An overview of the GSM system

Javier Gozálvez Sempere

Research Engineer in Mobile Communications
Communications Division
Department of Electronic&Electrical Engineering
University of Strathclyde
Glasgow, Scotland

j.gozalvez@ieee.org

To be aware of the latest developments in Mobile Communications, Transportation Systems and Automotive Electronics, join the
IEEE Vehicular Technology Society

Table of Contents

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

1 History of the cellular mobile radio and GSM

The idea of cell-based mobile radio systems appeared at Bell Laboratories (in USA) in the early 1970s. However, mobile cellular systems were not introduced for commercial use until the 1980s. During the early 1980s, analog cellular telephone systems experienced a very rapid growth in Europe, particularly in Scandinavia and the United Kingdom. Today cellular systems still represent one of the fastest growing telecommunications systems.

But in the beginnings of cellular systems, each country developed its own system, which was an undesirable situation for the following reasons:

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

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

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

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

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

The most important events in the development of the GSM system are presented in the table 1.

Year	Events
1982	CEPT establishes a GSM group in order to develop the standards for a pan-European cellular mobile system
1985	Adoption of a list of recommendations to be generated by the group
1986	Field tests were performed in order to test the different radio techniques proposed for the air interface
1987	TDMA is chosen as access method (in fact, it will be used with FDMA) Initial Memorandum of Understanding (MoU) signed by telecommunication operators (representing 12 countries)
1988	Validation of the GSM system
1989	The responsability of the GSM specifications is passed to the ETSI
1990	Appearance of the phase 1 of the GSM specifications
1991	Commercial launch of the GSM service
1992	Enlargement of the countries that signed the GSM- MoU> Coverage of larger cities/airports
1993	Coverage of main roads GSM services start outside Europe
1995	Phase 2 of the GSM specifications Coverage of rural areas

Table 1: Events in the development of GSM

From the evolution of GSM, it is clear that GSM is not anymore only a European standard. GSM networks are operationnal or planned in over 80 countries around the world. The rapid and increasing acceptance of the GSM system is illustrated with the following figures:

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

Since the appearance of GSM, other digital mobile systems have been developed. The table 2 charts the different mobile cellular systems developed since the commercial launch of cellular systems.

Year	Mobile Cellular System
1981	Nordic Mobile Telephony (NMT), 450>
1983	American Mobile Phone System (AMPS)
1985	Total Access Communication System (TACS) Radiocom 2000 C-Netz
1986	Nordic Mobile Telephony (NMT), 900>
1991	Global System for Mobile communications> North American Digital Cellular (NADC)
1992	Digital Cellular System (DCS) 1800
1994	Personal Digital Cellular (PDC) or Japanese Digital Cellular (JDC)
1995	Personal Communications Systems (PCS) 1900- Canada>
1996	PCS-United States of America>

Table 2: Mobile cellular systems

2 Cellular systems

2.1 The cellular structure

In a cellular system, the covering area of an operator is divided into cells. A cell corresponds to the covering area of one transmitter or a small collection of transmitters. The size of a cell is determined by the transmitter's power.

The concept of cellular systems is the use of low power transmitters in order to enable the efficient reuse of the frequencies. In fact, if the transmitters used are very powerful, the frequencies can not be reused for hundred of kilometers as they are limited to the covering area of the transmitter.

The frequency band allocated to a cellular mobile radio system is distributed over a group of cells and this distribution is repeated in all the covering area of an operator. The whole number of radio channels available can then be used in each group of cells that form the covering area of an operator. Frequencies used in a cell will be reused several cells away. The distance between the cells using the same frequency must be sufficient to avoid interference. The frequency reuse will increase considerably the capacity in number of users.

In order to work properly, a cellular system must verify the following two main conditions:

- The power level of a transmitter within a single cell must be limited in order to reduce the interference with the transmitters of neighboring cells. The interference will not produce any damage to the system if a distance of about 2.5 to 3 times the diameter of a cell is reserved between transmitters. The receiver filters must also be very performant.
- Neighboring cells can not share the same channels. In order to reduce the interference, the frequencies must be reused only within a certain pattern.

