NEAR EAST UNIVERSITY
LIBRARY
1988 - LEFKOŞA

# NEAR EAST UNIVERSITY

## Faculty of Engineering

## Department of Electrical and Electronic Engineering

# GSM 1800
# PERSONAL COMMUNICATION NETWORK

## GRADUATION PROJECT

Student Bora Enis Tuğlu(971419)

Supervisor Prof.Dr.
Fakhreddin Mamedov

Lefkoşa-2000

# ACKNOWLEDGMENTS

First of all I would like to thank my family;Father,Mother and Sister for be obliged to educate for me in this school.Because they want take a very good education for my life.

I would like thank our dean Prof.Dr. Khalil Ismailov.

Also I would like to thank my supervisor and our department head Prof.Dr. Fakhreddin Mamedov for help and tolerating me.

I would like to thank for my advisor Özgür Özerdem for encouraging to me and other all teachers.

I would like to thank assistant student Jamal for give good idea and help me through to complete this project.

I would like to acknowledge the especially helpful comments of my friends : Fatih Karadağ ,Recep Kürkçü ,Bahattin Şanlı ,Mehmet Kinsiz ,Gökhan Evran, Erdal Yıldız ,Murat Ünlü,Bahadır Soysal and my home friend M.Fatih Keleş.

Finally;I would like to thank my girl friend Nimet for show understanding me.

*"THANK GOD ! I AM ELECTRİCAL AND*

*ELECTRONİC ENGİNEER NOW"*

BORA ENİS TUGLU

# ABSTRACT

Peoples of fiction have sometimes depicted foure societies in which technology. especially telecommunication technology, has come to have a sinister, rather than a wholly beneficial, significance in people's lives.

Such a view of an intrusive and pervasive information environment, in which individuals are dominated by the technology they themselves have created, makes the concept of personal communications appear more a threat than a promise. However, the transition that is now taking place as personal communications evolves from a specialized minority service to a generally available one, merely marks a natural step in the process of maturity in telecommunications. Of course society, and the individual will want to maintain control over how this technology is used so as to reap its benefits without suffering any negative impact on our lives.

It has always been obvious that telecommunication should preferably be able to follow the user around, but only lately has the required technology (or in truth, the combination of several technologies) developed to the stage where this science-fiction idea can become fact.

This project gathers together views of where personal communications is now and where it is going.

First of all I explain GSM technology at te first two chapter in 1.2. For example Digital Cellular Mobile Radio System,GSM Phases,What is Layer ..etc.

Chapter 1 describes for history and development of the GSM standard ,the services and security offered to the users of a GSM-based network ,and the structuresand architechure of the network

Chapter 2 briefly explains how GSM is embedded in the integrated services digital network (ISDN),describes the ISO/OSI (International Standrds Organization /open systems interconnection )layer model ,and explains how the lower three layers of this model functıon .

I explain the extent to which second generation systems –GSM,DCS 1800,and DECT- are able to support the personal communications requriment.

The requriment for personal communication services arises from the changing enviroment at the end of the 20th century,which is bringing changes in life and work styles in the developed world; we should also not forget the burgeoning recognition of basic communication needs of the third world.Because the emerging technology adresses real human needs ,we can be confident that personal communications will not be just another still born technology or sterile market prospect

INDEX

**CHAPTER 1**

## CHAPTER 2

## CHAPTER 3

## CHAPTER 4

## CHAPTER 5

# LIST OF FIGURE

## CHAPTER 1

## CHAPTER 2

## CHAPTER 3

## CHAPTER 4

## CHAPTER 5

# INTRODUCTION

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

. We include a description of some of the services offered by a GSM public land mobile network (PLMN), and introduce some basic terms and the general architecture of a cellular network. Also introduced are the new terms and the components of a GSM system, and which come from the structure and operation of analog networks, which may already be known to the reader. We focus especially on security features inherent in a GSM network.

A brief note concerning the term GSM is in order now. Since GSM stands for global system for mobile communications, it is redundant to say "GSM system," for this would mean we said "global system for mobile communications system." However, since terms such as GSM system are widely used in the industry, it is common to be redundant when using system abbreviations (e.g., ISDN network), since the redundancy in such terms has some clarifying effect.

A telecommunications system cannot work without a minimum number of signaling functions to organize the interworking of its network entities and the interworking with other networks. Signaling is required to establish, maintain, and terminate connections or communication links. Signaling is necessary to make sure that the provision of services is taking place by the use of defined procedures. Measures have to be taken for all cases of service and system usage and in case of problems or malfunctions. Compared to the means of signaling used in the old, conventional telephone networks (e.g., dial tone, ring-down, dial pulses) and taking into account the higher complexity of a mobile network, which provides uncounted service features, a considerably higher signaling overhead can be expected for a system like GSM. The signaling overhead is great, although transparent (i.e., not obvious to or recognized by the end user).

An analog cellular radio is replaced by second-generation digital systems such as (in Europe) GSM and DCS 1800, the attention of the telecommunications community is turning toward the specification of future mobile communications systems aimed at increasingly personalized services. However, an alternative approach to personal communications is also emerging, termed personal communications services, or PCS. This approach is based a combined strengths of two entities: the existing telephone network (either private public) and a radio access part.

Personal communications is not defined by a specific technology; rather, it is described features a user would wish for from an individual telecommunications service.Although a single definition is not possible, the features sought by most people can be encompassed by a common vision. The objective of a personal communications network(PCN) is to meet this vision as fully as possible and bring the mobile phone to the mass market.

# CHAPTER 1

## GSM-A DIGITAL CELLULAR MOBILE RADIO SYSTEM

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

In this chapter, we confine our focus to GSM. We start with a brief review of its history and then follow with the evolution of the GSM standard and its worldwide adoption. We include a description of some of the services offered by a GSM public land mobile network (PLMN), and introduce some basic terms and the general architecture of a cellular network. Also introduced are the new terms and the components of a GSM system, and which come from the structure and operation of analog networks, which may already be known to the reader. We focus especially on security features inherent in a GSM network.

A brief note concerning the term GSM is in order now. Since GSM stands for global system for mobile communications, it is redundant to say "GSM system," for this would mean we said "global system for mobile communications system." However, since terms such as GSM system are widely used in the industry, it is common to be redundant when using system abbreviations (e.g., ISDN network), since the redundancy in such terms has some clarifying effect. This book will use both the redundant and nonredundant forms with reckless abandon.

### 1.1 DEVELOPMENT AND INTRODUCTION OF THE GSM STANDARD

In Table 1.1, the milestones in the course of establishing the GSM system specifications and the spread of GSM over the globe are listed (1).

When looking only at the adoption of the GSM standard in Europe, it becomes clear that the unification of cellular mobile radio will finally become a reality. Figure 1.1 illustrates this.

Words cannot easily express the tireless efforts expended 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.

With teamwork to an extent never before seen in Europe in the whole industry, in administrations and their national or international institutes, and among operators and manufacturers, a rich and detailed standard for a promising, future-proof mobile communications system has been developed.

The new standard has given new momentum to the economy and has created new markets. A common standard for a market whose customers number in the tens of millions leads to minimized costs for the manufacturers of appropriate equipment. They can produce larger numbers of terminals for a large market, which drives down the cost to end users. Together with deregulation, the provision of cellular service means competition, again to the benefit of end users. Tariffs, products. and services become subject to the higher dynamics imposed by this competition.

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. Other attractive features and services, which have not yet appeared in any cellular network, are waiting in line (see following paragraphs).

The standardization work is not yet finished. It will be continued for years to come. The GSM standard can be regarded as an evolving standard. Today, networks are already operational, but to what extent does the equipment and the provision of cellular services comply with the standard? When it became obvious that the whole standardization process could not be completed before an actual launch of the services-necessary because of economic factors-a phased approach to rolling out the specifications and the networks was adopted. This meant that a subset of network features was to be introduced. The reduced features were initially designed to be upwardly compatible add-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. Now, there is even thought given to features beyond Phase 2. These future implementations are known by the term Phase

2- The networks, which are operational now, feature GSM Phase 1, whose specifications were frozen as early as 1991. GSM Phase 2 specifications and

(Table 1.1)

Development and Spread of the GSM Standard

| | |
|---|---|
| 1982 | CEPT decides to establish a Groupe Specials Mobile (the initial origin of the term GSM) to develop a set of common standards for a future panEuropean cellular mobile network. |
| 1984 | Establishment of three Working Parties (WP1-3) to define and describe the services offered in a GSM PLMN, the radio interface, transmission,signaling protocols, interfaces, and network architecture. |
| 1985 | Discussion and adoption of a list of recommendations to be generated by the group >100 recommendations in a series of 12 volumes). |
| 1986 | A so-called permanent nucleus is established to continuously coordinate the work, which is intensely supported by industry delegates. |
| 1987 | Initial Memorandum of Understanding (MoU) signed by telecommunication network operator organizations (representing 12 countries).<br>Major objectives:<br>• Coordinating the introduction of the standard and time scales<br>• Planning of service introduction<br>• Routing, hilling, and tariff coordination |
| 1988 | Validations and trials (particularly the radio interface) show that GSM will work. |

| | |
|---|---|
| 1988/89<br>to<br>1991/1992 | With the establishment of the european stadandards ınstute (ETSI) the specification work was moved to this ınternational body.GSM becomes a technical committee within ETSI and splits up into GSM groups 1-4 later called special mobile groups (SMG)1-4 which are technical subcommittees. |
| 1990 | The GSM specifications for the 900 MHz band are also applied to a Digital cellular system on the 1,800 MHz band (DCS 1800) ,a PCN application initiated İn the United Kingdom. |
| 1991 | The GSM Recommendations comprise more than 130 single documents including more than 5,000 pages |
| 1991 | july:Planned commercial launch of GSM service in europe delayed to 1992 because of nonavailability of type-approved terminals(GSM then stands for God send mobiles). |
| 1992 | Official commercial launch of GSM service in erope (God Has Sent Mobiles) |
| 1993 | The GSM-MoU has 62 members in 39 countries worldwide.In addition 32 potential members in 19 other countries.(2) |
| 1993 | The end of 1993 shows one million subscribers to GSM networks however more than 80% of them are to be found in Germany alone. |
| 1993 | First commercial services also start outside Europe: Australia,Hong Kong,New Zealand.GSM networks are operational in Denmark,Finland,France,Greece Ireland,Italy,Norway,Portugal,Sweden,United Kingdom |
| 1994 | GSM services can be expected in the following additional countries :Andorra,Austria,Belgium, Brunei,Cameroon,Cyprus,Iran,Netherlands, Pakistan,Spain,Syria,Turkey,Unıted Arab Emirates, and many others. |

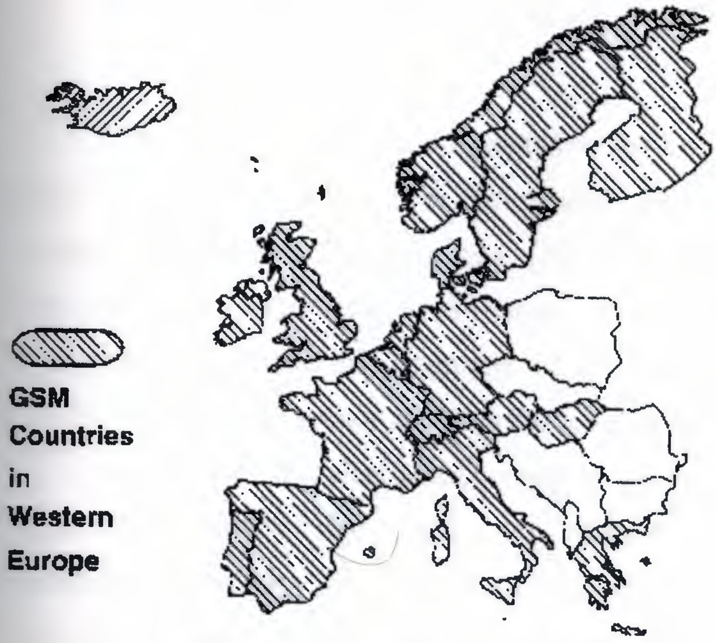


**Figure 1.1**.The GSM standard in Europe.

products should be available in 1994. Phase 2+ addendums are intended to be updated on a regular basis according to market needs and the availability of specifications.

An appropriate comment on this chapter comes from Jonas Twingler, GSM coordinator of ETSI (3):

Originally, GSM was seen as a Pan-European "only" system, in one single version and a fixed step towards the future. It turned Out, for several reasons, that it would be more beneficial for all parties, to launch an interim version of the standard at an early point in time-Phase 1-and to produce the full version of GSM-Phase 2-adapted to the "latest" news, situations and experience gained in Phase 1.

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 varieties. Even before the Phase 2 standard has been completed, GSM has grown far beyond its original geographical "limitations" and the Global System for Mobile communication really starts to deserve its name. With Phase 2, an.d 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.

## 1.2 SERVICES OFFERED IN A GSM SYSTEM

The features and benefits expected in the new system were (1) superior speech quality (equal to or better than the existing analog cellular technology), (2) low terminal, operational, and service costs, (3) a high level of security (confidentiality and fraud prevention), (4) international roaming (under one subscriber directory number), (5) support of low-power hand-portable terminals, and (6) a variety of new services and network facilities. This section explores the services that are offered in a GSM PLMN.

It was only a logical consequence of the prevailing reality that a measure of interworking compatibility with the services offered by other existing telecommunication networks was sought. In particular, the basis for the services in the GSM standard can be found in the ISDN concept.

We can distinguish three categories of services: (1) teleservices, (2) bearer services, and (3) supplementary services. As already mentioned above, the phased approach to introducing the services led to a subset of these services being included in Phase 1, and another set of services added later. In the following, these services are listed according to their phases (1 and 2), and the features supplied in the individual phases are discussed. Complete lists of the services defined for a GSM PLMN can be found in (4).

### 1.2.1 GSM Phase 1 Services

The Phase 1 technical specifications, valid for the networks in operation since 1992, provide the definitions for the set of services and features listed in Table 1.2 (3). It must be noted that bearer services are restricted to a maximum of 9,600 bps for technical reasons. ISDN networks use rates of up to 64 kbps. Adaptations are necessary.

These services are made available, or can be made available, by the operator of a Phase 1 network (their implementation is optional for the operators). Of course, the manufacturers and developers of infrastructure equipment and mobile terminals have to cope with the specifications of these services, since they have to provide the specific functions in their products.

**Table1.2**

**GSM pase 1 services**

| Service Category | Service | Comment |
|---|---|---|
| Teleservices | Telephony (speech) | So-called full rate,13 kbps |
| | Emergency calls (speech) | |
| | Short-message services: point-information: user to-user and network to all and point-to-multipoint (cell broadcast) | Alphanumeric to-point users |
| | Telefax | Group 3 |
| Bearer services | Asynchronous data | 300-9,600 bps,1,200/75 bps |
| | Synchronous data | 300-9,600 bps |
| | Asynchronous PAD (packet-switched, packet assembler/ disassembler) access | 300-9,600 bps |
| | Alternate speech and data | 300-9,600 bps |
| Supplementary services | Call forwarding | For example,subscriber busynot reachable or does not answer |
| | Call barring | For example,all calls, international calls,incoming calls |

### 1.2.2 GSM Phase 2 Services

Following the availability of the technical specifications for GSM Phase 2, there will be additional services defined that can be made available to end users. There are number of supplementary services defined for Phase 2. Table 1.3 gives an overview of these (3).

GSM Phase 2 also has many enhancements made possible through the experience with operational Phase 1 networks, through new ideas, and through the dedication of the involved parties to steadily improve the system and its services.

