones* (SAT) that the mobiles transponder back to the base stations. The distance is half the time of the phase shift multiplied by the propagation speed of the signal.

The situation in the GSM system is different. The mobile station must continuously monitor the neighboring cell's perceived power levels. To do this, the base station gives the mobile a list of base stations (channels) on which to perform power measurements. The list is transmitted on the base channel (again, system information), which is the first channel a mobile tunes to when it is turned on. The mobile station performs continuous measurements on the quality and the power level of the serving cell, and of the power levels of the adjacent cells. The measurement results are put into a *measurement report,* which are periodically sent back to the base station. The base station itself may also be performing measurements on the quality and power of the link to the mobile station. If these measurements indicate the necessity for a handover, such can be performed without delay, as the appropriate base station for a handover is already known. The measurements are coming in constantly, and they reflect the mobile's point of view. It is up to the operator to act upon different quality or power levels, and the handover constraints or thresholds can be adjusted in accordance with changing environment and operating conditions.

The GSM system distinguishes different types of handovers. Depending on what type of cell border the mobile station is crossing, a different entity may have to control the handover to ensure that a channel is available in the new cell. If a handover has to be performed within the area of a BSC, it can be handled by the BSC without consulting the MSC, which, in any case, must at least be notified. This type of handover Is called a simple handover between BTSs (Figure 2.9).

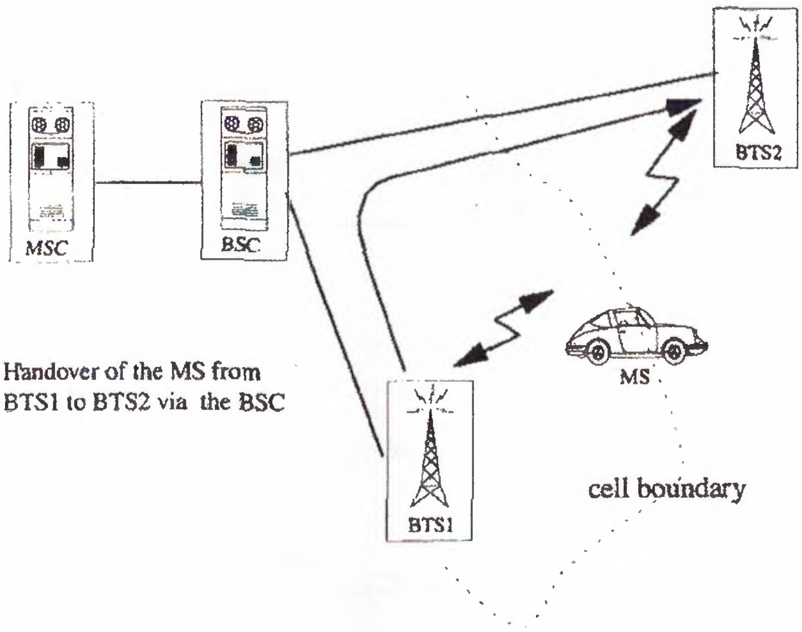


Figure 2.9, Handover Between BTSs

If, instead, a mobile station is crossing the border of a BSC (rather than a BTS), then the MSC has to control the procedure in order to ensure the smooth transition of the conversation. This can be continued for a handover between two MSCs (Figure 2.10). The only difference, in this latter case, is that even though the mobile is eventually handled by the second MSC, the first MSC still has to maintain control of the call management.

In theory, it is possible to perform a handover at a political border between two countries. There are no technical restrictions to this feature. Due to the different roaming agreements, however, it is not possible to start a phone call, let us say, in Germany, and cross the border to Switzerland and still continue the call. The call will be dropped, and subscribers have to register themselves in the new foreign network.

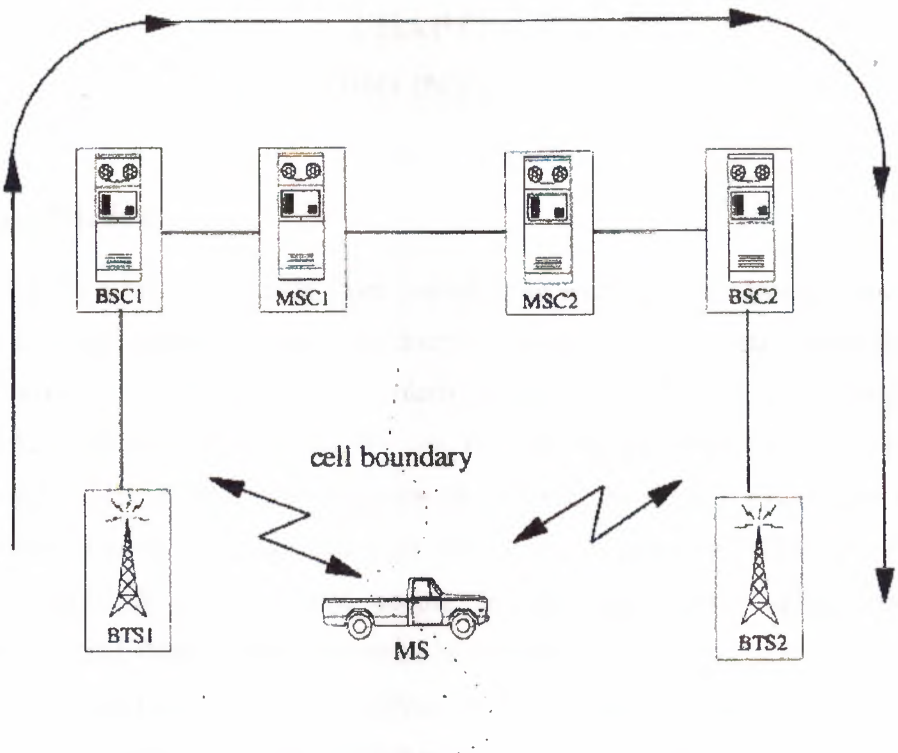


Figure 2.10, Handover Between MSCs

CHAPTER 3
RADIO INTERFACE

3.1 Introduction

Radios move information from one place to another over channels, and a radio channel is an extraordinarily hostile medium on which to establish and maintain reliable communications. The channel is particularly messy and unruly between mobile radios. All the schemes and mechanisms we use to make communications possible on the mobile radio channel with some measure of reliability between a mobile and its base station are called the *physical layer,* or the *Layer 1* procedures. These mechanisms include modulation, power control, coding, timing, and a host of other details that manage the establishment and maintenance of the channel

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

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

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

Two frequency bands, of 25 M Hz each one, have been allocated for the GSM system:

- The band 890-915 M Hz has been allocated for the uplink direction (transmitting from the mobile station to the base station).
- The band 935-960 M Hz has been allocated for the downlink direction (transmitting from the base station to the mobile station).