In order to exchange the information needed to maintain the communication links within the cellular network, several radio channels are reserved for the signaling information.

2.2 Cluster

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

2.3 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

2.3.1 Macrocells

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

2.3.2 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 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.

2.3.3 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 a coverage of 360 degrees is not needed. In this case, a selective cell with a coverage of 120 degrees is used.

2.3.4 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.

3 The transition from analog to digital technology

In the 1980s most mobile cellular systems were based on analog systems. The GSM system can be considered as the first digital cellular system. The different reasons that explain this transition from analog to digital technology are presented in this section.

3.1 The capacity of the system

As it is explained in section 1, cellular systems have experienced a very important growth. Analog systems were not able to cope with this increasing demand. In order to overcome this problem, new frequency bands and new technologies were proposed. But the possibility of using new frequency bands was rejected by a big number of countries because of the restricted spectrum (even if later on, other frequency bands have been allocated for the development of mobile cellular radio). The new analog technologies proposed were able to overcome the problem to a certain degree but the costs were too important.

The digital radio was, therefore, the best option (but not the perfect one) to handle the capacity needs in a cost-efficiency way.

3.2 Compatibility with other systems such as ISDN

The decision of adopting a digital technology for GSM was made in the course of developing the standard. During the development of GSM, the telecommunications industry converted to digital methods. The ISDN network is an example of this evolution. In order to make GSM compatible with the services offered by ISDN, it was decide that the digital technology was the best option.

Additionally, a digital system allows, easily than an analog one, the implementation of future improvements and the change of its own characteristics.

3.3 Aspects of quality

The quality of the service can be considerably improved using a digital technology rather than an analog one. In fact, analog systems pass the physical disturbances in radio transmission (such as fades, multipath reception, spurious signals or interferences) to the receiver. These disturbances decrease the quality of the communication because they produce effects such as fadeouts, crosstalks, hisses, etc. On the other hand, digital systems avoid these effects transforming the signal into bits. This transformation combined with other techniques, such as digital coding, improve the quality of the transmission. The improvement of digital systems comparing to analog systems is more noticeable under difficult reception conditions than under good reception conditions.

4 The GSM network

4.1 Architecture of the GSM network

The GSM technical specifications define the different entities that form the GSM network by defining their functions and interface requirements.

The GSM network can be divided into four main parts:

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

The architecture of the GSM network is presented in figure 1.

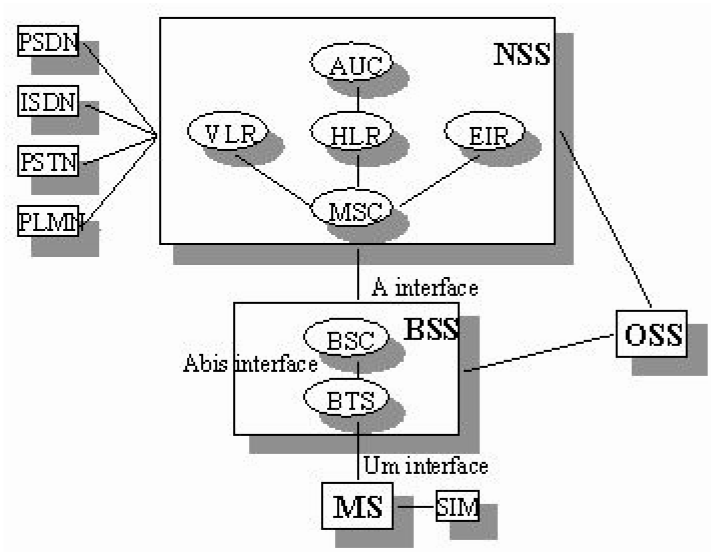

figure 1: Architecture of the GSM network

4.1.1 <u>Mobile Station</u>

A Mobile Station consists of two main elements:

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

4.1.1.1 <u>The Terminal</u>

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 handhels 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 to decrease the maximum allowed power to 0.8 W.