**Table 1.3**

**Services Added Thgrough GSM Phase 2**

| Service Category | Service | Comment |
|---|---|---|
| Teleservices | Telephony (speech)<br>Short-message services | Half rate, 6.5 kbps<br>General improvements |
| Bearer services | Synchronous dedicated packed data access | 2,400-9,600 bps |
| Supplementary Services | Calling/connected line identity presentation | Displays calling partys directory number before/ after call connection |
| Calling/connected line identity restriction | | Restricts the display of the calling party's number at called party's side before/after call connection |

| | |
|---|---|
| Call waiting | Informs the user about a second(incoming) call and allows to answer it |
| Call hold | Puts an active call on hold in order to answer or originate another (second) call |
| Multiparty communication | Conference calls |
| Closed user group | Establishment of groups with limited access |
| Advice of charge | Online charge information |
| Unstructured supplementary service data | Offers an open link for use between network and user for operator-defined services |
| Operator-determined barring | Restriction of different services call types by the operator |

## 1.3 WHAT IS A CELLULAR NETWORK?

Now that we know where GSM stands in the world, how it got to where it is today, and what it is supposed to do for its customers, we take a first look at how it works. We start at the very top, at the network level, to get an initial glimpse of how a GSM system works. First, however, a note on language. From now on,does lots of explaining of how radios work in cellular systems. In these explanations, the radios are referred to with language and terms usually reserved for living beings, such as “when the base station ‘discovers’ that . . .,“ or “the mobile ‘replies’ with Base stations do not really “discover” anything, and only people “reply” to commands. Radios in cellular systems do many things, and it helps if one separates a radio’s signaling tasks from everything else it does (carry voice traffic). To do this, the authors refer to radios as if they were alive and have personalities and habits, both good and bad, when describing signaling tasks. Users do not care about all the signaling tasks cellular radios perform; they only want their voices heard at the other end of the channel and to hear what is being said to them. In order for reliable communications to occur in a digital cellular system, radios have to do lots of channel maintenance tasks in the background, and they do all these tasks-invisibly and silently-with signaling routines as if they were, in fact, alive and carrying on their own little private conversations with each other, united in the task of moving the user's voice from one place to another. Think of radios as efficient and busy servants, and you will have much less trouble making sense out of all the details.

### 1.3.1 A Little Bit of History

It was some time since the days of Heinrich Rudolf Hertz until the first real achivements 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. Guglielmo 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 [5].

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 (1) small, low-power transmitters (run from motor generators in the vehicle), and (2) 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.

### 1.3.2 Cellular Structure

In the beginning of radio, engineers were happy to achieve a simple dedicated link between a transmitter and a receiver. As we saw in the previous section, these first links were not even two-way ones, but remained one-way dispatch links; that is, the people who catted 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 chan-nels at a single base site (Figure 3.2). 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.

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 have several cells coexist next to each other (Figure 1.3). The cellular structure was born. In order for this scheme to work properly, some restrictions had to he applied:

- 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.

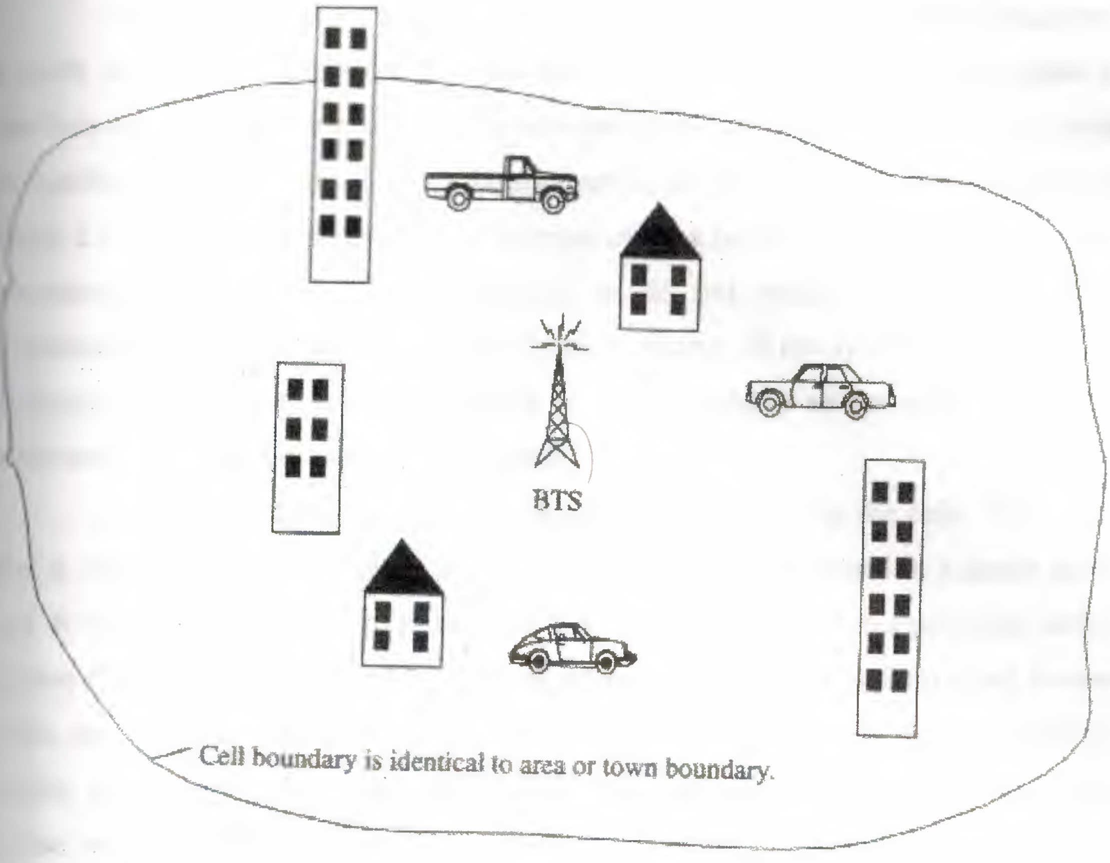
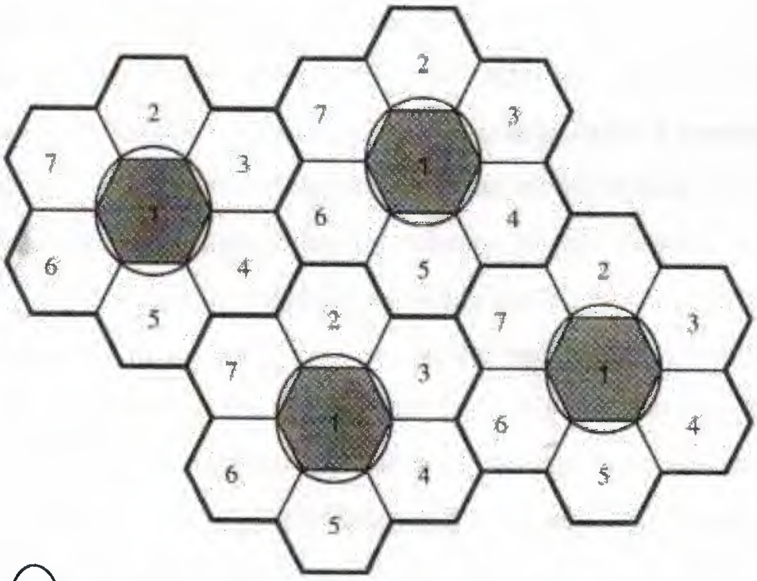


**Figure 1.2** Single cell structure



○ Transmission range ofcell No 1.

— Border of a cell.

▬ Cluster of cells using different frequencies

**Figure 1.3** Cellular structure

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. We will investigate how all this is done in the coming sections and chapters. For now, we can leave the mobile caller content to stay on the phone for a nearly unlimited time and still travel anywhere within the network's cell site coverage areas.

### 1.3.3 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 iiew capacity funds. A rather basic idea was to split the existing space into smaller portions, thus multiplying the number of channels available (Figure 1.4). 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. 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 1.5). Such antennas may be located at the entrances of tunnels, on the edge of a valley, or at the ends of streets among skyscrapers.

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 1.6) to address this

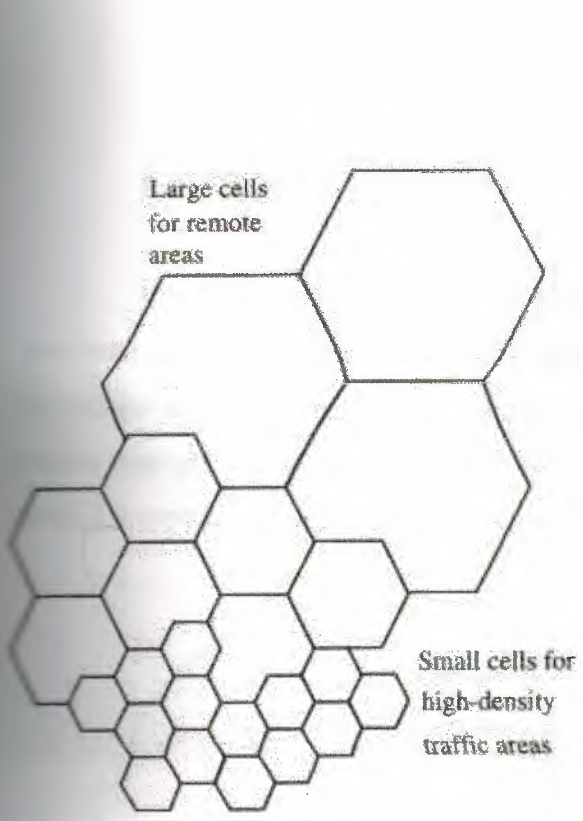
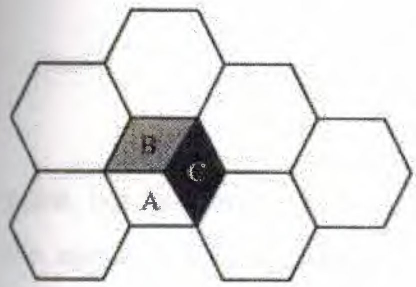

Large cells for remote areas
Small cells for high-density traffic areas

**Figure 1.4** Cell splitting and microcells



Three direction location

**Figure 1.5** Selective cells

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.

## 1.4 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.

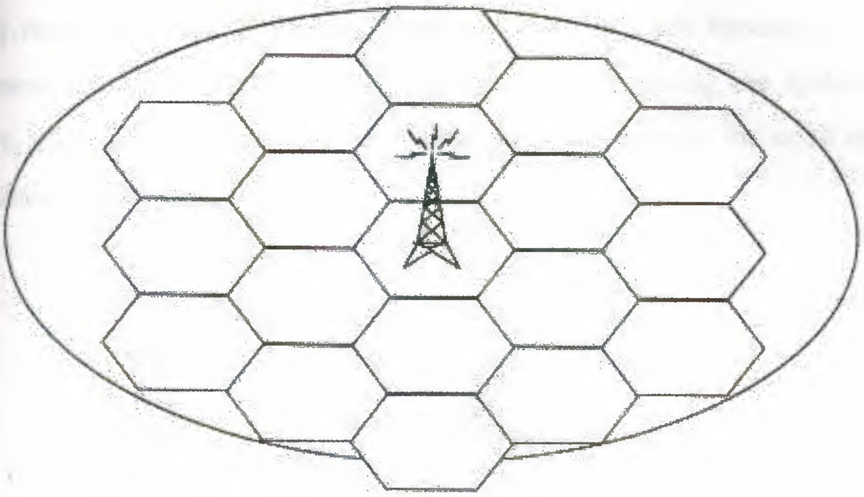


**Figure 1.6** Umbrella cell

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 1.7).

### 1.4.1 Mobile Station Terminal Equipment

The best known part of the cellular network is certainly the mobile station. Different types of stations are distinguished by power and application. Fixed mobile stations are permanently installed in a car and may have a maximum allowed RF output power of up to 20W. Portable units (bag phones) can emit up to 8W and hand-portable units up to 2W. With second-generation mobiles (on the market since 1993), the GSM system is becoming more and more attractive. Hand-portable units are becoming much smaller and are now not much larger than analog units. This is giving the system a boost in popularity, especially in those markets with a particular demand for small mobiles, such as in the Asian and Pacific areas.

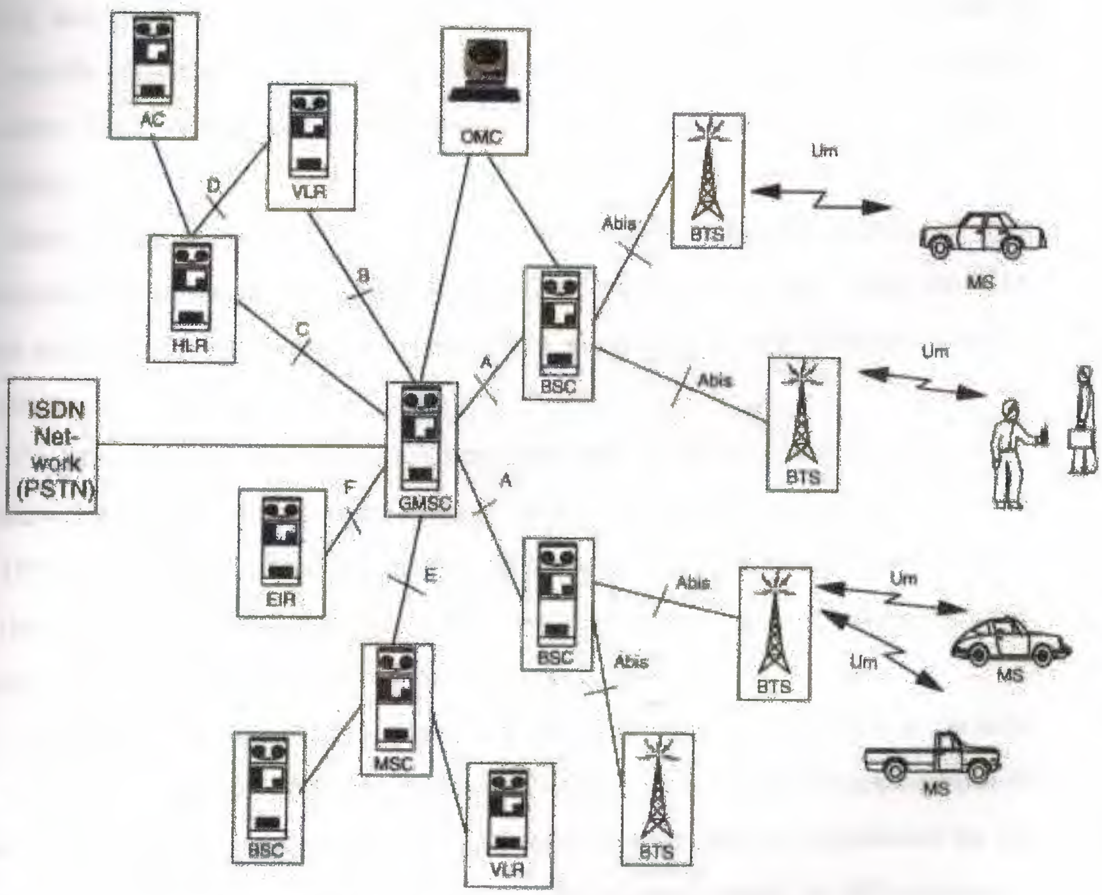


**Figure 1.7** GSM system architechure

### 1.4.2 Subscriber Identity Module

The subscriber identity module (SIM) provides mobile equipment with an identity. Without a SIM, a mobile is not operational (except for emergency calls). The SIM is a smart card and has a computer and memory chip permanently installed in a plastic card the size of a credit card. The SIM has to be inserted into a reader in a mobile station before the mobile terminal can be used for its intended routine purposes. For very small hand-portable phones, the credit-card type is too large. There is, therefore, a small version of the SIM, called the plug-in SIM.

Certain subscriber parameters are stored on the SIM card, together with personal data used by the subscriber, such as personal phone numbers. The SIM card identifies the subscriber to the network. Since only the SIM can personalize a phone, it is possible to travel abroad, taking only the SIM card, rent a mobile phone at the destination, and then use the phone (with the SIM card inserted) just as if it were a personal mobile phone at home. Anyone may reach a subscriber using the subscriber's home number. Every phone call, from wherever it is placed, is billed to the subscriber's home account.

Short messages received from the network may also be stored on the card. The recent introduction of larger memories and better microprocessors will make the SIM card even more flexible and powerful in the future, combining it with different services, such as credit and service cards.

To protect the SIM card from improper use, a security feature is built in. Before they can use the mobile, users have to enter a four-digit personal identification number (PIN). The PIN is stored on the card. If the wrong PIN is entered three times in a row, the card blocks itself, and may only be unblocked with an eight-digit personal unblocking key (PUK), which is also stored on the card.

We have explored only the salient aspects of the SIM card, which are related directly to the GSM system. With the increasing number of services and applications of smart cards, additional auxiliary functions and features may also be introduced on the SIM cards intended for use in the GSM systems. One example might be different access priorities for good customers, or restricted usage in certain areas.

### 1.4.3 Base Station or Base Transceiver Station

The counterpart to a mobile station within a cellular network is the base transceiver station (BTS), which is the mobile's interface to the network. A BTS is usually located in the center of a cell. The transmitting power of the BTS determines the absolute cell size. A base station has between one and sixteen transceivers, each of which represents a separate RF channel. Some of the intelligence, which was incorporated into analog base stations and the host network, such as measurements on the radio channels as criterion for handover, is now shifted to the mobile stations (see Section 1.7). Dumping some of the work on the mobile's "desk" makes the GSM infrastructure cheaper than that of some analog systems. The result is that in some less wealthy countries, digital cellular systems are installed instead of analog ones (such as AMPS, NMT, or TACS).