But not all the countries can use the whole GSM frequency bands. This is due principally to military reasons and to the existence of previous analog systems using part of the two 25 M Hz frequency bands.

3.2 Access to Trunking Systems:

Unless the reader who is familiar with analog radio systems also has considerable experience with fixed wire-line telephone systems, the notion of access will be unfamiliar and confusing. It is for this reason, therefore, that we explore various forms of access to trunked radio resources in an intuitive way.

If the number of channels available for all the users of a radio system is less than the number of all possible users, then such a system is called a *trunked* radio system. Trunking is the process whereby users share a limited number of channels in some orderly way. Sharing channels, or providing fewer channels than there are users who need them, works because we can be sure that the likelihood that everyone will want a channel at the same time is very low. The method of sharing channels is termed *access;* users ask for and are granted access to the trunked resource. A cellular phone system is a trunked radio system, because there are fewer channels than there are subscribers who could possibly want to use the system at the same time. Access is granted to multiple users of the system by dividing the system into one or more of its operating domains: frequency, time, space, or code.

3.2.1 Frequency-Division Multiple Access

Frequency-division multiple access (FDMA) is the most common form of trunked access and is what most radio people think of when they hear the words *access* or— *channel.* With FDMA, users are assigned a channel from a limited set of channels ordered in the frequency domain. If the number of available channels is greater than about 15, then the best trunking efficiency is realized if the initial assignments to channels are made from a common control channel, to which all radios tune for instructions when they first try to use the system. There are a bewildering variety of signaling schemes used in FDMA systems. Radios designed to be used in such systems seek out and then tune to the designated control channel when they are turned on. On this control channel, the radios find signaling data that contain instructions on which frequency new entrants should tune their transmitters and receivers to when they want to pass user traffic, which is often voice. The signaling in these systems works something like a directory of businesses one may see on the lobby wall of a large office building. The larger the number of users assigned to an FDMA system, the greater the catalog of available frequencies must be. Frequency channels are precious and are assigned to systems by government regulatory bodies in accordance with the common needs of a society. When there are more users than the supply of frequency channels can support, users are *blocked* from access to the system. With more available frequencies comes more users, and more users means more signaling information has to pass on the control channel. Very large FDMA systems often have more than one control channel to handle all the access control tasks. An important characteristic of FDMA systems is that once a frequency is assigned to a user, the assigned frequency is used exclusively by the user (even during short periods of silence) until he no longer needs the resource.

There are many small trunked radio systems in the world with fewer than 15 frequencies available for use. Such small systems, which are seldom cellular, usually do not have a dedicated control channel. Instead, a simple signaling routine (tones or data) is included on each and every channel, which tells radios where to tune to for an idle traffic channel. The signaling works something like a "no vacancy" signs in a motel window.

Channels in an FDMA system are defined by their assigned number (e.g., 3), their center frequencies (e.g., 890.600 MHz), and their widths (e.g., 200 kHz).

3.2.2 Time-Division Multiple Access

TDMA is common in fixed telephone networks. The enabling technology in radio systems is speech encoding and data compression, which remove redundancy and silent periods and decrease the time it takes to represent any period of speech. Users are assigned access to a channel in accordance with a schedule. Though there is no strict technical requirement for it, cellular systems, which employ TDMA techniques, always overlay TDMA on top of an FDMA structure. A pure TDMA radio system would have only one physical operating frequency, not a particularly useful system. TDMA is a rather old concept in radio systems, too. The short-wave broadcast services on the HF band (3 to 30 MHz) are assigned channels (operating frequencies) on a worldwide schedule so that they do not interfere with each other during certain propagation conditions.

In modern digital cellular systems, TDMA implies the use of digital voice compression techniques, which allow multiple users to share a common channel on a schedule. Modern voice encoding greatly shortens the time it takes to transmit voice messages by removing most of the redundancy and silent periods in speech communications. Other users can share the same channel during the intervening times. Users share a physical channel in a TDMA system, where they are assigned time slots. All the users sharing the physical resource have their own assigned, repeating time slot within a group of time slots called a *frame*. If everything works well, the users cannot tell that they are using a TDMA system, and each of the users assigned a time slot within a frame will insist they have their own channel. A time slot assignment, therefore, is often called a channel. GSM sorts users onto a physical channel in accordance with simple FDMA techniques. Then the channel's use is divided up in time into frames, during which eight different users share the channel. A GSM time slot is only 577 μs, and each user gets to use the channel for 577 μs every 4.615 ms (577 $\mu s \bullet 8 = 4.615$ ms).

3.3 Channel structure

A channel corresponds to the recurrence of one burst every frame. It is defined by its frequency and the position of its corresponding burst within a TDMA frame. In GSM there are two types of channels:

- The traffic channels used to transport speech and data information.
- The control channels used for network management messages and some channel maintenance tasks.

3.3.1. Traffic channels (TCH)

Full-rate traffic channels (TCH/F) are defined using a group of 26 TDMA frames called a 26-Multiframe. The 26-Multiframe lasts consequently 120 ms. In this 26-Multiframe structure, the traffic channels for the downlink and uplink are separated by 3 bursts. As a consequence, the mobiles will not need to transmit and receive at the same time, which simplifies considerably the electronics of the system.

The frames that form the 26-Multiframe structure have different functions:

- 24 frames are reserved to traffic.
- 1 frame is used for the Slow Associated Control Channel (SACCH).
- The last frame is unused. This idle frame allows the mobile station to perform other functions, such as measuring the signal strength of neighboring cells.

Half-rate traffic channels (TCH/H), which double the capacity of the system, are also grouped in a 26-Multiframe but the internal structure is different.

3.3.2. Control channels

According to their functions, four different classes of control channels are defined:

- Broadcast channels.
- Common control channels.
- Dedicated control channels.
- Associated control channels.

(a) Broadcast channels (BCH)

The BCH channels are used, by the base station, to provide the mobile station with the sufficient information it needs to synchronize with the network. Three different types of BCHs can be distinguished:

- The Broadcast Control Channel (BCCH), which gives to the mobile station the parameters needed in order to identify and access the network
- The Synchronization Channel (SCH), which gives to the mobile station the training sequence needed in order to demodulate the information transmitted by the base station
- The Frequency-Correction Channel (FCCH), which supplies the mobile station with the frequency reference of the system in order to synchronize it with the network

(b) Common Control Channels (CCCH)

The CCCH channels help to establish the calls from the mobile station or the network. Three different types of CCCH can be defined:

- The Paging Channel (PCH). It is used to alert the mobile station of an incoming cal
- The Random Access Channel (RACH), which is used by the mobile station to request access to the network
- The Access Grant Channel (AGCH). The base station, to inform the mobile station about which channel it should use, uses it. This channel is the answer of a base station to a RACH from the mobile station

(c) Dedicated Control Channels (DCCH)

The DCCH channels are used for message exchange between several mobiles or a mobile and the network. Two different types of DCCH can be defined:
The Standalone Dedicated Control Channel (SDCCH), which is used in order to exchange signaling information in the downlink and uplink directions.
The Slow Associated Control Channel (SACCH). It is used for channel maintenance and channel control.