4.1.1.2 <u>The SIM</u>

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.

4.1.2 <u>The Base Station Subsystem</u>

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).

4.1.2.1 <u>The Base Transceiver Station</u>

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.

4.1.2.2 <u>The Base Station Controller</u>

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

4.1.3 <u>The Network and Switching Subsystem</u>

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.

4.1.3.1 <u>The Mobile services Switching Center (MSC)</u>

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

4.1.3.2 <u>The Gateway Mobile services Switching Center</u> <u>(GMSC)</u>

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.

4.1.3.3 <u>Home Location Register (HLR)</u>

The HLR is considered as a very important database that stores information of the suscribers 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.

4.1.3.4 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.

4.1.3.5 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.

4.1.3.6 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).

4.1.3.7 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.

4.1.4 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.

4.2 The geographical areas of the GSM network

The figure 2 presents the different areas that form a GSM network.

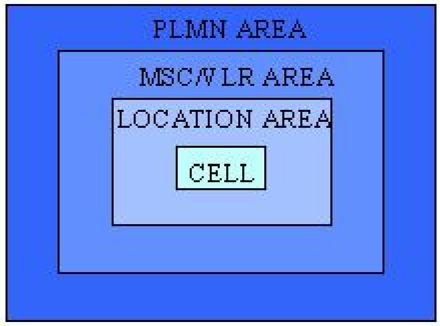

figure 2: GSM network areas

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

4.3 The GSM functions

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

- Transmission.
- Radio Resources management (RR).
- Mobility Management (MM).
- Communication Management (CM).
- Operation, Administration and Maintenance (OAM).

4.3.1 Transmission

The transmission function includes two sub-functions:

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

Not all the components of the GSM network are strongly related with the transmission functions. The MS, the BTS and the BSC, among others, are deeply concerned with transmission. But other components, such as the registers HLR, VLR or EIR, are only concerned with the transmission for their signaling needs with other components of the GSM network. Some of the most important aspects of the transmission are described in section 5.

4.3.2 Radio Resources management (RR)

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

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

- Channel assignment, change and release.
- Handover.
- Frequency hopping.
- Power-level control.
- Discontinuous transmission and reception.
- Timing advance.

Some of these procedures are described in section 5. In this paragraph only the handover, which represents one of the most important responsabilities of the RR, is described.

4.3.2.1 Handover

The user movements can produce the need to change the channel or cell, specially when the quality of the communication is decreasing. This procedure of changing the resources is called handover. Four different types of handovers can be distinguished:

- Handover of channels in the same cell.
- Handover of cells controlled by the same BSC.
- Handover of cells belonging to the same MSC but controlled by different BSCs.
- Handover of cells controlled by different MSCs.

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

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

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

4.3.3 Mobility Management

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

4.3.3.1 Location management

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

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

A location updating is also performed periodically. If after the updating time period, the mobile station has not registered, it is then deregistered.

When a mobile station is powered off, it performs an IMSI detach procedure in order to tell the network that it is no longer connected.

4.3.3.2 Authentication and security

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

Another security procedure is to check the equipment identity. If the IMEI number of the mobile is authorized in the EIR, the mobile station is allowed to connect the network.

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

Enciphering is another option to guarantee a very strong security but this procedure is going to be described in section 5.

4.3.4 Communication Management (CM)

The CM function is responsible for:

- Call control.
- Supplementary Services management.
- Short Message Services management.

4.3.4.1 Call Control (CC)

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

- a country code

- a national destination code identifying the subscriber's operator
- a code corresponding to the subscriber's HLR

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

4.3.4.2 Supplementary Services management

The mobile station and the HLR are the only components of the GSM network involved with this function. The different Supplementary Services (SS) to which the users have access are presented in section 6.3.