### 1.4.4 Base Station Controller

The base station controller (BSC) monitors and controls several base stations, *the number of which depends on the manufacturer and can be between several tens and several hundreds of stations. The chief tasks of the BSC are frequency administration,* the control of a BTS, and exchange functions. The hardware of the BSC may be located at the same site as the BTS, at its own standalone site, or at the site of the mobile switching center (MSC). BSC and BTS together form a functional entity sometimes referred to as the base station subsystem (BSS).

### 1.4.5 Gateway Mobile Services Switching Center

The gateway mobile services switching center (GMSC) is the interface of the cellular network to the PSTN. It is a complete exchange, and with all its registers it is capable of routing calls from the fixed network-via the BSC and the BTS-to an individual mobile station. The GMSC also provides the network with specific data about individual mobile stations. Depending on the network size, an operator might use several interfaces to the fixed network, thus using several GMSCs or only one. If the traffic within the cellular network requires more exchange capacity than the GMSCs can provide, *additional mobile services switching centers (MSC) might* coexist with no access to the fixed network. If not otherwise explicitly distinguished from each other, the capabilities of the GMSC and the MSC are the same. A major difference between the two is that the MSC has no related home location register (HLR).

### 1.4.6 Operation and Maintenance Center

The operation and maintenance center (OMC) has access to both the (G)MSC and the BSC, handles error messages coming from the network, and controls the traffic load of the BSC and the BTS. The OMC configures the BTS via the BSC and allows the operator to check the attached components of the system. As the cells become smaller and the number of base stations increases, it will not be possible in the future to check the individual stations on a regular basis for transceiver quality. Therefore, it is important to put remote control of the maintenance in place to save costs, but still maintain the quality of the system. This is supported by better self-test functions in the BTS. The distribution of maintenance tasks is treated differently by different manufacturers.

### 1.4.7 Home Location Register

The HLR stores the identity and user data of all the subscribers belonging to the area of the related GMSC. These are permanent data such as the international mobile subscriber number (IMSI) of an individual user, the user's phone number from the public network (which is not the same as the IMSI), the authentication key (see Section 1.8.1), the subscriber's permitted supplementary services, and some temporary data. Temporary data on the SIM include such entries as (1) the address of the current visitor location register (VLR), which currently administers the mobile station (see Section 1.4.8), (2) the number to which the calls must be forwarded (if the subscriber selects call forwarding), and (3) some transient parameters for authentication and ciphering.

The IMSI is permanently stored on the SIM card. The IMSI is one of the pieces of important information used to identify a subscriber within the GSM system. The first three *digits of the IMSI identify the mobile country* code (MCC) and the next two digits are the mobile network code (MNC, see Table 1.4). Up to ten additional digits of the mobile subscriber identification number (MSIC) complete the IMSI. The following IMSI:

262 02 454 275 1010

identifies a subscriber from Germany (MCC = 262), who is paying his or her monthly bill to the private operator D2 privat (MNC = 02). The subscriber's network identity number (MSIC) is 454 275 1010. The number with which the subscriber may be reached from the public network is totally different from the IMSI, and starts with an area code of 0172, followed by a seven-digit subscriber number. The first digits of this subscriber number identify the subscriber's related HLR. The number of digits used for this purpose is dependent on both the network size and the number of HLRs in the network. The IMSI is only used for internal network purposes.

### 1.4.8 Visitor Location Register

The VLR contains the relevant data of all mobiles currently located in a serving (G)MSC. The permanent data are the same as data found in the HLR;the.temporary data differ slightly. For example, the VLR contains the temporary mobile subscriber identity (TMSI), which is used for limited periods of time to prevent the transmission of the IMSI via the air interface. The substitution of the TMSI for the IMSI serves to protect the subscriber from high-technology intruders and helps point to the location of the mobile station through the cell identity. The VLR has to support the (G)MSC during a call establishment and an authentication procedure as it furnishes data specific to the subscriber. Locating subscriber data in the VLR, as well as in the HLR, reduces the data traffic to the HLR, because it is not necessary to ask for these data every time they are needed. Another reason for storing nearly identical data at two different locations (in the HLR and the VLR) is that each serves a different purpose. The HLR has to provide the GMSC with the necessary subscriber data when a call is coming from the public network. The VLR, on the other hand, serves the opposite function, providing the host (G)MSC with the necessary subscriber data when a call is coming from a mobile station (e.g., during authentication).

**Table 1.4**

List of Different Country Codes Among the GSM Systems

| MCC | Country | MNC | Network |
|---|---|---|---|
| 505 | Australia | 01 | Telecom Australia |
| 505 | Australia | 02 | Optus Communication |
| 505 | Australia | 03 | Vodafone |
| 232 | Austria | 01 | A E-NETZ |
| 206 | Belgium | 01 | BEL MOB-3 |
| 238 | Denmark | 01 | DK TDK-MOBIL |
| 244 | Finland | 91 | SF Tele Fin |
| 208 | France | 01 | F France Telekom |
| 208 | France | 02 | F SFR |
| 262 | Germany | 01 | D1-Telekom |
| 262 | Germany | 02 | D2 privat |
| 222 | Italy | 01 | I SIP |
| 204 | Netherlands | 08 | NL PTT |
| 530 | New Zealand | 01 | Bell South |
| 228 | Switzerland | 01 | CH Natel D |
| 240 | Sweden | 01 | S TELE RADIO |
| 240 | Sweden | 07 | S COMVIQ |
| 240 | Sweden | 08 | S NORDICTEL |
| 234 | United Kingdom | 10 | UK CELLNET |
| 234 | United Kingdom | 15 | UK VODAFONE |

If a mobile station is located in its own (G)MSC, it still uses the two different registers, even though the VLR, in this particular case, seems redundant. The consistency simplifies the underlying procedures.

### 1.4.9 Authentication Center

The authentication center (AC) is related to the HLR. It provides the HLR with different sets of parameters to complete the authentication of a mobile station. The AC knows exactly which algorithm it has to use for a specific subscriber in order to calculate input values and issue the required results (see Section 1.8.1). Since all the algorithms for the authentication procedures are stored within the AC, they are *protected against abuse. The SIM card issued in an area assigned to an AC contains the* same algorithms for authentication as the AC does. If the AC provides input and output parameters for these algorithms to either the HLR or the VLR, either location register can verify (authenticate) the mobile station.

### 1.4.10 Equipment Identity Register

The equipment identity register (EIR) is an option that is up to the network operator to make use of. The implementation of the EIR is a relatively new security feature of the GSM system. Within the EIR we find all the serial numbers of mobile equipment that is either stolen or, due to some defect in their hardware, may not be used in a network. The international mobile equipment identity (IMEI) is not only the serial number of a certain mobile station, but it also reveals the manufacturer, the country of production, and type approval. The idea is to check the identity at each registration or call setup of any mobile station, and then, depending on its IMEI, admit or bar access of the mobile station to the system.

*An example of a forbidden mobile might be that the* RF *quality of a certain* mobile station from a certain manufacturer is not as good as the recommendations specify; *for example, it produces spurious emissions or disturbs other radio services in* the area. The operator may check for this specific mobile station (since the model number and manufacturer are part of the IMEI) and reject it from its network.

Figure 1.7 not only shows the different parts of the network we have listed here, but also the names of the different interfaces between them. The Urn interface is sometimes called air interface. We also include a description of the Abis interface between the BTS and the BSC. An understanding of the Abis interface is required for testing a base station. The other interfaces are just named for further information, since they have nothing to do with the cellular quality or the radio character of GSM. How the different radio and network entities work together is shown in the next two sections about registration and call establishment.

## 1.5 REGISTRATION

After a mobile station is switched on, it scans the whole GSM frequency band with a certain scanning algorithm in order to detect the presence of a network in the least amount of time. When the network is detected, the mobile station reads the system information on the forward or, as it is called in GSM, the base channel. With this information, the mobile station is able to determine its current position within the network. If the current location is not the same as it was when the mobile was last switched off, a registration procedure takes place. Figure 1.8 describes the required actions in a registration procedure and their relationships to the different entities within the network.

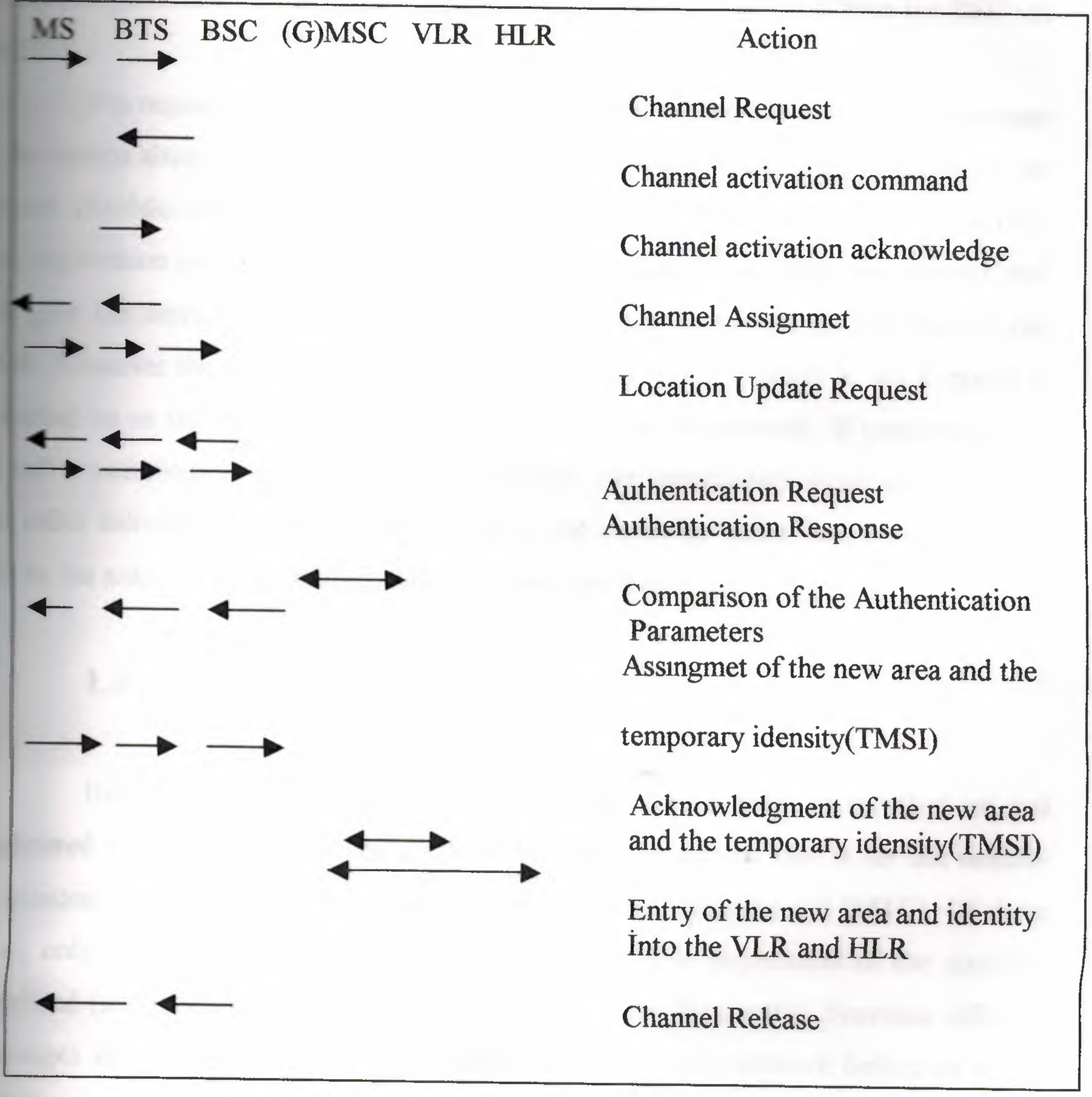

MS
BTS
BSC
(G)MSC
VLR
HLR
Action
Channel Request
Channel activation command
Channel activation acknowledge
Channel Assignmet
Location Update Request
Authentication Request
Authentication Response
Comparison of the Authentication Parameters
Assıngmet of the new area and the
temporary idensity(TMSI)
Acknowledgment of the new area and the temporary idensity(TMSI)
Entry of the new area and identity İnto the VLR and HLR
Channel Release

**Figure 1.8** Registration in the network

First, the mobile station requests a channel from the network, which will be assigned by the base station. Before the channel is actually assigned to the Urn interface, the BSC has to activate a channel on the BTS, which has to acknowledge the activation to the BSC in return. Now that the mobile station is connected to the infrastructure, the mobile station tells the system that it wants to perform a location update.

This wish is passed on, via the BSC, to the (G)MSC, which, being very stubborn *and bureaucratic, requires an authentication of the mobile station before taking* any further action. Upon the receipt of the correct parameters, the (G)MSC accepts the mobile, via the BSC and the BTS, into its new location, and-if this option is used in the network-assigns a temporary identity (TMSI), which the mobile station also has to acknowledge. When this procedure is finished, the channel is released from the BSC via the BTS.

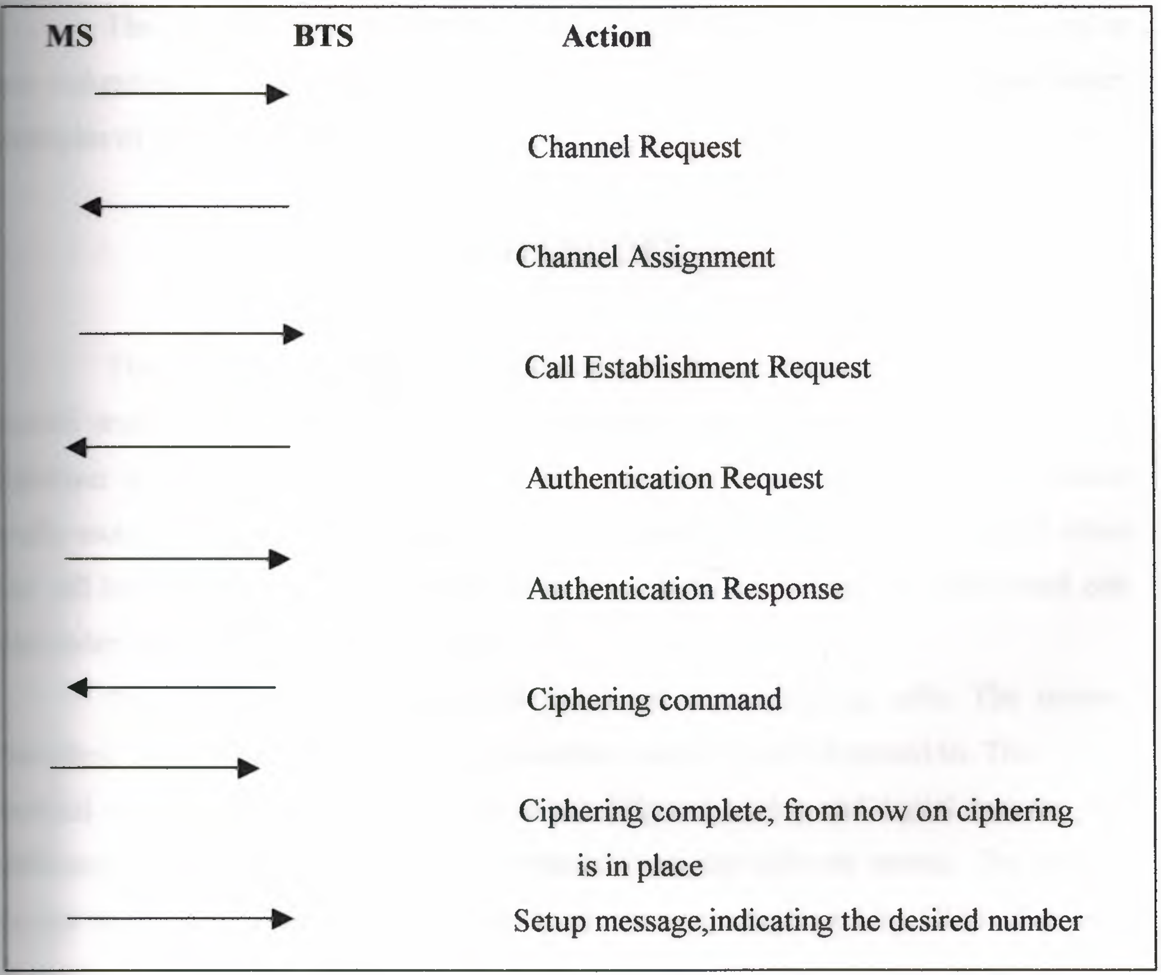
The registration could as well be accomplished by the network. This is the case if the system always wants to know exactly which mobiles are currently available on the system. (Mobile stations would notify the network when they are switched on or off.) The registration procedure is a means to limit the message flow within the network and still give the network virtual control. The network always knows the contents of the HLR. Whatever the HLR knows the GMSC also knows, and whether or not a mobile is switched on or off becomes common knowledge within the network. If someone wants to call a switched-off mobile station, the GMSC can immediately signal a message to the caller indicating that the specific mobile is not available, rather than try to route the call to the area where the mobile station was last heard from.