(d) Associated Control Channels

The Fast Associated Control Channels (FACCH) replaces all or part of a traffic channel when urgent signaling information must be transmitted. The FACCH channels carry the same information as the SDCCH channels.

3.4 Burst Structures

Information is moved between radios as data (ones and zeros) that are confined to time slots, and that there are eight time slots in a frame. The frame is something like a freight train with eight freight cars, and the time slots are the individual cars in the train. Now, as with freight trains, where some kinds of freight require special freight *cars (e.g.,* tankers for fluids, hoppers for loose solids, and boxcars for general freight), different burst structures can appear in a time slot when a special kind of data (freight) has to appear on the GSM channel.

One of the freight cars in the GSM freight train as the Power-versus-time template and learned that there are only 542.8 μs allotted in each time slot for data transmissions. This short period accommodates 147 data bits; there are 147 bits in a GSM freight car. Actually, there are 148 bits in each time slot, but the time reserved for the first and last half bits is, as we will soon see, reserved for the on-off RF switching time. Even at this lowest logical level at the time slot or burst level, there are many structures, just as there are many kinds of freight cars. These entire burst structures will be thoroughly explained.

3.4.1 Normal Burst

Figure 3.1 shows the structure, in the time domain, of a *normal burst.* A normal burst is something like a boxcar in a freight train; it carries almost anything except special freight (acids, automobiles, sand, and explosives). A normal burst is the most common burst in the GSM system and is transmitted in one time slot either from the base station or from the mobile station. There are eight time slots in a TDMA frame. The actual user data (coded data) occupy only a portion of the time slot, and the remainder of the bits are reserved for a host of control functions and some demodulating aids.

Type	T	Coded Data	S	Training Sequence	S	Coded Data	T	GP
Number of Bits	3	57	1	26	1	57	3	8.25

148 Bit = 546.12 μs

Figure 3.1, Structure of Normal Burst

Tail Bits (T). This small group consists of three bits at the beginning and the end of each burst and is used as *guard time.* The tail bit time covers the periods of uncertainty during the ramping up and down of the power bursts from the mobile in accordance with the power-versus-time template shown in Figure 3.2. The tail bits are always set to zero. Coincidentally, the demodulation process requires some initial zero bit values.

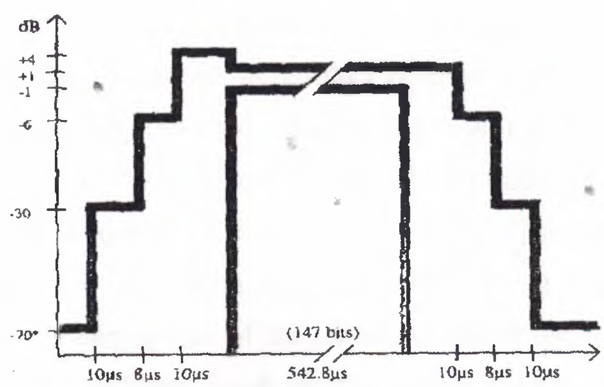


Figure 3.2, Power-Versus-Time template. *70 db or –36 dbm, whichever level is higher

Coded Data. These two times, of 57 bits each, contain the actual transmitted signaling data, or user data. Included and mixed in with the user's payload data are channel-coding bits, which are used in the receiver to help recover the original data. For now, you should think of the coding bits as packing material that protects the freight. Large parts of the remainder of this chapter explain channel coding, or data protection.

Stealing Flag (S). These two bits are an indication to the decoder (in the receiver) of whether the incoming burst is carrying signaling data, which are usually messages the radios use to maintain the link between themselves, or whether the burst is carrying user data. The indicating flag is needed because signaling data are very important and go to different places than user data go. Another word for user data is *traffic.* For example, during- a call, important signaling messages have to be exchanged to complete a handover. When it is time for a handover, the user data are substituted by signaling data

Training Sequence. This is a fixed bit sequence known to both the mobile and the base station, which lets radios synchronize their receivers with the bursts. Synchronization lets receivers interpret the recovered data correctly. It might not be fully clear why this bit pattern is required, since all the timing seems to be well defined so far. The reason we include the training sequence in each normal burst is to compensate for the effects of multipath fading.

Recall that *multipath propagation* results from reflections of the transmitted signal from houses, mountains, and other obstacles. The result is that the same signal takes different paths to the receiver, where each path yields valid signals with different relative time delays and different attenuations. Figure 3.3 shows this effect in principle. The main signal from the mobile station arrives directly at the receiver (the BTS) with no delay and exactly within its assigned time slot, as depicted with the dark arrow. A second signal, depicted with the thin arrows, is reflected from buildings, and arrives somewhat later with certain attenuation. The third signal, depicted with dashed arrows, is reflected from the mountains and has an even greater delay and attenuation. Looking at the figure, it does not seem difficult to distinguish the signals, but the signals typically arrive at the receiver overlapping each other, with nearly the same timing and power levels. The result is a *smearing* or *delay spread* of the recovered data in the receiver. To assist the receiver in separating the different signals, to sharpen and make the recovered data clear, the training sequence is used. There are eight different sequences defined in GSM. All the radios in a particular cell share the same training sequence. Great care was taken to make sure these bit sequences cannot be repeated within the normal coded data part of the burst, and to make the training sequence a unique part of the burst.