4.3.4.3 Short Message Services management

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

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

4.3.5 Operation, Administration and Maintenance (OAM)

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

- The components of the BSS and NSS provide the operator with all the information it needs. This information is then passed to the OSS which is in charge of analize it and control the network.
- The self test tasks, usually incorporated in the components of the BSS and NSS, also contribute to the OAM functions.
- The BSC, in charge of controlling several BTSs, is another example of an OAM function performed outside the OSS.

5 The GSM radio interface

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 eficiency 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.

5.1 Frequency allocation

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

- The band 890-915 Mhz has been allocated for the uplink direction (transmitting from the mobile station to the base station).
- The band 935-960 Mhz 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 Mhz frequency bands.

5.2 Multiple access scheme

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

5.2.1 FDMA and TDMA

Using FDMA, a frequency is assigned to a user. So the larger the number of users in a FDMA system, the larger the number of available frequencies must be. The limited available radio spectrum and the fact that a user will not free its assigned frequency until he does not need it anymore, explain why the number of users in a FDMA system can be "quickly" limited.

On the other hand, TDMA allows several users to share the same channel. Each of the users, sharing the common channel, are assigned their own burst within a group of bursts called a frame. Usually TDMA is used with a FDMA structure.

In GSM, a 25 Mhz frequency band is divided, using a FDMA scheme, into 124 carrier frequencies spaced one from each other by a 200 khz frequency band. Normally a 25 Mhz frequency band can provide 125 carrier frequencies but the first carrier frequency is used as a guard band between GSM and other services working on lower frequencies. Each carrier frequency is then divided in time using a TDMA scheme. This scheme splits the radio channel, with a width of 200 khz, into 8 bursts. A burst is the unit of time in a TDMA system, and it lasts approximately 0.577 ms. A TDMA frame is formed with 8 bursts and lasts, consequently, 4.615 ms. Each of the eight bursts, that form a TDMA frame, are then assigned to a single user.

5.2.2 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.

5.2.2.1 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.

5.2.2.2 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.

5.2.2.2.1 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

5.2.2.2.2 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). It is used, by the base station, to inform the mobile station about which channel it should use. This channel is the answer of a base station to a RACH from the mobile station

5.2.2.2.3 <u>Dedicated Control Channels (DCCH)</u>

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.

5.2.2.2.4 <u>Associated Control Channels</u>

The Fast Associated Control Channels (FACCH) replace 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.

5.2.3 <u>Burst structure</u>

As it has been stated before, the burst is the unit in time of a TDMA system. Four different types of bursts can be distinguished in GSM:

- The frequency-correction burst is used on the FCCH. It has the same length as the normal burst but a different structure.
- The synchronization burst is used on the SCH. It has the same length as the normal burst but a different structure.
- The random access burst is used on the RACH and is shorter than the normal burst.
- The normal burst is used to carry speech or data information. It lasts approximately 0.577 ms and has a length of 156.25 bits. Its structure is presented in figure 3.