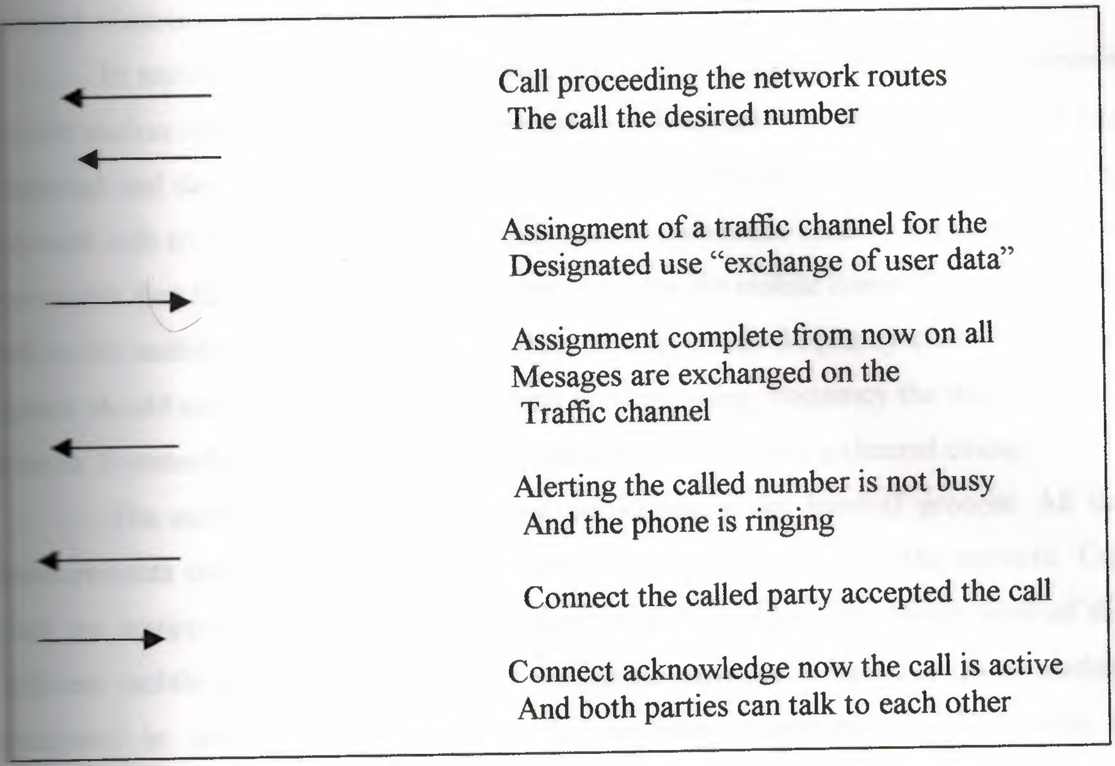
## 1.6 CALL ESTABLISHMENT

Before a call can be established, the mobile station must be switched on and registered into the system. There are two different procedures. One is for the mobile-originated call (MOC), and the other is for the mobile-terminated call (MTC). Of these two, only the MOC is described here, in order to give an impression of the signaling overhead (message exchanges) used in the GSM system. Be careful! Fourteen different messages are exchanged between the mobile station and the network before an actual call (i.e., exchange of user data) starts.

In a manner similar to the location update procedure, the mobile starts with a channel request, which is answered by the system with a channel assignment. The mobile station informs the system why it wants a channel (e.g., it wants to establish a call). Before the procedure is allowed to continue, the mobile again has to authenticate itself. To protect any further signaling messages from eavesdroppers, the network may now, with the next message, tell the mobile station to start ciphering its data. Ciphering means that the messages are transmitted in a scrambled way that only the mobile station and the BTS understand. In the Setup message, the mobile transmits the number it wants to call. While the call is proceeding, the BSC (via the BTS) assigns a traffic channel on which the exchange of user data is performed. Different types of messages and user data move on different types of channels. For the moment, it should be enough to know that there are channels that only support the message exchanges, and other channels on which the user data are handled. If the called party is not busy, the mobile alerts and the connection is established when the called phone is brought off the hook (Figure 1.9).

**Figure 1.9** Mobile-originated call establishment.


MS
BTS
Action
Channel Request
Channel Assignment
Call Establishment Request
Authentication Request
Authentication Response
Ciphering command
Ciphering complete, from now on ciphering is in place
Setup message,indicating the desired number



Call proceeding the network routes
The call the desired number

Assingment of a traffic channel for the
Designated use “exchange of user data”

Assignment complete from now on all
Mesages are exchanged on the
Traffic channel

Alerting the called number is not busy
And the phone is ringing

Connect the called party accepted the call

Connect acknowledge now the call is active
And both parties can talk to each other

The opposite MTC procedure is almost identical to the MOC procedure and is too redundant to be included in our discussion. We will, however, see many other examples of all kinds of message exchanges throughout this project.

## 1.7 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 transpond 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 catted a simple handover between BTSs (Figure 1.10).

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 1.11). 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.

## 1.8 SECURITY PARAMETERS

In the previous sections some security parameters have already been mentioned. Now it is time to summarize these features and describe their operations.

### 1.8.1 Authentication

The authentication procedure (Figure 1.12) checks the validity of subscribers' SIM cards, and whether they are permitted in a particular network. The authentication is based on the authentication algorithm, A3, which is stored on the SIM card and in the AC.

The A3 algorithm uses two input parameters:

one is the authentication key, Ki, which is stored only on the SIM card and in the network.The second value, the randomly generated number (RAND), is transmitted to the mobile station on the Urn interface.

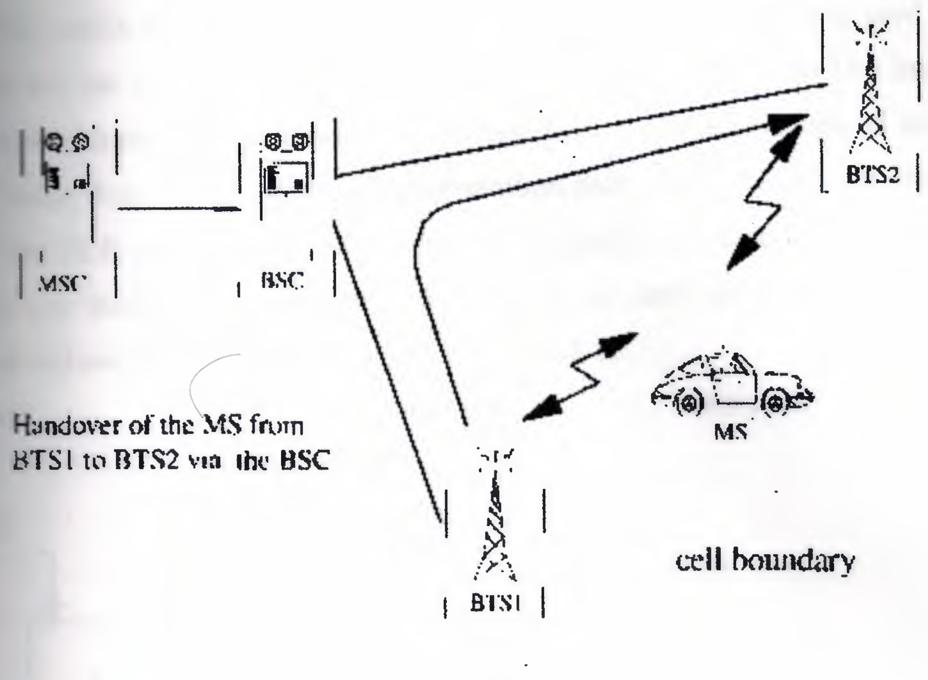


**Figure 1.10** Handover between BTSs

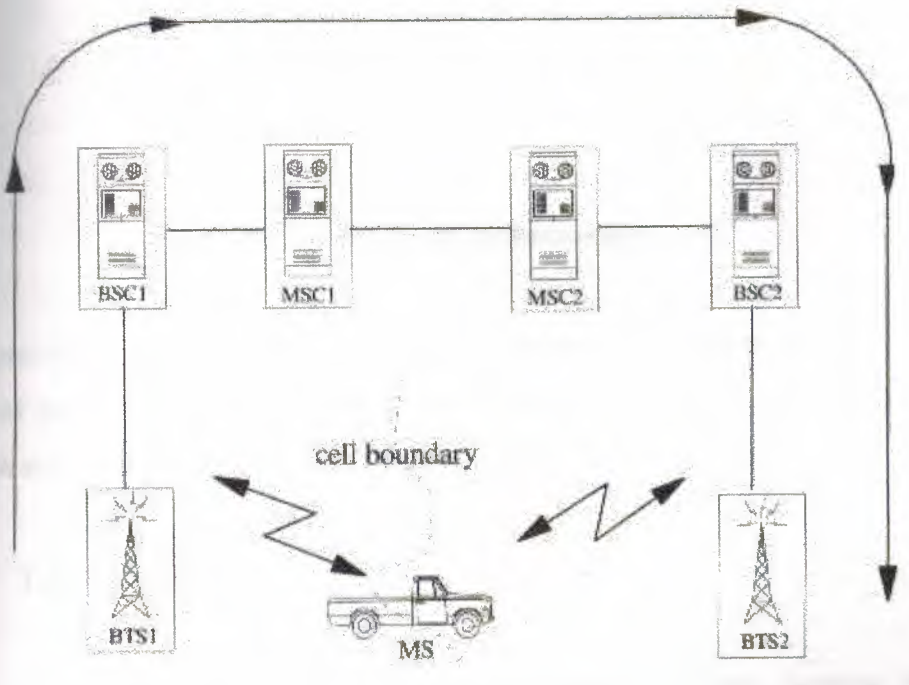


**Figure 1.11** Handover between MSCs.

The mobile station passes the RAND to the SIM card where it is used as an input value for the A3 algorithm. The result, SRES, is returned-via the Urn interface from the mobile station-to the network where the value of SRES is compared with the calculated value from the AC. A set of authentication parameters (RAND and SRES) is stored in the HLR and VLR for use by the AC. Usually, a number of sets of these parameters are stored there because a different set is used for each call setup or registration and are discarded alter each use. If the HLR or

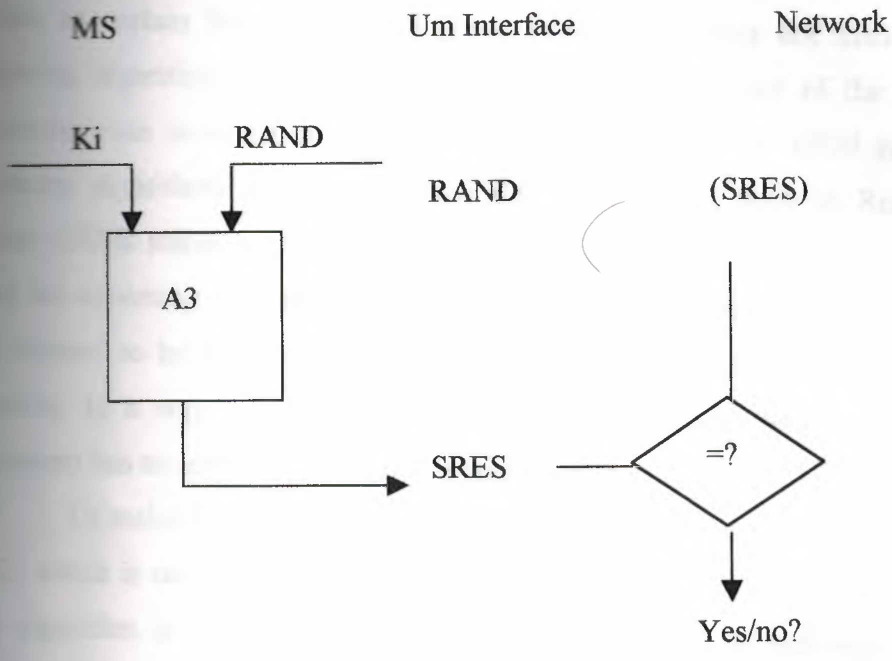


**Figure 1.12** Principle of authentication

VLR runs low on parameter sets, some new ones are requested from the AC. One important point of this security feature is that the relevant parameters (A3 and Ki) are stored in secure places and are never transmitted on the Um interface.

### 1.8.2 Ciphering

Digital transmission is suitable for the ciphering of data, because bit streams merely have to be scrambled with a certain method known only to both sides of the air interface. The GSM system uses such a ciphering method to protect signaling and user data. In order to ensure that the ciphered data from one side can be deciphered on the other side, a reversible algorithm is used. This means that if the ciphering algorithm, A5 is used to encipher a data stream, the same algorithm is used to decipher this stream and get back the original data stream.

One can easily understand that it is important that both entities use the same ciphering algorithm. In the current system only one algorithm is used, which is called A5/1. This is a special, protected algorithm, and the protection afforded the algorithm makes it is difficult to export the GSM system, with this ciphering capability, into countries other than the COCOM states (the Eastern European states restricted from access to certain Western technologies). Typically, it does not matter whether the ciphering algorithm is disabled or not, as long as it is part of the software. It is becoming even more difficult, if not impossible, to export the GSM system (with the ciphering algorithm) into former non-COCOM countries such as Russia, the other former USSR states, and China. Although COCOM does not exist anymore,the basic rules for exporting systems using the elaborate A5/1 ciphering still apply (i.e., A5/1 is not allowed to be exported). There are even new assemblies dealing with this kind of question. In a way, it might even be said that a company willing to export cellular equipment has to apply for individual export licenses.

To make exporting easier, the ETSI developed a new, simpler algorithm called A5/2, which is used for these former non-COCOM countries. The ciphering with this new algorithm is as secure as it is with the old one. This technique for achieving security does not use as much mathematics as the old one uses. Both algorithms can coexist in a network, and measures are employed to make sure that a mobile coming from a country using only the A5/2 algorithm has access to the European systems where the A5/1 algorithm is used. This is the reason why western European networks support both algorithms.

The designers of the ciphering aspects claim that this algorithm is so well protected against eavesdropping that even if someone knows the complete specifications, he or she would not be able to listen in on the data. This, of course, means that the security services, which in some countries listened in on private mobile phone conversations in the past, are no longer able to do so. This situation led to the delay of the acceptance of GSM in some countries.

Having only two algorithms for ciphering could make the life of professional eavesdroppers relatively easy. The algorithms, therefore, require a specific key, Kc. This key is calculated from a random number, RAND, delivered from the network. This is the same number that was used for the authentication procedure. The only difference is that a different algorithm, A8, is used to produce the ciphering key (Figure 1.13). The A8 algorithm is stored on the SIM card. The mobile equipment does not know anything about the security-related algorithms A3 and A8. This Kc key issued by the A8 algorithm is then used with the ciphering algorithm, A5/1 or A5/2, to encipher or decipher the data. The A5 algorithm is implemented in the mobile station whether it is A5/1 or A5/2.

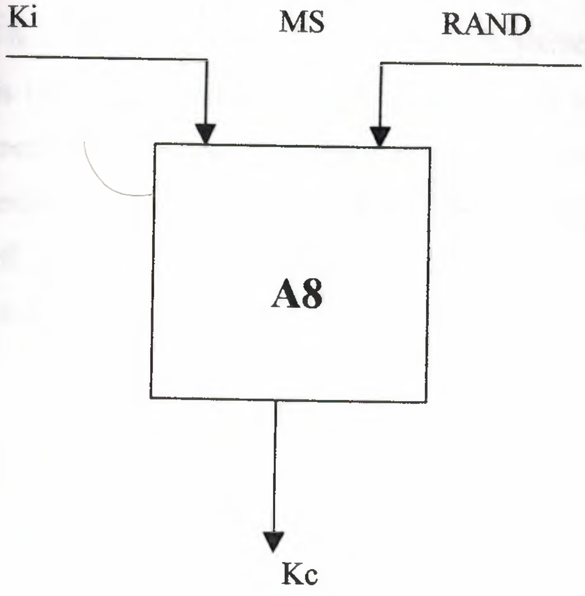


**Figure 1.13** Calculation of the ciphering key(Kc).

To start the ciphering procedure, the network commands the mobile station to start ciphering with a specific ciphering sequence. From this time onward, the mobile station transmits ciphered data, where even the acknowledgment that ciphering is being used is already transmitted with enciphered data (Figure 1.14).