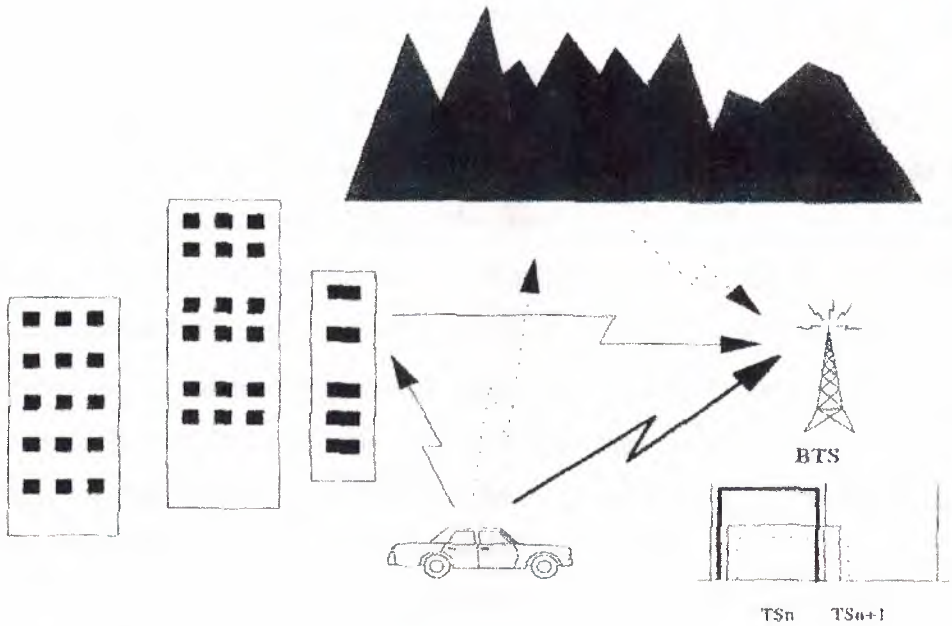


Figure 3.3, Multipath Propagation in the GSM system

The part of the receiver that clears up the distorted and "fuzzy" data and which needs the training sequence to do so is called an *equalizer*. An equalizer is a filter that melds the different signals together into a single nonambiguous signal. The equalizer does this by first looking at the distorted training sequence in each time slot it sees and then adjusting its own filter characteristics to get the original, clean training sequence back again. The equalizer knows what all the training sequences are supposed to look like, and the network tells the equalizer which training sequence to look for in a particular cell. If the training sequence is cleaned up, then all the other bits in the time slot must be clean too. Think of an equalizer as a set of spectacles with corrective lenses for the receiver. The longer the possible delays, the fancier an equalizer has to be. The equalizer in GSM radios can compensate for timing delays of up to 16 μs .

In other words: The training sequence helps the equalizer, which is part of the receiver section of a digital radio, to demodulate the bit content of the data section in the burst. Being a bit pattern that is known to the receiver, the equalizer detects the filter function (so-called *impulse response}* imposed on the modulated signal. This filter function is due to the transmission over the radio interface, including its multipath and Doppler effects. By applying the *inverse* filter function (the equalizer **does** this by calculating appropriate digital filter coefficients) to the signal part containing the data (two times 57 bits), the equalizer then regenerates the actual modulated symbols in the signal .

Guard Period (GP). It probably seems odd to specify *fractions of* a bit, so instead it should be considered as a defined time (measured in bits), rather than as actual data bits. No data are transmitted during the guard period, which is reserved for the ramping time. Taking the bit length defined in the system as 3.69 μs /bit, the guard period can be calculated as 8.25 bits • 3.69 μs /bit = 30.4 μs, which is approximately the time used during power ramping (Figure 3.2). During this time, two consecutive bursts from two mobiles may overlap (i.e., the previous burst ramps down and the current burst ramps up). No data are transmitted during the ramp time (GP), and communication is not disturbed while radios are ramping their RF power outputs.

This explanation of the parts of a normal burst shows that the introduction of TDMA techniques requires additional control functions on the radio path. These additional functions represent an overhead in the system and are part of the price we pay for improved performance.

3.4.2 Random Access Burst

Within a cell, strict timing has to be maintained in order for the bursts from mobile stations to arrive at the base station within their assigned time slots. The assumption is that the link has already been established. What happens *before* the link is established? How can you adjust and synchronize something that does not exist yet? There must be an initial situation during which the base station can make a preliminary rough estimate on timing advance settings for a mobile, a way for the base station to measure the time delay a mobile's burst is experiencing. The delay is proportional to the distance between the base and the mobile, and the distance can change.

If this measurement were taken on a normal burst, there would be a great likelihood that such bursts from many mobiles would overlap each other at the base station, particularly when mobiles are transmitting from the edge of a large cell. To avoid this useless situation, the mobiles use a shorter burst during initial access, which takes the maximum cell radius into account. Even if a mobile station is at the border of a large cell, its shortened burst would still not overlap onto any adjacent normal bursts. The burst type used for this purpose is called the *random access burst.* It gets this curious name from the fact that mobile stations transmit this type of burst at random times and only when the mobile is trying to gain initial access to the system.

Figure 3.4 shows the content of a random access burst. The significance of the bits within the burst is the same as that explained for the normal burst. The *synchronization sequence* has the same significance as the training sequence. The obvious difference is that the synchronization sequence is much longer because the equalizer needs more information; it needs to take a longer look to synchronize properly with a new signal.

Type	T	Synchronization Seq.	Coded Data	T	GP
Number of Bits	8	41	36	3	68.25

88 Bit = 324.72 μs

Figure 3.4, Structure of random Access burst.

Look at the random access burst's long *guard period.* Take the guard period's actual time as 68.25 bits • 3.69 $\mu s/bit = 252\ \mu s$. Perform a rough calculation for the maximum distance (to the BTS) that the random access burst can survive. Ignore propagation conditions and assume the speed of the radio waves is similar to the speed of light. The result is a maximum distance of 252 μs • (3×10^8 m/s) = 75.5 km. Now radio waves have to travel twice the distance between stations in order to have an effect on the link: one way from the BTS to the mobile station, where the mobile station synchronizes with the system's timing, and then the other way from the mobile station back to the BTS. To make sure the random access burst will not collide with a normal burst in the same cell, the maximum allowed distance between mobile station and BTS is half the maximum delay, which is only 37.75 km.

3.4.3 Frequency-Correction Burst

Since timing is a critical need in the system, the base station has to provide the means for a mobile station to synchronize with the master frequency of the system. To achieve this, the base station transmits, during certain known intervals, a pure sine wave signal for the period of exactly one time slot. What a comfort this must be for the mobile. Due to the nature of the type of modulation used in GSM, this can be accomplished by simply sending a fixed sequence of zeros (000. . .) in the time slot. See Section 5.15 for a thorough discussion of this technique. The mobile ' station has precise knowledge of when to expect a *frequency-correction burst.* (See Figure 3.5 for its structure.) Depending on the quality of the clock reference inside the mobile station, the mobile station's design engineer can determine how often it is necessary to resynchronize the mobile station (how often to look for and acquire the frequency-correction burst).

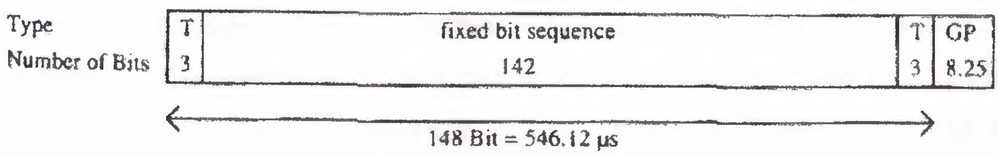


Figure 3.5, Structure of Frequency-Correction burst

3.4.4 Synchronization Burst

When a mobile station starts to synchronize with the network, it first looks for and detects only the frequency where the base channel is located. The mobile does not yet have a key with which to demodulate and decode the information provided in the forward base channel, which is information that contains some valuable system parameters. As was explained previously, the key is one of the eight defined training sequences. The base tells the mobile which key to use with the *synchronization burst.* Figure 3.6 shows the content of this burst type, which is similar to the normal burst. The difference is the longer synchronization sequence and the presence of some diminished coded data. The coded data contain the base station information code (BSIC) indicating the current training sequence (base station color code (BCC)) and the national color code (NCC), and another figure indicating the so-called shortened TDMA frame number.