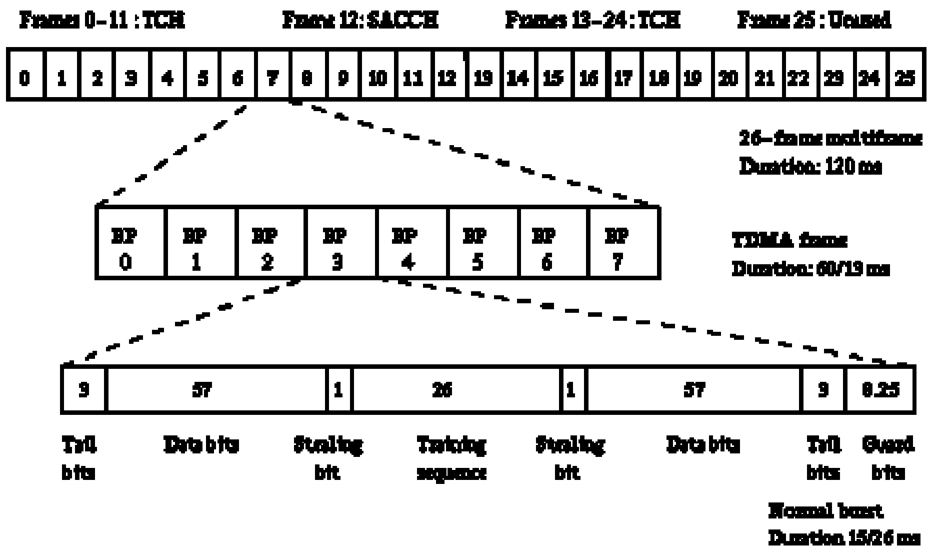

figure 3: Structure of the 26-Multiframe, the TDMA frame and the normal burst*

**This figure has been taken, with the corresponding authorization, from "An Overview of GSM" by John Scourias (see Other GSM sites)*

The tail bits (T) are a group of three bits set to zero and placed at the beginning and the end of a burst. They are used to cover the periods of ramping up and down of the mobile's power.

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

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

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

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

5.2.4 Frequency hopping

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

There are different types of frequency hopping algorithms. The algorithm selected is sent through the Broadcast Control Channels.

Even if frequency hopping can be very useful for the system, a base station does not have to support it necessarily On the other hand, a mobile station has to accept frequency hopping when a base station decides to use it.

5.3 From source information to radio waves

The figure 4 presents the different operations that have to be performed in order to pass from the speech source to radio waves and vice versa.

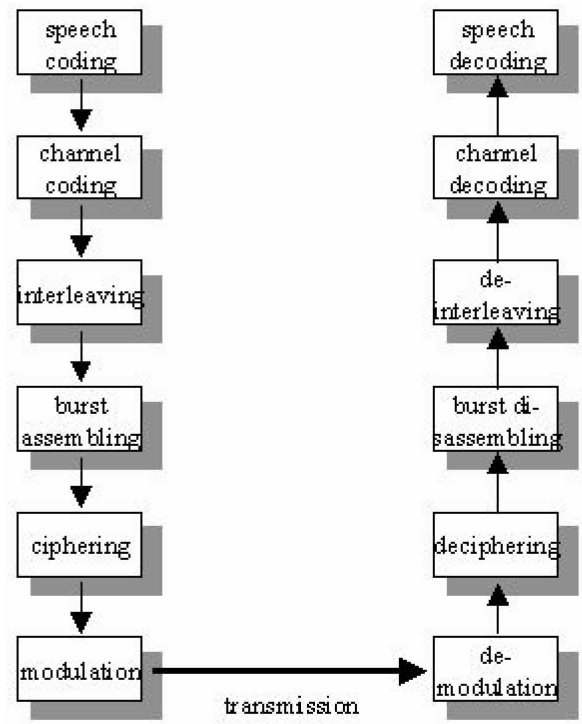

figure 4: From speech source to radio waves

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

5.3.1 <u>Speech coding</u>

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.

5.3.2 <u>Channel coding</u>

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

5.3.2.1 <u>Channel coding for the GSM data TCH channels</u>

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 :

$C(11 + 15j)$ for $j = 0, 1, ..., 31$

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

5.3.2.2 <u>Channel coding for the GSM speech channels</u>

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 Ib 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.

5.3.2.3 <u>Channel coding for the GSM control channels</u>

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.

5.3.3 <u>Interleaving</u>

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.

5.3.3.1 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 interleaver for control channels is called a block rectangular interleaver.

5.3.3.2 Interleaving for the GSM speech channels

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

5.3.3.3 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.

5.3.4 Burst assembling

The busrt assembling procedure is in charge of grouping the bits into bursts. Section 5.2.3 presents the different bursts structures and describes in detail the structure of the normal burst.

5.3.5 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.

In order to decipher correctly, the receiver has to use the same algorithm A5 for the deciphering procedure.