### 1.8.3 Temporary Mobile Subscriber Identity

To prevent a possible intruder from identifying GSM users by their IMSI, which is a permanently assigned number, a temporary identity is assigned to all subscribers while they are using the network. This identity is stored, along with the real identity, in the network. The temporary identity is assigned during the location updating procedure, and is used as long as a subscribers remain active in the network. The mobile station uses this temporary number when it reports to the network or originates a call. Similarly, the network uses the temporary number to page the mobile station. The assignment, administration, and updating of the TMSI is performed by the VLR. When it is switched off, the mobile station stores its TMSI on the SIM card to make sure it is available when it is switched on again.

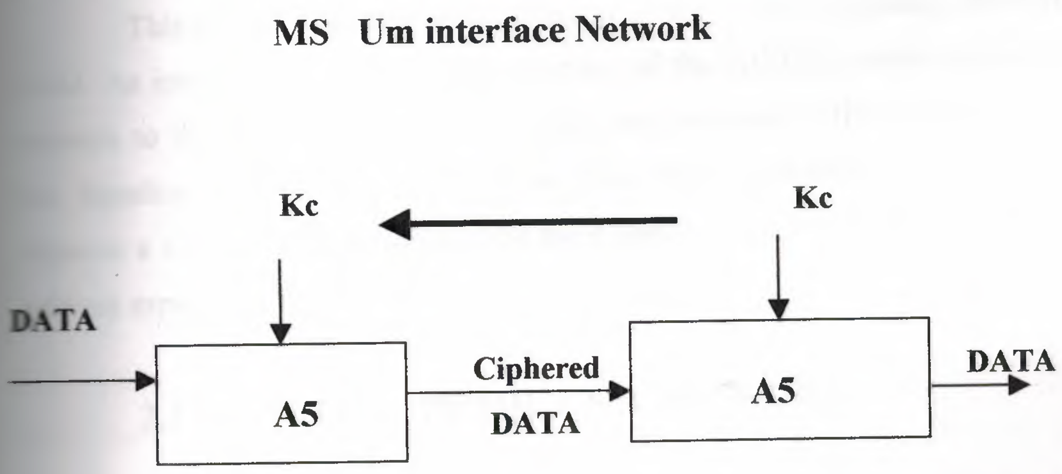


**Figure 1.14** Start and execution of ciphering

## CHAPTER 2

# LAYERS AND SIGNALING PRINCIPLES IN THE GSM SYSTEM

A telecommunications system cannot work without a minimum number of signaling functions to organize the interworking of its network entities and the interworking with other networks. Signaling is required to establish, maintain, and terminate connections or communication links. Signaling is necessary to make sure that the provision of services is taking place by the use of defined procedures. Measures have to be taken for all cases of service and system usage and in case of problems or malfunctions. Compared to the means of signaling used in the old, conventional telephone networks (e.g., dial tone, ring-down, dial pulses) and taking into account the higher complexity of a mobile network, which provides uncounted service features, a considerably higher signaling overhead can be expected for a system like GSM. The signaling overhead is great, although transparent (i.e., not obvious to or recognized by the end user).

This chapter describes the architecture of the complex signaling system used in GSM. An introduction to the layered structure of the ISO/OSI model is given, with an example to illustrate its functionality. Finally, an overview of the functional entities in the signaling system is given. Because this book emphasizes signaling protocols between a GSM mobile station and the fixed network (MSC/BSC/BTS), particular and relevant aspects are introduced.

## 2.1 SIGNALING IN THE GSM NETWORK

In order to cope with the task of having to organize a complex network system, the creators of the GSM specifications have chosen to rely on some already defined procedures and interface descriptions, and to adapt them for the mobile environment. The GSM system makes use of the so-called signaling system no. 7 (SSN7), which ISDN signaling is also based on. The SSN7 has been described by CCITT (International

ISDN signaling is also based on. The SSN7 has been described by CCITT (International Telegraph and Telephone Consultative Committee), which originally defined it for fixed-network signaling and exchange switching. For use in a mobile telephone system, it had to be adapted and expanded by adding, for example, a so-called mobile application part (MAP), which contains additional procedures for coping with the mobility of the user. SSN7 provides a number of signaling channels and procedures for the communication (signaling transport) between the single entities in a GSM PLMN (e.g., the MSC, BSC, BTS, VLR, HLR, AC, and MS).

One means of describing the architecture and the interworking of the above-mentioned signaling system is the layered model according to the International Standards Organization (ISO) with the open systems interconnection (OSI) presentation.

## 2.2 THE ISO/OSI LAYER STRUCTURE

The ISO/OSI layer model contains seven layers, each of which represents a certain entity with its particular functions and tasks.

### 2.2.1 What Is a Layer?

A separate layer can be regarded as a logical block in a communications entity, such as a mobile phone or a telephone exchange (switch). A logical block has certain functions, tasks, or assignments. It also has its own tools for executing its tasks. These tools consist of protocols, comparable to a language, that allow the layer (e.g., in a mobile station) to contact and communicate with its peer layer, which is a layer on the same level within another communications entity (e.g., in a switching center). The protocol used by two peer layers to communicate with each other is called peer-to-peer protocol.

Such a protocol also contains functions and conventions that describe how to use its own functions and those provided by the next lower layer to (1) execute the tasks in its own layer and (2) provide functions to the next higher (the upper) layer.

We can also find notifications, which are exchanged between one layer and its upper or lower layer in the same entity; for example, to inform the upper layer that a message (information) has been received or to instruct the lower layer to pass on a message (information). Such notifications are called primitives. They are part of the layer's protocol to organize the interworking with the neighboring layers (upper and lower). Figure 2.1 illustrates the functions and interconnection of layers.

### 2.2.2 An Example of the Layer Model

An example of communication over three layers can help with understanding the functionality and the dynamics of the layer model and its use in a communications system.

In this example, we watch the captains of two large ships, one coming from Brazil and the other one from Germany. They happen to meet, as they did very often before, at sea, far out on the ocean. Both captains are fond of soccer and they always like to exchange the latest results from their home country's first division. They also discuss the latest weather forecasts for the regions they are sailing to. Unfortunately, the Brazilian captain only speaks Portuguese and the German captain only knows his mother tongue. To get around this little problem, they employ their cooks as interpreters. The cooks both speak fluent French-what else, for a cook? Still, both sides also need the help of their radio operators, who have the task of "physically" connecting the two cooks; that is, to transmit their voices or dictated text between each other. Figure 2.2 illustrates this arrangement.

The two captains can be seen as part of the uppermost layer; in this example, it is Layer 3. They need the help (functions) of the lower layers in order to be able to communicate with each other. The two cooks, the interpreters, are part of Layer 2 and the radio operators are located in Layer 1, the lowest layer. With their own tools and their lower layers' functions, the three layers can now start to communicate with each other.

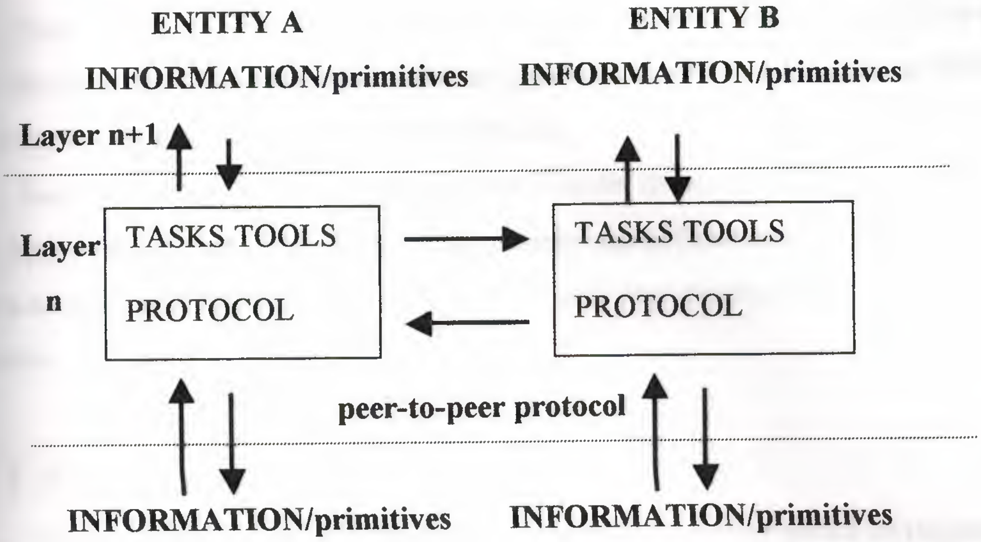


**Figure 2.1** Layer fuctionality

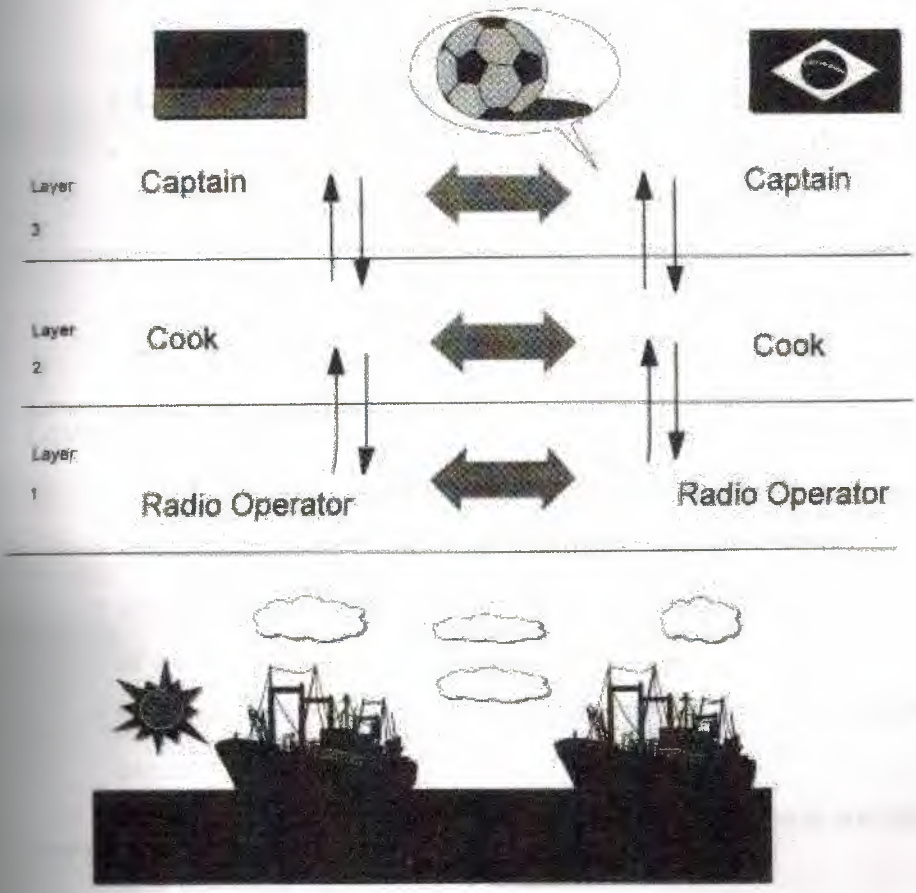


**Figure 2.2** Example of a coatiommunicn over three layers.

Even though the two captains seem to pass and receive their information in a vertical direction, the communication is virtually horizontal, and so is the conversation between the cooks and between the radio operators.

Each layer keeps to a common protocol in order to successfully communicate with its peer without contention and in order to make use of functions or supply functions to the layers below or above. Such a protocol may consist of the following procedures.

### Layer 1, the radio operators:

- Transmit messages, or information, they receive from their cooks on request;
- Notify their respective cooks when a message is received and pass it on when each cook is ready;
- Agree on a form of radio transmission, such as which frequency channel and whether to transmit speech or Morse signals;
- Comply with the international rules for radio transmission and communication;
- Acknowledge messages, ask whether the transmissions were readable, and notify the other party if something is not understood;
- Change the channel or increase the transmitted radio power in the case of bad reception.

### Layer 2, the cooks:

- Translate the received information from their mother tongues into French and vice versa;
- Inform their captains every time there is a new message, such as another result of a soccer match;
- Partition the flow of speech from their captains into short and understandable blocks;
- Inform their counterpart when a block of information is not understood and may ask for a repetition;
- Count the information blocks (e.g., each soccer result), and should the need arise, can tell by the number which block has not been received.

Layer 3, the captains:

- Introduce themselves to each other and tell their counterpart what they would like to know;
- Exchange the final results of last weekend's soccer matches;
- Discuss the latest weather forecast;
- Pass their information to the cooks and instruct them to translate a message and pass it on for transmission.

In each of the virtually horizontal connections between peer layers, changes in the protocol of the other layers are not relevant and have no influence. Theoretically, the following could happen.

- The captains change the subject and start to chat about their last climbing tours in the mountains, since both are fond of this activity in their leisure time. What kind of information (text) they translate or transmit is irrelevant to the cooks and radio operators, respectively.
- Both cooks find out by chance that both of them study the Chinese language (Mandarin) for a better understanding of the Chinese kitchen. In order to exercise and improve their skills, they decide to use Mandarin instead of French. Theoretically, presuming a certain level of mastery, this change will have no influence on the conversation between the captains or on the radio transmis-sions. A channel change or the use of Morse instead of voice radio transmission in Layer 1 will have no virtual influence on the other two upper layers.

## 2.3 THE SEVEN LAYERS OF THE ISO/OSI MODEL

The ISO/OSI model for an open communication system defines seven layers. Table 2.1 shows these layers and their meanings according to the model.

The signaling between all the interfaces from a GSM mobile station to the

MSC takes place in the lower three layers (i.e., Layers 1 to 3).

Their functionality, with emphasis on the signaling taking place between a GSM mobile station and the fixed network (Urn or radio interface), will be dealt with in the following chapters.

It should be noted here that layer 1, the physical layer, can be regarded as a means for transporting signaling data as well as user data. For the transmission of user data (e.g., speech data) the layer model does not apply. Due to the fact that in GSM (as in all communication systems) user data is transmitted over basically the same physical channel, with differences only in the logical organization and in the coding, our description of Layer 1 will also include, in the following chapters, the handling and transmission of user data.

**Table 2.1**

| The Seven Layers of the ISO/OSI Model | | |
|---|---|---|
| Layer 7 | APPLICATION | Application protocols, user- oriented provision of communication media |
| Layer 6 | PRESENTATION | Application-specific format transfer |
| Layer 5 | SESSION | Connection of application processes, billing |
| Layer 4 | TRANSPORT | Flow control for point-to-point connections |
| Layer 3 | NETWORK | Connection and switching of communication links |
| Layer 2 | DATA LINK | Control of signaling links, block transfer of signaling data |
| Layer 1 | PHYSICAL | Physical transmission, coding, error correction, modulation, etc. |

# CHAPTER 3

## The TDMA Approach: DECT Cordless Access as a Route to PCS

An analog cellular radio is replaced by second-generation digital systems such as (in Europe) GSM and DCS 1800, the attention of the telecommunications community is turning toward the specification of future mobile communications systems aimed at increasingly personalized services. However, an alternative approach to personal communications is also emerging, termed personal communications services, or PCS. This approach is based a combined strengths of two entities: the existing telephone network (either private public) and a radio access part.

In this chapter, we explore this approach in relation to cordless access that conforms to DECT standard.

### 3.1 PCs

The aim of PCS is to provide personalized voice, data, image, and video communications services that can be accessed regardless of location, network, and time. The PCS concept includes terminal mobility, personal mobility, and service mobility.

PCS can bring many benefits to its users. Personalizing the communications services is in effect an increase in the efficiency of the telecommunication services to deliver calls to its users. Current telephone networks supply services at places where people are expected to be. For example, in a private branch exchange (PBX) network, calls are delivered to desks, and it is far from certain that the person for whom a call is intended is at his or her desk.

Personalizing networks means, in effect, that users can access services wherever they are and, hence, that services are made available where the users are, at any moment.