Type	T	Coded Data	Synchronization Sequence	Coded Data	T	GP
Number Of Bits	3	39	64	39	3	8.25

148 Bits = 546.12 μs

Figure 3.6, Structure of Synchronization burst.

3.5 Frequency Hopping

The propagation of a radio signal and the corresponding quality of speech are influenced by the environment. Digital radio enhances the apparent quality of the radio channel through coding and error protection techniques, which hide the destruction of the information in the channel until the received signal strength is almost lost. A further improvement can be made to the radio channel on top of all the coding. The radio channel, as we have seen, is a frequency-selective fading channel, which means the *propagation conditions* are different for each individual radio frequency channel. Whereas channel number 1, for example, experiences problems when a mobile passes a large building, channel number 92 may not suffer any degradation in quality. As some channels degrade, others are improving as a mobile moves around in a cell. To average these conditions over all the base station's available frequencies in a cell, *slow frequency hopping* (SFH) is introduced. It is so called (to distinguish it from *fast frequency hopping)* because the operating frequency is changed only with every TDMA frame. Fast frequency hopping is used in spread spectrum systems and changes the operating frequency of a link many times per symbol, rather than only one time in each frame. The rather slow frequency changes in SFH are in deference to the synthesizers in the mobile station, which are required to alter their operating frequency even more often than once per frame so that they can monitor adjacent cells as well as hop around in the frequency domain. To perform well, a frequency synthesizer must be able to change its frequency, and settle quietly on a new one, within approximately one time slot (577 μs).

Frequency hopping reduces the SNR required for good communications. For a nonhopping link, the minimum required ratio is 11 dB whereas frequency hopping reduces the requirement to only 9 dB, which is an additional increase of 2 dB of margin in the channel . The hopping adds frequency diversity to the channel.

Frequency hopping is an option for each individual cell. A base station is not required to support this feature. A mobile, however, has no choice but to switch to a frequency-hopping mode when the base station tells it to; mobiles must support SFH. A mobile station has much less RF power to flood a channel with than a base station does; it has only a small antenna, is roughly handled, and is carried around to locations far from optimum for propagation conditions, such as parking structures.

The mobile needs to add frequency diversity to its transmissions as it moves toward the edge of a cell or as it enters an area of high interference, or at any other time the channel becomes marginal. When the BSC observes the failing channel from the mobile and decides to tell the mobile to turn on frequency hopping, it simply assigns the mobile a full set of RF channels rather than a single RF channel. The mobile performs a "dance" on the assigned set of frequencies to satisfy its SFH obligations. Different *hopping algorithms* can be assigned to the mobile station with the channel set. One is *cyclic hopping, in* which hopping is performed through the assigned frequency list from the first frequency, the second frequency, the third, and so on until the list is repeated. The other general algorithm is (pseudo) *random hopping,* in which hopping is performed in a random way through the frequency list. There are 63 different random dances that can be assigned to the mobile. When the mobile station has to assume SFH operation, it is advised of the channel assignment (a set of channels), and which one of the hopping algorithms it should use with an appropriate *frequency-hopping sequence number* (HSN). The base channel is not allowed to hop. The base channel, confined to time slot number 0—carrying the FCCH, the SCH and the BCCH—is the beacon upon which mobiles perform their periodic signal strength measurements on neighboring cells, and it is also the signal the mobile station uses to synchronize with a system as it initially seeks service or gets ready to move to another cell. The FCCH, SCH, BCCH exist only on the base channel on time slot 0, and all the other time slots on the base channel's frequency are filled with some kind of data to bring the base channel's power above all the other channels in the cell. A hopping traffic channel, however, can use time slot 0 on any BTS frequency channel not reserved for the base channel.

There are also two different implementations for frequency hopping in base stations. One of the implementations is *baseband hopping,* which is used if a base station has several transceivers available. The data flow is simply routed in the baseband to various transceivers, each of which operates on a fixed frequency in accordance with the assigned hopping sequence. The different transceivers receive a specific individual time slot in each TDMA frame, which contains information destined for different mobile stations (see Figure 3.7).

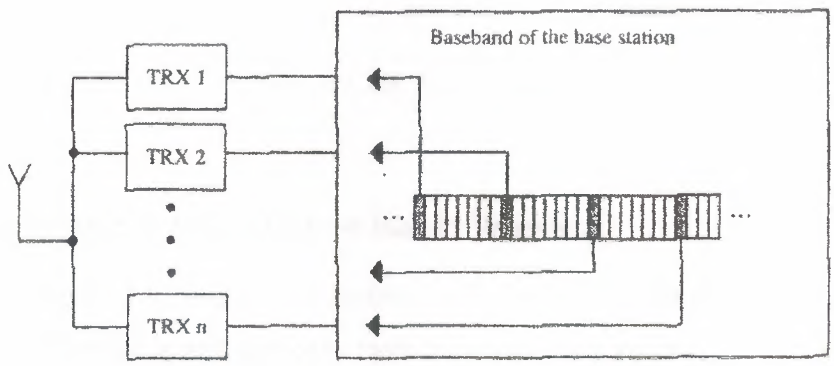


Figure 3.7, Implementing Frequency Hopping

The other implementation is *synthesizer hopping.* One can find base stations in remote areas fitted with only one or two transceivers, but still want to use SFH (e.g., in hilly terrain). In this unusual case, the hopping is performed on the RF transceiver, which requires the transceiver to hop on the different frequencies itself.

Figure 3.8 shows the timing conditions for a mobile station during frequency hopping. It is SFH applied on three different frequencies. Since the mobile station first receives a message from the base station and then responds back to the base station three time slots later, there are four time slots of time during which the mobile station can accomplish different tasks, such as *monitoring adjacent cells,* before it has to hop to the next frequency, on which it will find the base station.