5.3.6 Modulation

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

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

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

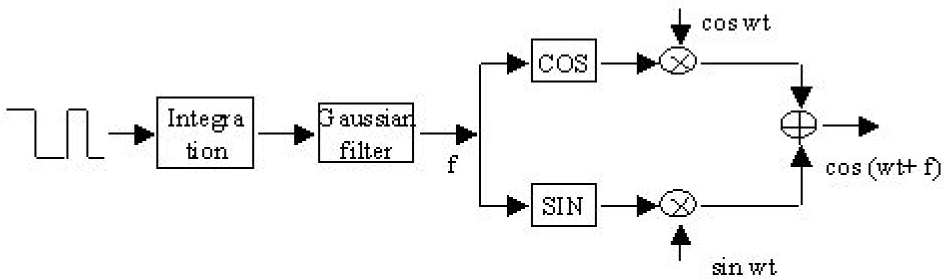

figure 5: GMSK modulator

5.4 Discontinuous transmission (DTX)

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

- The Voice Activity Detection (VAD), which has to determine whether the sound represents speech or noise, even if the background noise is very important. If the voice signal is considered as noise, the transmitter is turned off producing then, an unpleasant effect called clipping.
- The comfort noise. An inconvenient of the DTX function is that when the signal is considered as noise, the transmitter is turned off and therefore, a total silence is heard at the receiver. This can be very annoying to the user at the reception because it seems that the connection is dead. In order to overcome this problem, the receiver creates a minimum of background noise called comfort noise. The comfort noise eliminates the impression that the connection is dead.

5.5 Timing advance

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

5.6 Power control

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

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

5.7 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.

5.8 Multipath and equalisation

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 equaliser 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 equaliser 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.

6 GSM services

It is important to note that all the GSM services were not introduced since the appearance of GSM but they have been introduced in a regular way. The GSM Memorandum of Understanding (MoU) defined four classes for the introduction of the different GSM services:

- E1: introduced at the start of the service.
- E2: introduced at the end of 1991.
- Eh: introduced on availability of half-rate channels.
- A: these services are optional.

Three categories of services can be distinguished:

- Teleservices.
- Bearer services.
- Supplementary Services.

6.1 Teleservices

- Telephony (E1® Eh).

- Facsmile group 3 (E1).

- Emergency calls (E1® Eh).

- Teletex.

- Short Message Services (E1, E2, A). Using these services, a message of a maximum of 160 alphanumeric characters can be sent to or from a mobile station. If the mobile is powered off, the message is stored. With the SMS Cell Broadcast (SMS-CB), a message of a maximum of 93 characters can be broadcast to all mobiles in a certain geographical area.

- Fax mail. Thanks to this service, the subscriber can receive fax messages at any fax machine.

- Voice mail. This service corresponds to an answering machine.

6.2 Bearer services

A bearer service is used for transporting user data. Some of the bearer services are listed below:

- Asynchronous and synchronous data, 300-9600 bps (E1).
- Alternate speech and data, 300-9600 bps (E1).
- Asynchronous PAD (packet-switched, packet assembler/disassembler) access, 300-9600 bps (E1).
- Synchronous dedicated packet data access, 2400-9600 bps (E2).

6.3 Supplementary Services

- Call Forwarding (E1). The subscriber can forward incoming calls to another number if the called mobile is busy (CFB), unreachable (CFNRc) or if there is no reply (CFNRy). Call forwarding can also be applied unconditionally (CFU).

- Call Barring. There are different types of `call barring' services:

- Barring of All Outgoing Calls, BAOC (E1).
- Barring of Outgoing International Calls, BOIC (E1).
- Barring of Outgoing International Calls except those directed toward the Home PLMN Country, BOIC-exHC (E1).
- Barring of All Incoming Calls, BAIC (E1)
- Barring of incoming calls when roaming (A).

- Call hold (E2). Puts an active call on hold.

- Call Waiting, CW (E2). Informs the user, during a conversation, about another incoming call. The user can answer, reject or ignore this incoming call.