Users may apply PCS for whatever benefits they want to derive from it, like improving convenience levels, business performance levels, competitiveness, or service levels. PCS may also be applied for reducing the costs of business operations.

LIBRARY
1988 - LEFKOŞA

levels. PCS may also be applied for reducing the costs of business operations.

If a user requires service access only in a limited area, for example, merely in and around the home, a system consisting of a single radio cell that can offer several access channels (i.e., a single-cell multiuser, or SC/MU, system) will probably meet that user's requirements. An SC/MU system is a simple "radio tail" of the network, delivering local mobility.

If services have to be accessible in larger areas, such as in factories, office buildings, or airports, a multicell, multiuser (MC/MU) system may be the optimum solution. MC/MU systems are a sophisticated means of delivering PCS in defined areas of radio coverage.

In some cases the requirements may even be such that users want PCS in a number of areas, as in a company's headquarters as well as its branch offices, or a factory outside the city center with its sales office in the city center. In those cases several MC/MU systems have to be networked into one, integrated system. Networks like these are of a higher level of complexity and have become available recently.

### 3.1.1 Network Plus Radio Access

To provide a PCS, one needs a network with the ability to route calls and services to the location where the subscribers actually are, not to the locations where the subscribers are registered. In addition, wherever the subscribers actually are, they should be able to access the same set of services as where they are registered and for which they pay their subscription fees. One way of achieving this service is by connecting databases, which are available at several places in the PCS network, such that subscriber information (like a user's personal number and the set of services he or she has subscribed to) is accessible at any point in the network.

In the network that provides the backbone for GSM, this database connection is accomplished with home location registers (HLR) and visitor location registers (VLR). *This chapter's focus is not on these registers but on the radio access part into the* network. For simplicity it is assumed that so called intelligent telecom networks will have the capability of delivering database services for PCS purposes.

The second building block for PCS is the ability to have (many) users access the network over a radio link. This is the focal point of this paper: radio access to a network provides for local, terminal mobility. Local mobility is defined as the area covered by the MC/MU radio access system. Terminal mobility is defined as the capability for the subscriber to carry an access (voice or data) terminal and access the network for services at any place and any time.

### 3.1.2 Requirements

The successful candidate for the radio access standard for personal communications has to meet the following requirements:

- **Low-cost terminals:** Personal communications can become truly personalized only if the cost of handsets is low enough to address the consumer market. This requires a technology that leads to low-cost hardware. Uncomplicated terminal design should be possible.
- **Low-cost network infrastructure:** The future of personal communications is envisaged whereby multiple operators offer total or partial area coverage. The required investment in infrastructure should be small, to reduce the operator's outlay.
- **High voice quality:** Personal communications will compete with wired telecommunications. For end users, voice quality comparable to current wired quality is important.
- **Data applications:** The growth of data communications, both in number of users as well as in data-throughput requirements, will also become manifest in personal communications.
- **Features:** Users will demand two types of features. On the one hand, they will request features related to the radio access, such as speech encryption to secure the privacy of their conversations; on the other hand they will require access to network features such as call forwarding, database access, call screening, message waiting indications, and dual-tone multifrequency (DTMF)—related features.
- **Uncoordinated, multioperator situation:** Probably the most important requirement is that numerous PCS operators compete to provide service to end users in the same geographical area (neighborhood, town, or country). This competition sets tough technical requirements on the radio access standard, since it has to support a cost-effective way of handling multiple operators.

### 3.1.3 The Technology: TDMA

Marketing a PCS based on radio access can be done successfully only if the product is based on a technology that meets the requirements listed in Subsection 3.1.2. The only currently available technology that meets these requirements is TDMA (time-division multiple access), as is applied in DECT (digital European cordless telecommunications).

The principle of TDMA is relatively simple. Traditionally, voice channels have been created by dividing the radio spectrum into (ever narrower) frequency RF carriers(chanels), with one conversation occupying one (duplex) channel. This technique is known as FDMA (frequency-division multiple access). TDMA divides the radio carriers into an endlessly repeated sequence of small time slots (channels). Each conversation occupies just one of these time slots. So instead of just one conversation, each radio carrier can carry a number of conversations at once.

The price that has to be paid for splitting up RF carriers into time slots is the bandwidth of each RF carrier. On average, the bandwidth per carrier has to be wider in the case of TDMA than in the case of FDMA. However, the main advantages of TDMA become evident when it is realized that a transceiver, when handling a conversation, is occupied for only a part of the time. In the case of traditional (analog or digital) FDMA systems, a transceiver is fully occupied when handling a conversation. The fact that in the case of TDMA a transceiver is occupied only for the duration of the time slot creates two important advantages:

- Cost reduction, because one transceiver can handle a number of calls simultaneously;
- Decentralized RF management, because a portable has time available to send and to receive additional information.

TDMA is the access method used in CT3, PHP, and DECT. Table 3.1 summarizes the air-interface characteristics of these systems, in comparison with the older FDMA technology of CT2.

- CT3 is the name of the so-called third generation of cordless telephony.
- PHP (personal handy phone) is the Japanese standard for cordless access that

aims especially at residential and public-operated applications.

- DECT is the acronym for the European standard on digital cordless telecommunications. We will focus on DECT.

## 3.2 DECT

The DECT standard was originally intended to solve the problem of providing cordless telephones in high-density, high-traffic environments, such as offices. It was instigated by the Council of European PTT's (post. telephone, and telegraph service operators) as a European standard for cordless telecommunications, with applications that included residential telephones, telepoint, the cordless PBX. and cordless local area access to the public network

DECT enables users to make and receive calls when in range of a base station (about 100m in an indoor environment and more than 500m in an outdoor environment). The standard has a seamless handover facility, which allows users to move between base stations during a call without being cut off. This means that users do not notice the range limitations on a base station, because they just roam from base to base. The small cell size does, however, provide advantages for capacity and speech quality. Also, the digital radio link and the 32-kbit/s adaptive differential pulse code modulation (ADPCM) speech code contribute to a speech quality that is as good as wireline quality. The radio link is encrypted to provide absolute call privacy.

**Table 3.1**

Digital Cordless Comparisons

| | CT2 | CT3 | DECT | PHP |
|---|---|---|---|---|
| Multiple access and duplex | FDMA/TDD | TDMA/TDD | TDMA/TDD | TDMA/TDD |
| Time frame | 2 ms | 16 ms | 10 ms | 5 ms |
| Speech coding | G.721 | G.721 | G.721 | G.721 |
| RF frequency | 864.1—868.1MHz | 862—866 MHz | 1880—1900 MHz | 1895—1911 MHz |
| Carrier spacing | 100 kHz | 1 MHz | 1.728 MHz | 300 kHz |
| Channels per carrier | 1 | 8 | 12 | 4 |
| Number of carriers (channels) | 40 (40) | 4 (32) | 10 (120) | 53 (212) |
| RF bit stream | 72 kbit/s | 640 kbit/s | 1152 kbit/s | 384 kbit/s |
| Modulation | GFSK | GFSK | GFSK | QPSK |
| Average power | 5 mW | 5 mW | 10 mW | 10 Mw |

DECT uses a multicarrier TDMA/time-division duplex (TDD) format for radio communications between handset and base station. With DECT, 10 radio carriers are available, each 1.728 MHz wide. Each radio carrier is divided in the time domain into 24 time slots, two of which provide a duplex speech channel. When a call is set up, it uses only 2 of the 24 time slots, alternating between transmitting and receiving signals. The remainder of the time can be used by the handset to monitor all other frequencies *and time slots and shift the call if a better speech channel is available.*

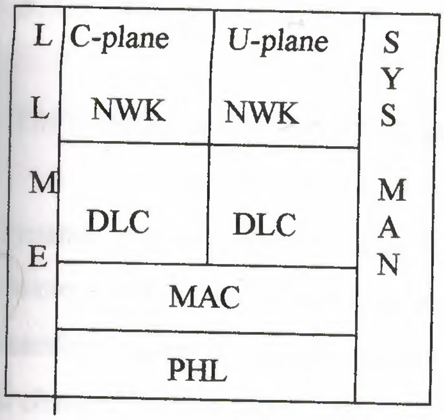
This continuous dynamic channel selection (CDCS) technique is a function under the control of the handset. CDCS is a process whereby the handset is continuously gathering information to decide on selecting better speech channels. This process may occur if, for example, the user moves away from one base station and toward another. The handover is undetectable by the user, which is important in a picocellular environment, where several handovers may be necessary during a short call.

The strength of DECT as a standard for cordless access is not only based on the TDMA principle. The standard has been specified in such a way that it caters for access to a range of host networks, including PBXs, networked PBXs, public switched telephone networks (PSTNs) (including telepoint), GSM networks, packet switched public data networks (PSPDNs), and integrated services digital networks (ISDNs). *DECT is highly capable of providing mobile services based on an intelligent host network, and therein lies its strength as a candidate for PCS.*

### 3.2.1 DECT and OSI

The DECT standard has been structured according to the open systems interconnection (OSI) model. The RF access occupies the lower three layers of OSI, but as OSI takes no account of radio transmission uncertainties and handover, DECT has redefined this part into four layers plus a lower-layer management entity (Figure 3.1).

The physical layer (PHL) defines the radio spectrum management. The medium access control (MAC) layer performs three main functions. First, it selects, establishes, maintains, and releases channels. Second, it multiplexes error-control information with higher-layer information into the time-slot packages. Third, the MAC layer provides a reliable point-to-point link. The data link control (DLC) layer provides reliable data links to the network layer. In this way, high levels of data integrity over the radio interface are provided.



PHL=Physical layer

MAC=Medium access control layer

DLC=Data link control layer

NWK=Network layer

LLME=Lower layer management entıty

Sys.Man=System management

**Figure 3.1** DECT reference model

The fourth layer in DECT is the network (NWK) layer, which is the main signaling layer of the protocol and mainly supports the establishment, maintenance, and release of calls.

Finally, a lower-layer management entity (LLME) has been defined to cater for procedures that concern more than one layer. LLME is intertwined with MAC, DLC, and NWK layers.

### 3.2.2 PHL: The TDMA Format

DECT's TDMA format is described in Part 2 of the DECT standard, the physical layer. Every radio carrier supports 12 duplex channels, which consist of 12 pairs of time slots per TDMA time frame. Each time frame is available on every carrier. DECT has 10 carriers of 1.728 MHz each. The TDMA time-frame and slot structure for DECT is shown in Figure 3.2.

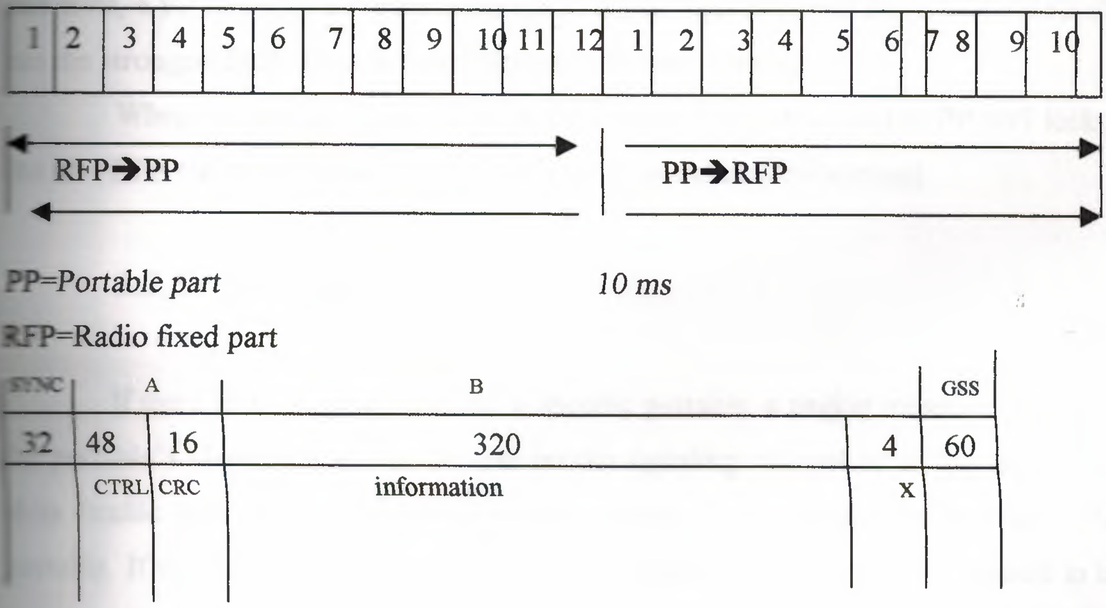
The TDMA format for the RFP-to-PP connection is time-duplexed with the PP-toRFP connection. This process is called time-division duplex (TDD).

Because DECT uses 10 carriers over which this TDMA/TDD format is applied, it is basically a multiple-carrier (MC) TDMA/TDD technology.

### 3.2.3 Main Features

The main features of the DECT standard are:

- Dynamic channel selection, a process whereby the portable continuously scans the environment and dynamically selects better channels when they become available;
- Seamless bearer *(or* channel) handover, the undetectable handover from channel to channel or from cell to cell;
- Two-way call setups, both call originate and call receive;
- Roaming, which is the ability to make or receive calls anywhere in the radio coverage network;
- Authentication and encryption, which provides high-level security.



*PP=Portable part*

RFP=Radio fixed part

SYNC=Synchronization

CTRL=MAC layer control data

CRC=Cyclic redundancy check bits

X=Check bits

GS=Guard space(equals 52.1ms or 60 bits)

**Figure 3.2** TDMA frame and slot structure for DECT(or carrier only)

These features emphasize the unique capabilities DECT as a standard offers.

However, because DECT is specified to provide cordless access to a number of host networks, not all of these features may be available in the applications expected to be on the market in the coming years. For example, a DECT residential set may provide high voice quality and many additional features, but handover is not required in a single- cell environment. Also, roaming in a DECT-telepoint application will be difficult, as long as DECT-telepoints are providing access to the current PSTN.

### 3.2.4 Idle State

Each RFP in the system is always active on at least one time slot. This can be a traffic slot(i.e., one that is being used for an ongoing call between an RFP and a PP) or a so-called dummy slot.

Both traffic slots and dummy slots contain system and RFP identification. In idle state, a PP scans on a regular base the available time slots and locks to the RFP that has the strongest field strength (and belongs to its own system).

Whenever another valid RFP gives a higher field-strength the PP will lock to the new RFP (although some hysteresis is built in to stabilize the system).

### 3.2.5 Call setup

If there is an incoming call for a specific portable, a paging message containing the portable's identification will be sent on the signaling channel of all the active time slots (traffic slots and dummy slots) in the system. This message will be read by the portable. If the portable is locked to a dummy channel, it will send a call request in the corresponding time slot in the second half of the TDMA frame, addressing the RFP to which it is locked.

If the portable is locked to a traffic channel, it will take the best time slot available (with the lowest measured field strength) in the first half of the frame and then send a call request in the corresponding time slot in the second half, addressing the RFP it was locked to in the idle state. (The DECT standard allows for different call-setup procedures as well). After the portable and the RFP control logic have agreed on the time slot to be used, the RE will switch the incoming call to the appropriate RFP and time slot. In case an outgoing call is initiated from the PP. a call request is sent in the same way as for the incoming call. After the portable and the RFP have agreed on the time slot to be used, the RE will allocate a speech channel to the call and send out the dialing information to the network interface.

### 3.2.6 Handover

The principle of seamless handover can be explained by using a simplified model of a single carrier system with only two cells RFP1 and RFP2) and two portables (PP1 and PP2). Assume the situation illustrated in Figure 3.3(a). PP1 is in conversation with RFP1 using time slot TS2. a traffic channel. PP2 is in idle state and is locked to RFP2 using time slot TS5, a dummy channel. The dummy channel on TS5 is also monitored by PP1, which is geographically somewhere between RFP1 and RFP2.

Apart from the time slots to which they are locked, PP1 and PP2 will scan all the other 11 available time slots on a regular basis and have information on the status of these alternative time slots stored in memory. When PP1 movies from RFP1 toward RFP2, the field strength measured on TS5 will increase and at a certain moment become higher than the field strength measured on TS2, which will decrease. If that difference is above a certain value, portable PP1 will decide to initiate a handover.