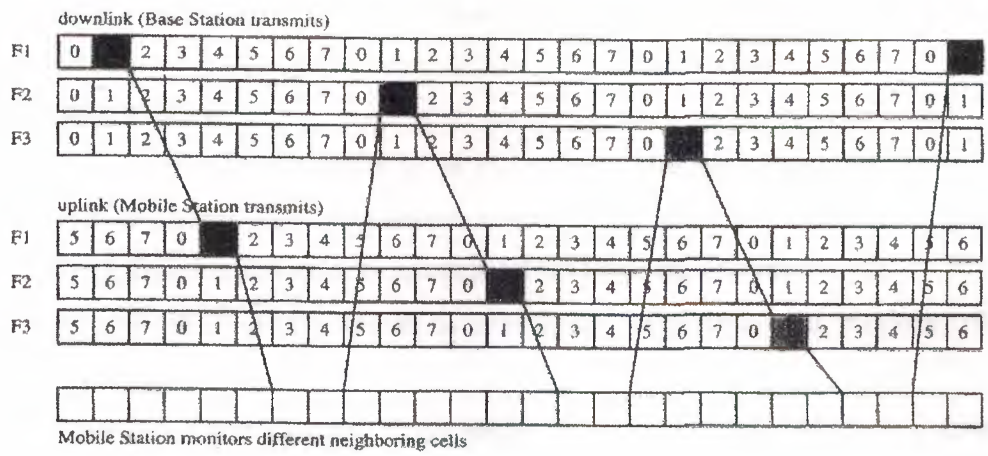


Figure 3.8, SFH Timing

3.6 From Source Information to Radio Waves

The figure 3.9 presents the different operations that have to be performed in order to pass from the speech source to radio waves and vice versa.

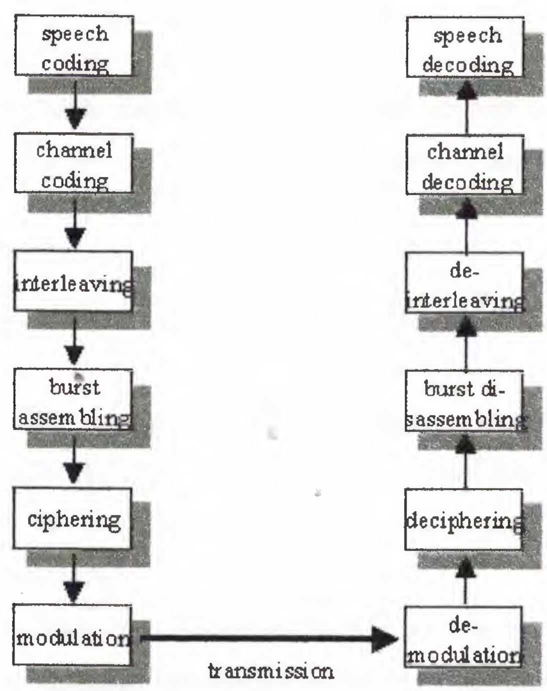


Figure 3.9, From Speech Source to radio Waves

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

3.6.1 Speech Coding

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

- A good speech quality, at least as good as the one obtained with previous cellular systems.
- To reduce the redundancy in the sounds of the voice. This reduction is essential due to the limited capacity of transmission of a radio channel.
- The speech codec must not be very complex because complexity is equivalent to high costs.

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

3.6.2 Channel coding

Channel coding adds redundancy bits to the original information in order to detect and correct, if possible, errors occurred during the transmission.

(a) Channel coding for the GSM data TCH channels

The channel coding is performed using two codes: a block code and a convolutional code.

The block code corresponds to the block code defined in the GSM Recommendations 05.03. The block code receives an input block of 240 bits and adds four zero tail bits at the end of the input block. The output of the block code is consequently a block of 244 bits.

A convolutional code adds redundancy bits in order to protect the information. A convolutional encoder contains memory. This property differentiates a convolutional code from a block code. A convolutional code can be defined by three variables : n, k and K. The value n corresponds to the number of bits at the output of the encoder, k to the number of bits at the input of the block and K to the memory of the encoder. The ratio, R, of the code is defined as follows: R = k/n. Let's consider a convolutional code with the following values: k is equal to 1, n to 2 and K to 5. This convolutional code uses then a rate of R = 1/2 and a delay of K = 5, which means that it will add a redundant bit for each input bit. The convolutional code uses 5 consecutive bits in order to compute the redundancy bit. As the convolutional code is a 1/2 rate convolutional code, a block of 488 bits is generated. These 488 bits are punctured in order to produce a block of 456 bits. Thirty two bits, obtained as follows, are not transmitted:

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

The block of 456 bits produced by the convolutional code is then passed to the interleave.

(b) Channel coding for the GSM speech channels

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

(c) Channel coding for the GSM control channels

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

3.6.3 Interleaving

An interleaving rearranges a group of bits in a particular way. It is used in combination with FEC codes in order to improve the performance of the error correction mechanisms. The interleaving decreases the possibility of losing whole bursts during the transmission, by dispersing the errors. Being the errors less concentrated, it is then easier to correct them.

(a) Interleaving for the GSM control channels

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

(b) Interleaving for the GSM Speech Channels

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

(c) Interleaving for the GSM data TCH channels

A particular interleaving scheme, with an interleaving depth equal to 22, is applied to the block of 456 bits obtained after the channel coding. The block is divided into 16 blocks of 24 bits each, 2 blocks of 18 bits each, 2 blocks of 12 bits each and 2 blocks of 6 bits each. It is spread over 22 bursts in the following way :

- The first and the twenty-second bursts carry one block of 6 bits each
- The second and the twenty-first bursts carry one block of 12 bits each
- The third and the twentieth bursts carry one block of 18 bits each
- From the fourth to the nineteenth burst, a block of 24 bits is placed in each burst

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

3.6.4 Ciphering

Ciphering is used to protect signaling and user data. First of all, a ciphering key is computed using the algorithm A8 stored on the SIM card, the subscriber key and a random number delivered by the network (this random number is the same as the one used for the authentication procedure). Secondly, a 114 bit sequence is produced using the ciphering key, an algorithm called A5 and the burst numbers. This bit sequence is then XORed with the two 57 bit blocks of data included in a normal burst.

The ciphering algorithm is a pure *XORing of* the coded Layer 1 data with a key. In the receiver, we XOR the ciphered data with the same key to get the clear Layer 1 data back again. A special key (ciphering sequence) is used together with the burst numbers, which the radio has full knowledge of thanks to the counters Tl, T2, and T3. The data appear on the Um interface as a nearly random bit sequence. It is impossible for anybody to decode the data without lots of information, most of which never appears on the radio channel. Table 3.1 shows the principle of ciphering as it applies the XOR function to the data on either end of the radio channel.

Table 3.1, Principle of Ciphering

Plain Data	01110010100011100101...
Ciphering Sequence	00011010101000110110...
XORed	
Ciphered Data (transmitted)	01101000001011010011...
Ciphering Sequence	00011010101000110110...
XORed	
Recovered Data	01110010100011100101...

3.6.5 Modulation

The modulation chosen for the GSM system is the Gaussian Modulation Shift Keying (GMSK), with *BT*= 0.3 and rate 270 5/6 kbauds. . GMSK is a type of constant-envelope FSK, where the frequency modulation is a result of a carefully contrived phase modulation. The most important feature of GMSK is that it is a constant-envelope variety of modulation. This means there is a distinct lack of AM in the carrier with a consequent limiting of the occupied bandwidth. The constant amplitude of the GMSK signal makes it suitable for use high-frequency amplifiers

There are as many ways to generate a GMAK signal, as there are Engineers to build modulators. The example in Figure 3.10 illustrates a method employing a quadrature process.