- Advice of Charge, AoC (E2). Provides the user with an online charge information.

- Multiparty service (E2). Possibility of establishing a multiparty conversation.

- Closed User Group, CUG (A). It corresponds to a group of users with limited possibilities of calling (only the people of the group and certain numbers).

- Calling Line Identification Presentation, CLIP (A). It supplies the called user with the ISDN of the calling user.

- Calling Line Identification Restriction, CLIR (A). It enables the calling user to restrict the presentation.

- Connected Line identification Presentation, CoLP (A). It supplies the calling user with the directory number he gets if his call is forwarded.

- Connected Line identification Restriction, CoLR (A). It enables the called user to restrict the presentation.

- Operator determined barring (A). Restriction of different services and call types by the operator.

7 Conclusion

The aim of this paper was to give an overview of the GSM system and not to provide a complete and exhaustive guide.

As it is shown in this chapter, GSM is a very complex standard. It can be considered as the first serious attempt to fulfil the requirements for a universal personal communication system. GSM is then used as a basis for the development of the Universal Mobile Telecommunication System (UMTS).

Bibliography

`An introduction to GSM' by Redl, Weber and Oliphant. Published by Artech House. ISBN 0-89006-785-6.

'The GSM System for Mobile communications' by Mouly and Pautet. Published by Cell & Sys. ISBN 2-9507190-0-7.

`Telecommunications Engineering' by J.Dunlop and D.G. Smith. Published by Chapman & Hall. ISBN 0-412-56270-7.

`Modern Personal Radio Systems'. Edited by R.C.V. Macario. The Institution of Electrical Engineers. ISBN 0-85296-861-2.

`Mobile Radio Communications' by Raymond Steele. Pentech Press publishers and IEEE Press. ISBN 0-7803-1102-7.

'Overview of the Global System for Mobile communications' by John Scourias (University of Waterloo). Web document found in: *http://ccnga.uwaterloo.ca/~jscouria/GSM/index.html*

'A brief overview of the GSM radio interface' by Thierry Turletti (Laboratory for Computer Science, Massachussets Institute of Technology).

'An introduction to GSM' from the book 'Cellular Radio Systems', edited by Balston and Macario. Published by Artech House.

'The GSM tutorial'. Web document found in: *http:/www.iec.org*

Acronyms

A3	Authentication algorithm
A5	Ciphering algorithm
A8	Ciphering key computation
AGCH	Access Grant CHannel
AMPS	Advanced Mobile Phone Service
AoC	Advice of Charge
ARQ	Automatic Repeat reQuest mechanism
AUC	Authentication Center
BAIC	Barring of All Incoming Calls
BAOC	Barring of All Outgoing Calls
BOIC	Barring of Outgoing International Calls
BOIC-exHC	Barring of Outgoing International Calls except those directed toward the Home PLMN Country
BCCH	Broadcast Control CHannel
BCH	Broadcast CHannel
BER	Bit Error Rate
bps	bits per second
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Station
CC	Call Control
CCCH	Common Control CHannel
CDMA	Code Division Multiple Access
CEPT	Conference of European Posts and Telecommunications
CFB	Call Forwarding on mobile subscriber Busy
CFNRc	Call Forwarding on mobile subscriber Not Reachable
CFNRy	Call Forwarding on No Reply
CFU	Call Forwarding Unconditional
CGI	Cell Global Identity
C/I	Carrier-to-Interference ratio
C/I	Carrier-to-Interference ratio
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CM	Communication Management
CoLP	Connected Line identification Presentation
CoLR	Connected Line identification Restriction
CUG	Closed User Group