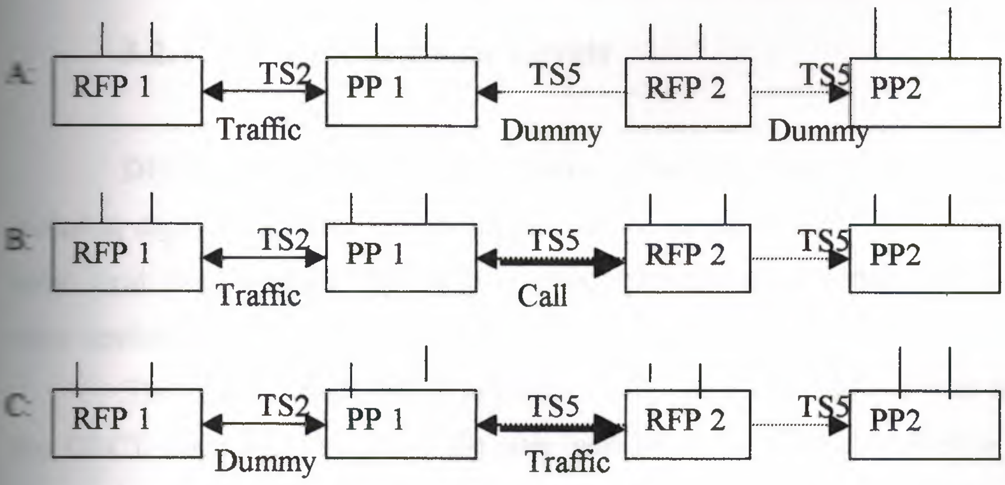


**Figure 3.3** A handover example

PP1 transmits a handover request on the next possible occasion in TS5 in the second half of the time frame. This handover request includes the identification of PP1 and of RFP2, the base that is addressed. RFP2 will answer in the corresponding time slot TS5 in the first half of (one of) the following frame(s).

After some specific signaling, PP 1 and the base station control logic of RFP2 will agree on the time slot to be used, which in this case will be TS5. (Note: If TS5 were a traffic channel instead of a dummy channel, the connection request from PP1 to RFP2 would have been transmitted on the time slot where the lowest field strength was measured by PP1 being the best channel.) During the time needed to set up a new channel to RFP2, PP1 maintains in parallel the existing channel with the ongoing call on TS2 to RFP1 (see Figure 3.3(b)).

When the new channel to RFP2 has been set up, the RE will be informed that a handover will be made, and the RE will then switch the ongoing call to the appropriate base station and time slot. This switching can be done without the user of PP1 noticing it because the old and the new channels overlap for a short time. After that, the channel to RFP1 will be released (see situation illustrated in Figure 3.3(c)). The handover described is called an intercell handover and is the most common type of handover. It makes sure that the system is always in a stable mode with all the portables locked to the nearest base station. No deterioration of the existing call quality will be detected before or after the handover occurs.

### 3.2.7 CI Conformance Levels

DECT caters for the standardization of a rather wide number of applications, including digital residential telephone sets; public access systems, such as telepoint and radio local loop; wireless PBX (sub)systems; wireless data networks; and a number of other applications.

The core of these DECT products is that the radio interface is as described in the DECT standard. Therefore, the user will be offered the choice of a number of interworking levels A well-defined level is called public access profile (PAP).

PAP is part of the DECT-CI-PROFILE family. This is a level of common interface (CI) conformance, whereby interoperability between equipment of different origin is catered for. DECT-CI also allows for proprietary additions (DECT-CI-

PROFILE-PLUS) In the case of PAP-PLUS, a manufacturer could add proprietary additions to the PAP interface. These additions may consist of, for example, nonstandardized features. However, within PAP many features are already standardized.

At a lower level of CI conformance, the DECT-CI-BASE has been defined. At its lowest level, equipment specified to meet the minimum DECT-CI conformance will be using the DECT PHL and some MAC-layer protocols. However, it is also possible to follow the DECT-CI-BASE on MAC, DLC, and NWK layers. Once again, the possibility is created to add proprietary additions.

In this way DECT is a standard that meets four very important requirements:

1 It allows for CI conformity, which will be beneficial both for cost-reduction as for faster market takeoff;

2 It allows for a multiple-operator environment, where a (large) number of uncoordinated systems (which may even address different applications) can coexist in the same physical environment using the same frequency band:

3 It allows for the deployment of vendor-specific (or operator-specific) product-technology additions, creating the opportunity to have product differentiation as well as a future flexible standard:

4 It provides for one and the same product for all of Europe (though differences in software applications are allowed for. creating an opportunity for low-cost volume manufacturing

## 3.3 APPLICATIONS WITH DECT

This section describes examples of residential, business, and public access applications of DECT.

### 3.3.1 Residential Applications

Residential cordless telephones provide the same facilities as fixed residential telephones but they enable domestic users to move around the house while dialing and when engaged in conversation. They have become widely used in a number of countries, notably the United Kingdom and the United States.

Residential sets are currently available that conform to the CTO, CT1, and CT2 standards. DECT-based products were becoming available in 1993.

It is interesting to note that the manufacturers of DECT-based residential cordless telephone sets have selected DECT as the basis for their products because of the cost advantages DECT brings. This becomes manifest in applications whereby one base station is handling more than one cordless telephone. The time multiplexing of calls, inherent in the DECT standard, offers an immediate cost advantage.

### 3.3.2 Cordless PBX

The primary aim of the DECT standard was to meet the need for cordless extensions on large PBX systems. The office worker uses a pocket-sized portable telephone, which provides all the facilities of a wired extension to the office PBX, wherever the user is on the premises. Every handset has its own unique identity, and its location is tracked by the PBX. The identity allows the handset to be called when an incoming call is directed to it.

The cordless PBX eliminates one familiar problem: telephoning someone who, while in the building, is not at his or her desk to receive the call. It is ideal for staff who by he nature of their jobs are difficult to locate, such as messengers, maintenance staff, and .warehouse staff. The cordless PBX also reduces the amount of telephone wiring needed in offices. This makes office reorganizations easier and reduces the administrative work-load. For example, when an employee moves to another office, his or her extension number does not have to be changed, nor does the telephone system need to be reprogrammed.

### 3.3.3 Telepoint or Public Access

Telepoint systems enable the subscriber who is in range of a base station either to make or to make and receive telephone calls. A telepoint installation that allows only outgoing calls can be compared to a public telephone box, but with fewer restrictions: the user is not confined to the call box when making a call and does not have to worry about having suitable coins or a credit card available. In theory, base stations will also be more widely available than public call boxes.

### 3.3.4 Radio in the Local Loop

Another potential application of cordless technology is *radio in the local loop,* or RLL. This application uses radio to make the final link between residential subscribers and the PSTN. This can have advantages for both the local network operator and the residential subscriber.

Hard-wired connections in the local loop are both expensive and difficult for network operators to install and maintain, whether provided as overhead or underground cables. To install a new connection, engineers need access to the subscriber's premises, and maintenance may result in a lack of service for a period of time, both of which are inconvenient for the subscriber.

The huge investment needed for local cabling is also one of the largest obstacles to truly competitive service provision in a liberalized telecommunications environment. Competitive services offer cost advantages to the residential subscriber and business opportunities to potential new network operators. No market forecasts for the introduction of cordless local ioop services have been made. The introduction of services will depend on the network operators rather than on market forces.

### 3.3.5 Personal Telephony: The Cordless Concept

Personal telephony involves three basic system requirements: a personal handset, a radio transmitter to communicate with user handsets, and a network with the intelligence to follow a handset wherever it goes.

As DECT is deployed in the coming years for residential sets, business cordless. telepoint, and RLL, we can expect the availability of many handsets and many radio transmitters in the market. This will definitely facilitate the startup of DECT-based personal communications.

However, to complete the concept of PCS, one needs a network with certain intelligent capabilities. These networks do exist. One of them, interestingly, is the GSM network (not to be confused with the GSM access part). Another option is to add databases to a digital network. This is happening, for example, in the world of private digital networks (PBX networks).

### 3.3.6 *Market Availability*

Because of the flexible nature of the DECT standard, that is, the fact that it can be applied for various cordless access purposes, we should expect manufacturers to focus on various applications.

Product availability was expected as of 1993, and some manufacturers have already launched DECT products. OlivettilSixtel's primary focus is on a wireless local area network (LAN). Siemens has started marketing a residential set (SC/MU) with intercom facilities. Ericsson is marketing a PBX add-on (MC/MU) system that creates a business PCS environment in, for example, hospitals, factories, and offices. Virtually all manufacturers announced products for availability in 1993 and 1994, ranging from low-cost consumer products to sophisticated PCS access products.

All these products comply to the DECT standard as completed and ratified in 1992. With type-approval common technical regulations (CTRs) 6 and 10 finalized by mid-1993, nothing is stopping DECT from becoming a successful example of market-oriented standardization.

## 3.4 PCS IN NORTH AMERICA

Whereas in Europe the focus has been on standardization of technologies (in particular GSM and DECT), the United States has adopted a different approach.

The Federal Communications Commission (FCC) has allocated a range of spectrum for licensed and unlicensed PCS. Two bands are allocated for major trading area (MTA)

PCS services:

The A-band (1850—1865 MHz and 1930—-1945 MHz) and the

B-band (1865—1880 MHz and 1945—1960 MHz). For basic trading areas (BTAs), of which there are 492 in the United States, 5 bands (C-G) are identified.

The C-band is two times 10 MHz (1880-1890 MHz and 1960—1970 MHz), and the

D, E, F, and G bands are contiguous two times 5-MHz bands (2130—2150 MHz and 2180—2200 MHz).

For unlicensed PCS, 40 MHz is allocated, for both voice and data.

At the time of writing, the FCC Notice of Proposed Rule Making (NPRM) was still being debated, and it is therefore difficult to draw conclusions. However, the nature of the PCS allocations, both for licensed as well as for unlicensed services, seems to allow for DECT or DECT-like technologies to be deployed.

In 1993, Ericsson and US WEST started a field trial for PCS, based on DECT cordless access products. The trial was scheduled to start toward the end of 1993 in Boise, Idaho. Initial results indicate that DECT is a likely candidate for providing local mobility and PCS.

## 3.5 CONCLUSION

The revolution that cellular communications has aroused will find its logical sequence in achieving a world of personal communications. In this respect, radio technologies play an important role. However, the challenge in current radio communications is to offer high-density solutions without compromising voice quality.

This is exactly what has been achieved with the DECT standard. The standard offers ways to provide cordless access to host networks for a wide range of applications. DECT will prove to be as important to achieve the goal of PCS as cellular has been.

# CHAPTER 4

## PCN SERVICE AND ITS IMPLEMENTATION USING DCS1800

Personal communications is not defined by a specific technology; rather, it is described features a user would wish for from an individual telecommunications service.Although a single definition is not possible, the features sought by most people can be encompassed by a common vision. The objective of a personal communications network(PCN) is to meet this vision as fully as possible and bring the mobile phone to the mass market.

Mercury One-2-One launched its service in the United Kingdom in 1993, and can thus claim to be the first operator to establish a commercial PCN service. The initial coverage was of Greater London (within its orbital motorway, the M25), but it will extend over the whole of the country by around the turn of the century. The system implementation is based on DCS 1800, a variant of the GSM standard providing for operation in the 1800- MHZ band.In this chapter we see how the features defined for the DCS 1800 standard have enabled Mercury One-2-One to realize a service that embodies its perception of the personal communications vision.

## 4.1 MARKETING DRIVE

Market research reveals a consistent set of features that form a vision of personal communications recognized by themajority as representing their ideal individual communication system.However, any practical technology will favor some attributes at the expense of others.Thus, PCN sets out to satisfy the most important aspects from a low-cost base.In addition,where compromises have to be made, solutions that can be improved over time from predictable technology advances such as better semiconductor devices are sought. For example, it is considered more acceptable for early handsets to be slightly larger or to provide less than the desired battery life rather than for the network never tc be able to offer contiguous coverage.

PCN is essentially a single service that replaces mobile, cordless, and fixed phones with individual pocket or handportable phones.The emphasis is very much on the handportable and not the mobile car phone, although phones are expected to work if the user is in a vehicle, and car adaptors are an available option.

The network provides high-quality speech, ideally as good as that of the fixed public switched telephone network (PSTN).This requires good-quality voice coding with little degradation from the mobile network.Thus, PCN radio coverage must be very good,with its service area covered contiguously with an adequate radio signal strength.The radio coverage supports handsets both outdoors and in buildings.The geographic coverage is targeted on built-up environs and regularly visited areas such that there is a simple marketable proposition to the customer that the phone will work within a clearly specified area."Phones for people, not places" and "The mobile phone for everyday, for everyone" are more than just useful slogans; they are the keystone of the PCN *philosophy, which is to treat people as individuals by aligning the* telecommunications network to suit their specific needs.

PCN aims to create a mass market for mobile phones.Any restrictions or complications in the ways in which the phones can be used will limit its take-up.This means that the handset should always be able to make or receive calls anywhere within its service area, with its basic method of use identical to that of a conventional fixed phone.*In addition, calls once established should be maintained whether the user is* stationary or *mobile.*Other *features provided as enhancements to these basic functions* can include alerting lights or tones associated with cheap tariff zones and call waiting. A particularly attractive service is an integral voice-mail within the network, which provides two important features:

- There are times when calls to a personal phone can be an intrusion; for example, during important meetings or the theater. If the call is diverted to a voice-mail system and an alerting light set off on the handset, the message can be accessed at a more convenient fime.

- If the PCN phone is outside its geographic coverage area, incoming calls can still be completed by the voice-mailsystem.When the phone returns to the radio coverage area, a message waiting light is activated on the handset, and the voice-mail box can be accessed.

The benefits of a fully mobile pocket phone are clear, but for widespread acceptance the cost of usage must be low. The key is to put in place a low-cost infrastructure using economies of scale to aid its implementation and high levels of usage to spread fixed costs over many calls.Unlike conventional mobile cellular radio, the costs of interconnection to the PSTN for completing the delivery of calls to and from fixed telephones, are negotiated to be similar to fixed telephone rates, and use local and trunk bands. In contrast, previous implementations of mobile cellular have treated all calls as long distance trunk calls with high interconnect rates, which lead to high tariffs for the service.

The handset is the customer's direct contact with the PCN, and its attractiveness has a major effect on the potential purchase of the service. Size, weight, and ergonomic appearance must all be considered.The physical length of any telephone is governed by the distance between the mouth and the ear, although flip-phones can fold to a shorter lenght for carrying.However, the overall weight and volume are determined principally by the size of the battery. With today's technology for digital phones, the batteries required for a full day's usage, which consists of interminently making and receiving calls and conntinuously remaining affiliated to the network, are larger than ideal. As the powerconsumption of semiconductors continues to fall with succeeding generations of submicron feature sizes and higher-capacity(nickel hydride) batteries become widely available,handportables will reach the point where further reductions in size and weight are of diminishing value.

## 4.2 PCN STANDARD REQUIREMENTS

To meet the functionality required by the vision of personal communications, the only suitable technology basis is that of cellular radio. Fixed networks can provide personal mobility, such that users can use any access point, but some form of radio access is needed for terminals to be portable.Cordless technologies can be used to provide radio links to access points on a fixed network.Examples of cordless telephones with defined air-interface access *are CT2 and DECT ,but these standards do not define* the routing, switching, and service functions that are provided by the service network.

How ever, cellular network standards define complete telecommunications networks, including full terminal mobility, such that handsets are continuously affiliated with the network, and handover takes place from cell to cell such that handsets maintain calls even when highly mobile.

A further advantage of using cellular rather than cordless technology for PCN is in the range of cell sizes.Cordless access technologies have been designed only for quite small cells (up to 200m) and "stretching" the cells is difficult. In the case of CT2, range is limited by fast fading because there is no error protection on the speech channel. For DECT, the data rate (bit period =868 ns) was designed primarily for indoor operation,where delay spreads are short (typically 50 ns), and DECT does not have the necessary channel equalizer for greater delays.Cellular air-interfaces tend to be more complex and require more elaborate transceivers, but these are suitable for a wide range of cell sizes, indoors and outdoors, such that they can be used in small (high-capacity) cells and large (wide coverage area) cells.

The U.K. Department of Trade and Industry (DTI) required PCN to be based on existing standards produced by the European Telecommunications Standards Institute(ETSI), because doing so would enable early introduction of the service and encourage harmonization within Europe with the consequential advantage of market-size economies. In their PCN license applications to the DTI, the successful applicants proposed adapting the 900-MHz GSM standard for operation in the 1.8-GHz band (DcS1800). GSM was chosen because it provides a good match to PCN requrements, defining a complete digital cellular radio system incorporating these elements:

- Interfaces for radio, transmission, and switching networks;

- Network, radio link management, and location facilities;

- Large set of telecommunication services (aligned to the integrated services digital network, or ISDN);

- Support of cell sizes giving economical wide area coverage;

- Support of high-speed mobiles, including handover;

- Potential for use in the local loop;

- Defined interconnection to the PSTN.