Any modulated carrier, even our GMSK carrier G (t) can be expressed with relation to time as:

$$G(t) = a(t)\cos(\omega_0 t + \theta(t))$$

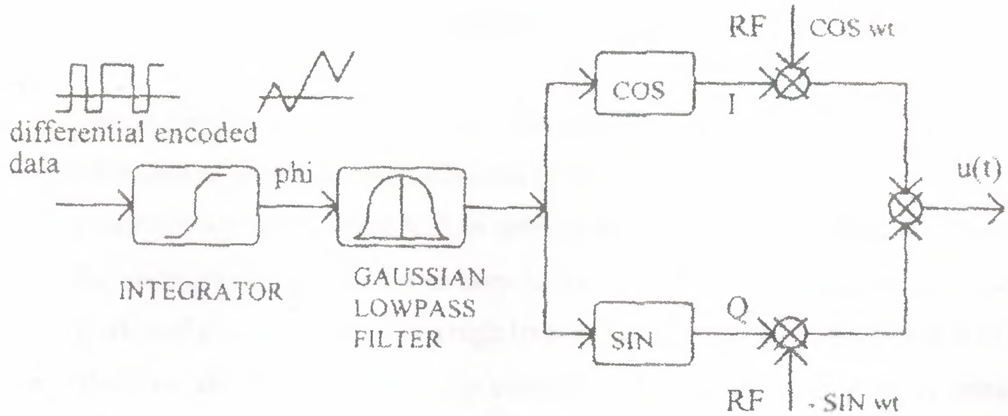


Figure 3.10, GMSK modulator

Where ω_0 *(t) is* the carrier frequency, θ *{t}* is the phase, and *a(t)* is the amplitude. GSM dictates that ω_0 *(t)* is decided by the network at handoff time and is the FDMA aspect of GSM. The power *a(t)* is controlled to prevent cochannel and adjacent-channel interference. In the base station, *a{t)* is constant until adjusted by the network. In the mobile, *a(t)* varies so that the mobile's RF output ramps up to a network-decided level during each time slot assigned to the mobile. All that remains for the modulation is θ *(t)*, which we can control to give the disciplined and gentle frequency shifts we need. We can consider the GMSK modulator as a type of OQPSK modulator, where we have not two bits per symbol, but less than one-half bit per symbol. We use phase transitions to cause frequency transitions, and we spread the phase transitions out to almost three bit times (Gaussian filter).

3.6.6 Discontinuous Transmission (DTX)

As mentioned earlier, another requested feature of the speech transcoder is the detection of pauses in speech. When a pause is detected, we discontinue or suspend radio transmissions for the duration of the pause. The use of this feature is a network option. The DTX option tends to reduce interference in adjacent cells and to mobile stations close to the base site. Since transmit time is further reduced when DTX is used, the power consumption of hand-held terminals is reduced, which gives users the option of fitting their terminals with smaller batteries. Pauses in normal speech occur at a rate that makes speech appear to have about a 50% duty cycle. This means that a telephony channel is only used for speech transmission about half the **time a** speaker is using the phone.

The possibility of invoking DTX functions have extended the original speech codec specifications to include two additional features:

- *Voice activity detection* (VAD) to determine the presence or absence of speech at the microphone. This is not as easy to implement as it may sound, for it has to work well even when there is a high level of background noise, such as in a car.
- The total absence of sound in the earpiece would annoy the user at the receiving end of a radio channel; the handset appears to be dead, and users tend to speak too loudly when there is total silence in the earpiece. There needs to be a minimum of conventional background noise present during pauses, and this minimal background noise is sometimes descriptively called *presence.* This is accomplished by transmitting *silence descriptor* (SID) frames at a rather slow rate of once every 480 ms. Upon receiving the SID frame, the receiving speech decoder has to fake an existing wire-line connection by generating some back-ground noise. The noise is called *comfort noise,* and comfort noise gives the system "presence."

As an aid, Fig 3.11 shows the logical blocks involved in the encoding, transmission, and the decoding of speech in GSM.

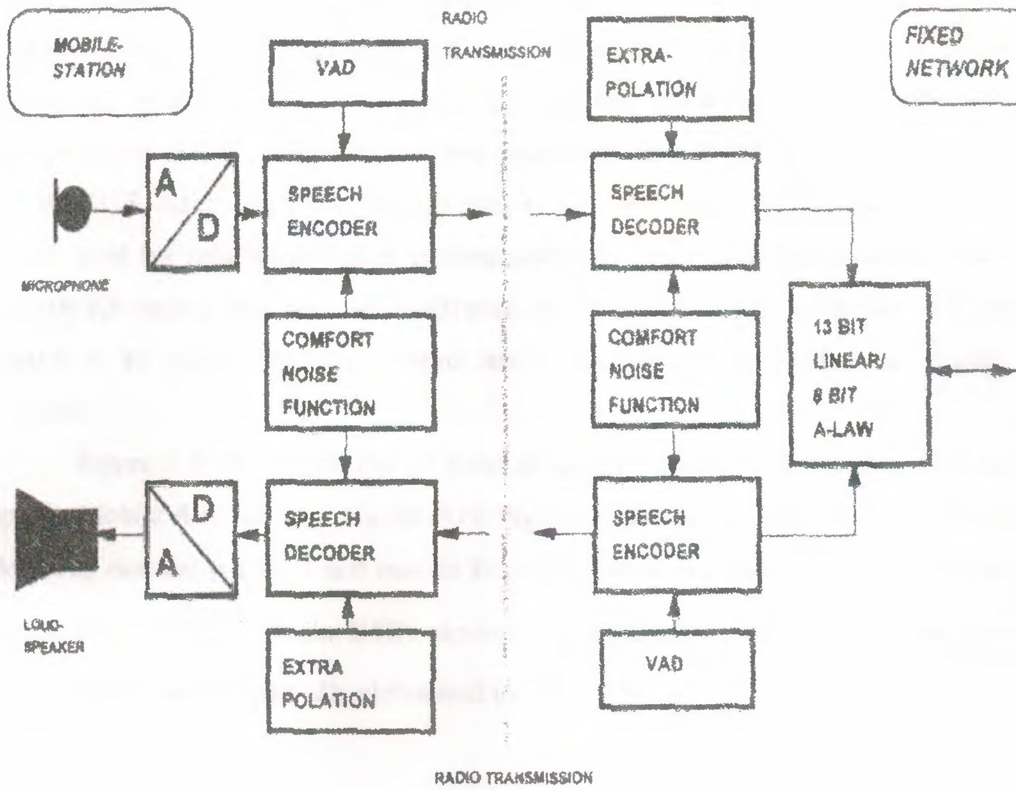


Figure 3.11, Speech Processing Function Used in GSM

3.6.7 Timing Advance and Power Control

Within a single cell, mobile stations can be found at different distances from the base station. Depending on the distance to the base station, the *delay time* and the attenuation of an individual mobile's signal is likely to be different from the delay and attenuation of any of the other mobile stations. It should be apparent by now that TDMA techniques rely heavily on the proper timing of the transmissions of bursts, as well as the correct reception of the bursts at the base station's receiver. To avoid the collision or interleaving of the signals from mobiles assigned to adjacent time slots, the base station performs measurements on the timing delay of each mobile station, and commands those mobiles with bursts arriving too late at the base site to advance their burst transmissions in time; late mobiles (mobiles farthest from the base station) are given a head start. This feature is called *timing advance.*