CW	Call Waiting
DCS	Digital Cellular System
DCCH	Dedicated Control CHannel
DTX	Discontinuous transmission
EIR	Equipment Identity Register
ETSI	European Telecommunications Standards Institute
FACCH	Fast Associated Control CHannel
FCCH	Frequency-Correction CHannel
FDMA	Frequency Division Multiple Access
FEC	Forward Error Correction code
FER	Frame Erasure Rate
GIWU	GSM Interworking Unit
GMSC	GSM Mobile services Switching Center
GMSK	Gaussian Minimum Shift Keying
GP	Guard Period
GSM	Global System for Mobile communications
HLR	Home Location Register
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
ISDN	Integrated Services Digital Network
JDC	Japanese Digital Cellular
LA	Location Area
LAI	Location Area Identity
LOS	Line-Of-Sight
MM	Mobility Management
MoU	Memorandum of Understanding
MS	Mobile Station
MSC	Mobile services Switching Center
MSISDN	Mobile Station ISDN number
MSRN	Mobile Station Roaming Number
NADC	North American Digital Cellular
NMT	Nordic Mobile Telephone
NSS	Network and Switching Subsystem
OAM	Operation, Administration and Maintenance
OSS	Operation and Support Subsystem
PAD	Packet Assembler Disassembler
PCH	Paging CHannel
PCS	Personal Communications Services
PDC	Personal Digital Cellular
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PSPDN	Packet Switched Public Data Network
PSTN	Public Switched Telephone Network
RACH	Random Access CHannel

	Radio Frequency
RPE-LTP	Regular Pulse Excitation Long-Term Prediction
RR	Radio Resources management
S	Stealing flags
SACCH	Slow Associated Control CHannel
SCH	Synchronisation CHannel
SDCCH	Standalone Dedicated Control CHannel
SDCCH	Standalone Dedicated Control CHannel
SIM	Subscriber Identity Module
SMS	Short Message Services
SMS-CB	Short Message Services Cell Broadcast
SMS-MO/PP	Short Message Services Mobile Originating/Point-to-Point
SMS-MT/PP	Short Message Services Mobile Terminating/Point-to-Point
SNR	Signal to Noise Ratio
SRES	Signed RESult
SS	Supplementary Services
T	Tail bits
TACS	Total Access Communication System
TCH	Traffic CHannel
TCH/F	Traffic CHannel/Full rate
TCH/H	Traffic CHannel/Half rate
TDMA	Time Division Multiple Access
TMSI	Temporary Mobile Subscriber Identity
UMTS	Universal Mobile Telecommunications System
VAD	Voice Activity Detection
VLR	Visitor Location Register

Other GSM sites

- The Telecoms Virtual Library about mobile communications. You can find information about GSM but also about other mobile commmunications systems. http://www.analysys.com/vlib/

- An overview of the Global System for Mobile Communications by John Scourias http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html

- Very complete page about GSM, By Henrik Kaare Poulsen http://www.geocities.com/henrik.kaare.poulsen/gsm.html

- GSM in Belgium http://www.luc.ac.be/~hbaerten/gsm/

- GSM World, the world wide web site of the GSM MoU Association http://www.gsmworld.com/

- The magazine GSMag International http://www.gsmag.com/

- A list of GSM operators and network codes by country http://kbs.cs.tu-berlin.de/~jutta/gsm/gsm-list.html

- Send messages to GSM Mobile phones
http://www.mtn.co.za/regulars/sms/

- Mobile World
http://www.mobileworld.org/

- ITU Selected Sites-Telecom-Wireless
http://www.itu.int/Sites/wwwfiles/tel_wireless.html

- GSM information network
http://www.gin.nl/

- Radiophone
http://radiophone.dhp.com/

- SMS reference
http://www.virtua.co.uk/sms/sms/index.html

- Ben Wood's GSM reference site
http://ds.dial.pipex.com/benw/

- A complete french web page about GSM (includes an overview of GSM, GSM services, useful information for GSM users, etc...). http://massena.univ-mlv.fr/~turloy/Gsm/frmGSM.html

- Some of the most important manufacturers of cellular phones: Motorola, Ericsson, Nokia and Alcatel

 Go back to my home page

---

The author acknowledges the help of Mr Patrice Kadionik in passing the original tutorial into html format.