To compensate for the attenuation over different distances within the cell, the base station, at the same time it is making timing adjustments on mobiles, commands the mobiles to use different power levels in such a way that the power arriving at the base station's receiver is approximately the same for each time slot. The *power control* is performed in steps of 2 dB. This means that a mobile station more distant from the base site has to transmit at a higher power level than those close to the base site.

. If the BTS discovers that a mobile station does not receive its signal at a sufficient power level for reliable downlink communications, it may also apply power control on its own RF output and transmit at different power levels in each time slot. BTS power control is an option for base stations and is not yet implemented in all brands and systems.

Figure 3.12 illustrates the problem of timing advance and power control on the uplink. Mobile A is farther from the BTS than mobile B is. Mobile A is assigned to time slot (TS) number n (TS_n) and mobile B is assigned to the time slot following the one assigned to A (TS_{n+1}). At the BTS's receiver, A's burst arrives with a lower level than B's burst, and A's burst is partially obliterated by B's burst.

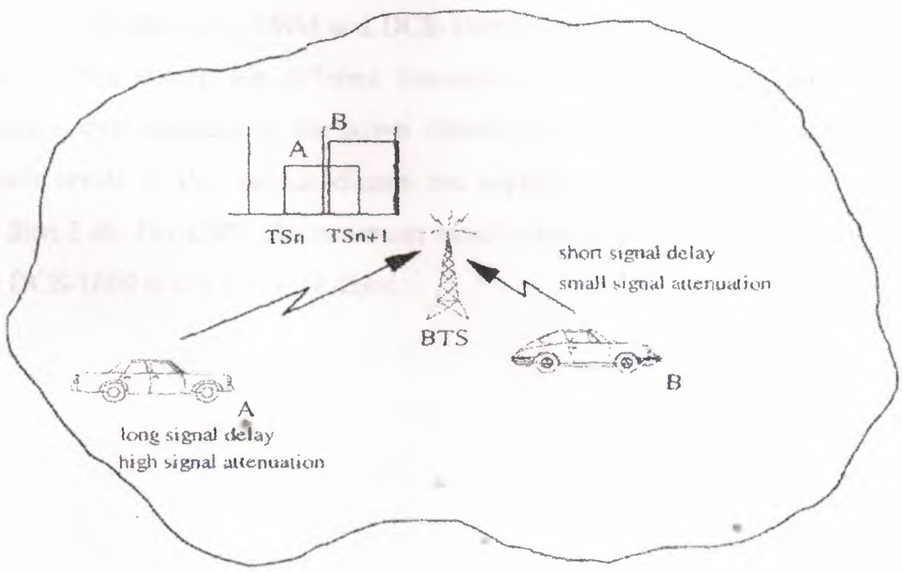


Figure 3.12, Timing Advance and Power Control

3.6.8 Discontinuous Reception

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

3.6.9 Multipath and Equalization

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

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

3.7 Radio Frequency Power Level

Radio equipment in GSM and DCS-1800/1900 are distinguished from each other by, among other things, the different transmitter power levels they can produce. The equipment is thus classified by the power classes shown in table 3.2 through 3.4. Each of the power levels in the various classes are separated from each other by something greater then 2 db. For GSM, the minimum mobile station power level is 20 mW 13 dbm), and for DCS-1800 it is 2.5 mW (4 dbm).

Table 3.2, power level in GSM System

Power Class	Maximum Power of a Mobile Station / (dbm)	Maximum Power of a Base Station / (dbm)
1	20W(43)	320W(55)
2	8w(39)	160W(52)
3	5W(37)	80W(49)
4	2W(33)	40W(46)
5	0.8(29)	20W(43)
6		10W(40)
7		5W(37)
8		2.5W(34)

In the next-generation GSM, which is called *phase 2,* additional decreased power levels are introduced. There are also some new microcell applications that call for some micro-BTS power levels. The reduced BTS power levels are shown in table 3.4.

Table 3.3, Power Level in the DCS-1800/1900 and *Phase 2* Systems

Power Class	Max. Power of a DCS-1800 MS (dbm)	Max. Power of a DCS-1900 MS (dbm)	Max. Power of a DCS-1800 BTS (dbm)	Max. Power of a DCS-1900 BTS (dbm)
1	1W(30)	1W(30)	20W(43)	20-40W(43-46)
2	0.25W(24)	0.24W(24)	10W(40)	10-20W(40-43)
3		2W(33)	5W(37)	5-10W(37-40)
4			2.5W(34)	2.5-5W(34-37)

Table 3.4, Power levels of Micro-BTS in the GSM and DCS-1800/1900 Systems

Power Class	Max. Power of a GSM Micro-BTS (dbm)	Max. Power of a DCS-1800 Micro-BTS (dbm)	Power of DCS-1900 Micro-BTS (dbm)
M1	0.25W(24)	16W(32)	0.5-1.6W(27-32)
M2	0.08W(19)	0.5W(27)	0.16-0.5W(22-27)
M3	0.03W(14)	0.16W(22)	0.05-0.16W(17-22)

CONCLUSION

In this project I have tried to give an overview of the GSM system emphasizing on Cell Planning and the Radio Interface. It's a big topic and there are many details missing but I believe, however, that I gave the general flavor of GSM and the philosophy behind its design. 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.

REFERENCES

[1] John Scourias, University of Waterloo, " A Brief Overview of GSM", http://kbs.cs.tu-berlin.de/~jutta/gsm/js-intro.html

[2] Mouly and B.Pautet, *"The GSM System Of Mobile Communication"*, 1989

[3] Twingler, *"The GSM standard in the present and in the future"* 1996

[4] Watson. C., *"Radio Equipment for GSM"* 1992

[5] Wiggert, D., *" Codes for Error and Control and synchronizatioin"*1998

[6] Lycksell, E., *"GSM system Overview"*, Swedish Telecom Radio Internal Report" 1992

[7] Forney, G. D. JR. *" The Viterbi Algorithm"* Proc. Of the IEEE. 2000