At the same time, it was recognized that enhancements to the GSM standard were needed not only to translate its operation to the 1.8-GHZ band but to refine the standard for:

- Support of small, low-power handsets;

- Close-proximity working;

- Wider available frequency band (150 MHz compared with 50 MHz for GSM);

- Improved internetwork roaming capabilities.

One enhancement has been to support a multioperator environment by incorporating national roaming. international roaming, as defined by GSM, caters for mobiles belonging to a network visiting another country and receiving service from a network of that country. National roaming allows operators of an individual country to restrict roaming to selected areas of the visited network. The key feature of the standard is to prevent a mobile from remaining on the visited network when the home network is available.

## 4.3 DCS18OO RF ASPECTS

Before DCS 1800 could be developed, a frequency band of operation had to be established. The band 1710 to 1880 MHz was ratified as the allocation for PCN in Europe by CEPT and consists of two bands of 75 MHz each with a 20MHz separation *for the split duplex operation, providing a maximum theoretical capacity of* 375 *radio* carriers, each with 8 or 16 (half-rate) voice/data channels. It is three times the allocation to GSM in the 900-MHz band and is consistent with supporting the peak traffic densities anticipated for PCN. Initial allocations from this band have been made for DCS 1800 systems in the United Kingdom and Germany.

The RF performance requirements of a radio link are complex and interrelated. To arrive at a self-consistent set of specifications that meet system needs and can be implemented at a reasonable cost, a rigorous and methodical approach was needed. To determine the system requirements, a range of scenarios was formulated, defining the relative physical positions of mobile and base stations likely to be encountered in operational conditions. Other constraints such as the channel spacing, frequency reuse assumptions, and the band of operation were also included.

Six scenarios were examined:

1. Single mobile station (MS), single base transceiver station (BTS);

2. Multiple MS and BTS where operation of BTSs is coordinated (single operator);

3. Multiple MS and BTS where operation of BTSs is uncoordinated (multiple operators);

4. MS in proximity to another MS;

5. BTS in proximity to another BTS;

6. Proximity to other, non-DCS 1800 systems.

Limit conditions were selected that were likely to occur relatively frequently in PCN usage. The impact of each scenario on the radio performance requirements was assessed to identify the most demanding scenarios. This enabled the requirements to be determined from a purely system point of view. These were considered alongside the complexity and cost of implementation, and, where necessary, compromise specifications were reached.

The two issues that have the greatest impact on the RF specifications and their practical implementation are the power output of the MS and the requirements for closeproximity working. These ussues determine the majority of RF performance requirements, including blocking, spurious emissions, and intermodulation characteristics.

### 4.3.1 Mobile Power Class

The selection of the power class is a tradeoff between the requirements for small, lightweight handsets with good battery life, high-quality RF coverage in a range of environments, and the need to minimize the cost of the radio network. Increasing the power improves the range but has a variety of implications. It increases the size of the handset and may lead to greater problems in controlling wideband noise and spurious emissions, and the output RF filter needs a higher power-handling capability.

On the other hand, lowering the power means that more base stations will be required, and so the cost of the radio network increases. However, adding more base stations means that the network capacity is increased, which is in line with the idea of PCN as a mass-market service. After study of various options and following discussions between manufacturers and operators, the MS power classes were defined as 250 mW and 1W.

Apart from these consideration, the choice of low-power classes only for PCN was also taken to aid close-proximity working. Since PCN intends to use small cells and be a high-capacity service, it is likely that there will be MSs from another operator close to a BTS on full power. This places stringent demands on the MS and BTS performance, but these problems are alleviated to an extent by the use of a low-power class.

### 4.3.2 Close-Proxirnity Operation

In a high-capacity PCN, not only will mobiles be operating close together, but as a result of small radio cells (for capacity) and low base station height (to control interference), there is a high probability that mobiles will operate close to base stations. This is not so significant in a single-operator environment (scenario 2) since the mobile will be powered down as it approaches the base station. However, in a multioperator environment (scenario 3), as will occur in the United Kingdom, mobiles can potentially be on full power and close to a nonserving base station (the "near-far" problem). This places stringent requirements on mobile and base station RF performance, particularly in respect to blocking to avoid destination, spectra due to modulation and switching of the "TDMA burst structure, and noise and spurious emissions. A mobile near limit range would be transmitting at full power. This mobile may be close to a base station of a second network, which is receiving signals close to limit sensitivity from its mobiles. In this case, out-of-band emissions from these mobiles can desensitize the base station line receiver of the first network, thus reducing its range. The RF specification must protect adjacent bands of different operators, or the base station range may be limited and capacity reduced through excessive interference.

Similar issues arise with the collocation scenarios (4, 5, and 6). To determine the worst-case coupling between MS and BTS, a variety of physical conditions were considered, taking into account antenna height, gain, and MS-BTS separation. A figure of 65 dB for the worst-case MS-BTS coupling was chosen (given, for example, by an MS on boresight of a 1O-dBi base station at a distance of 3Om) and used to derive the RFI performance requirements.

## 4.4 DCS18OO RADIO INTERFACE

The radio interface, or air-interface, of GSM/DCS1800 uses "TDMA to provide 8 or 16 channels/carrier with a gross data rate of 22.8 kbit/s in each full-rate (8 channelslcarrier) channel and a frame periodicity of 4.6 ms.

To accommodate the needs of the radio channel and the various signaling and control requirements, a complex TDMA frame structure has evolved (Figure 4.1). A burst of data is transmined during each active time slot of the 8-channel TDMA frame. Each time slot transmits 116 encryped message bits while in the center of the time slot; 26 bits are used as a training preamble sequence for the equalizer of the receiver to create a "model" of the radio channel and counteract the effects of multipath time dispersion. At the end of each time slot, a guard period of 8.25 bits is provided to allow for uncertainties in the arrival time of TDMA time slots at the base station from mobiles at varying distances. Such a small guard period is made possible by the use of a timing advance control whereby a base station continually monitors a mobile and instructs it to advance or retard its transmit timing so that time slots arrive at the base station at an approximately correct time.

Control information is generally mapped onto time slot 0 within the TDMA frame and a 51-frame multiframe is created to further multiplex control information channels,Frequency correction and syncbronization data are delivered within the time slot 0 structure at periodic intervals.

Traffic channels may be organized as full rate (eight per TDMA frame) or half rate, the latter being generated by using every other frame for information pertinent to the given traffic channel. It is possible to mix both full-rate and half-rate channels within a frame, although clearly a given time slot can be used only in full-rate or half-rate mode at any particular time.

The full-rate speech coder operates at a net rate of 13 kbit/s. Speech data are then heavily protected against errors by channel coding that takes the gross data rate up to the 22.8 kbit/s of the full-rate channel. The channel coding takes account of bit

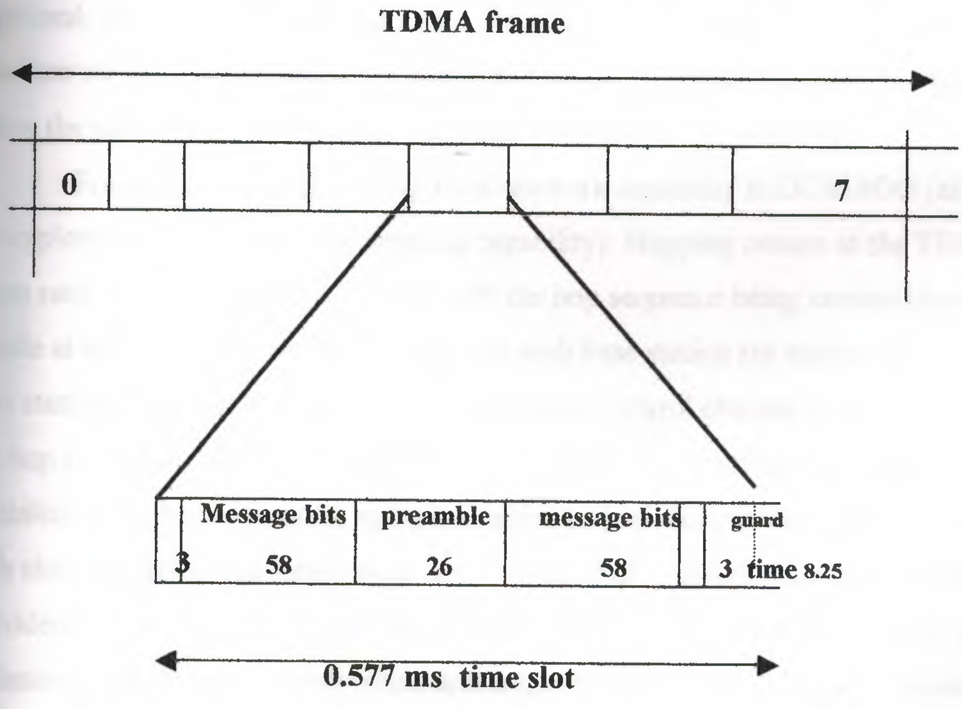


**Figure 4.1** TDMA frame structure

significance in the speech coder, and interleaving of the data across eight TDMA frames is also applied to minimize the effect of short error bursts on the radio channel.

The TDMA structure is also used by the mobile to decode signals from a number of surrounding base stations during a call (this is done in a sequential fashion) and report back to its current home base station the signal-quality parameters it has measured. This information can then be used to provide a basis for computing handover options-measurement by the mobile providing a better up-to-date view of the radio environment than a sequential polling of alternative base stations.

The instantaneous data rate over the radio channel is 270 kbit/s. Gaussian minimum shift keying (GMSK) modulation is employed with a normalized bandwidth of 0.3,enabling a channel spacing of 200 khz to be used. At this data rate, multipath channel equalization is required, and an extensive measurement campaign has identified that equalization up to 16 ms of multipath delay is adequate for most practical cellular-PCN environments. (Note: It is clear that in mountainous environments delayed reflections of greater than 16 ms can be encountered; however, cellular engineering can, in general, eliminate or at least minimize the effect of such reflections. Once outside the equalizer range, it is necessary that the level of such an unwanted signal be kept well below the carrier- and interference-handling capability of the system.)

Frequency hopping is an optional network capability in DCS18OO (all mobiles are implemented to support the hopping capability). Hopping occurs at the TDMA frame rate, that is, around 217 hops/s with the hop sequence being communicated to the mobile at call setup and handover times. At each base station (or sector of a sectorized base station), one carrier supporting the broadcast control channel (in time slot 0) does not hop so that mobiles can always listen for commands. Frequency hopping provides an ability to further counteract multipath fading over and above that already achieved with channel coding and interleaving and antenna spatial diversity (which is generally provided only at the base station). In addition, frequency hopping provides for a better statistical distribution of interference, and it is anticipated that its use will enable efficient frequency reuse within the cellular radio network.

## 4.5 DCS18OO NETWORK INTERFACES

The architecture of a GSM/DCS18OO network is illustrated in Figure 4.2. The figure shows a set of subsystems and interfaces that are defined in detail in a series of ETSI recommendation [1]. The key features of these recommendations are the description of open interfaces to the OSI framework and the use of ISDN standards for signaling and network functions. The interface approach gives manufacturers flexibility of implementation while allowing operators flexibility in equipment procurement.

The base station controller (BSC) controls and manages a number of base transceiver stations (BTSs) by providing the lower-level control of cellular functionality. ISDN LAPD signaling protocols are used within this base station subsystem and over-the-air interface.

The mobile services switching center (MSC) is primarily concerned with routing calls to and from mobile stations. The home location register (HLR) contains the customer information required for call routing and administration, including class-of-service data

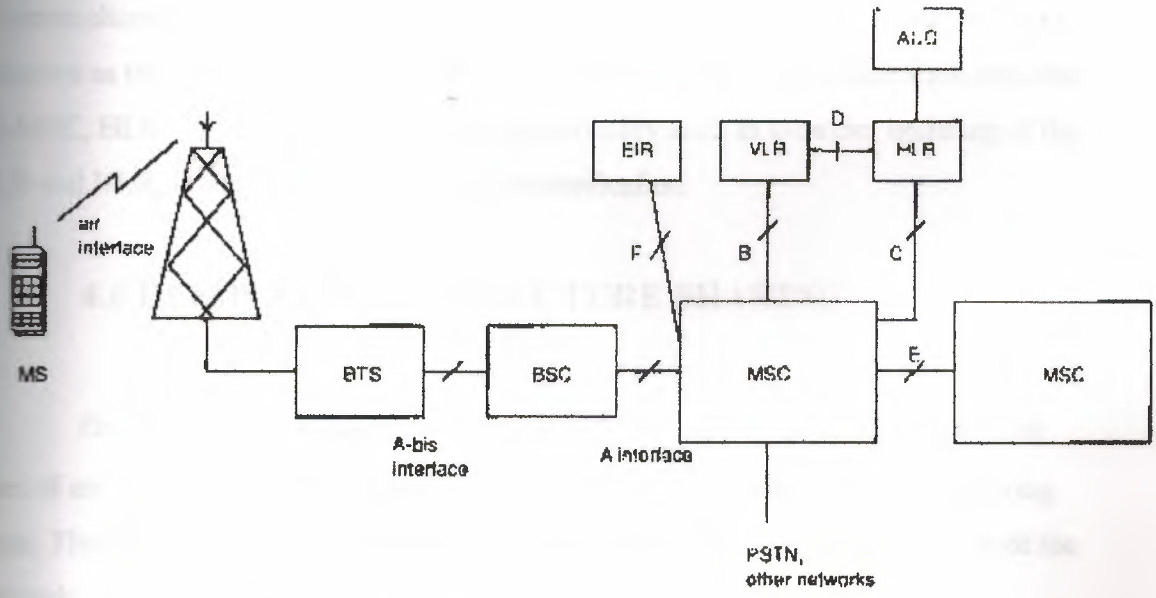


**Figure 4.2** DCS 1800 network interfaces

Identifying which services a particular customer is allowed access. Associated with each MSC is a visitor location register (VLR), which stores information, including detailed location data, about all mobiles currently active within that MSC's area of control.

Network access is controlled by algorithms that carry out rigorous authentication of the mobile stations. The equipment identity register (EIR) provides an up-to-date check on the validity of mobile equipment, while the authentication center (AuC) checks the validity of the subscriber idenfity module (SIM). A feature of GSM/DCS 1800 is that access to the network is granted through a SIM, which is generally mounted on a smart card plugged into the mobile station to personalize the equipment to a particular customer. Security is provided by the use of challenge/response pairs of signals for authenticating access to the network and encryption keys for decoding enciphered speech, data, and other signaling passing over the air-interface. All speech is digitally encoded at 13 kb/s (full-rate codec). A cryptographic algorithm, A5, produces ciphertext out of cleartext using a common cipher key (Kc). Kc is produced by an algorithm, A8, based on mutual agreement between the mobile station and the fixed part of the system. An algorithm, A3, produces a signed response to a challenge to authenticate that the user is a valid subscriber. The algorithms A3 and A8 are contained in the SIM that holds security and other subscriber-related information.

Network signaling between major elements makes extensive use of the CCITT common channel signaling system no.7 (C7). The extension to C7 for mobile networks, is known as the mobile application part (MAP). MAP supports communication between the MSC, HLR, VLR, and EIR providing funcfionality such as location, updating of the HLR and VLR, inter-MSC handover, and authenficafion.

## 4.6 DCS18OO INFRASTRUCTURE SHARING

One of the differences between GSM and DCS 1800 is that the Smaller Cell sizes of an 1800-MHz network could make the service financially unviable in outlying areas. Therefore, a new roaming approach has been developed to reduce the cost of the network.

### 4.6.1 National Roaming

A key enhancement of the specification of DCS 1800 has been the incorporation of national roaming. Roaming refers to a mobile of one network receiving service from another.Nafional roaming allows operators to restrict roaming in a single country to specific areas. This service is additional to the normal internafional roaming capability of GSM, which caters for mobiles belonging to one network visiting another country and receiving service from a network of that country.

National roaming was designed to deal primarily with the situation where multiple PCN networks are being deployed in a country but individually do not provide nationwide coverage. The aim is for mobiles to automatically switch between networks according to availability of coverage but return to their own (home) network when coverage from it becomes available. This gives the user a wider coverage area and reduces the cost of the networks by sharing between operators. The manner in which this is achieved is as follows.

The network is divided into location areas to allow the network to track and page mobiles efficiently. The size of the location area is set by the operator, and this feature provides a useful mechanism for implementing national roaming. Figure 4.3 shows the areas of coverage of networks A and B whose operators have reached a national roaming agreement.

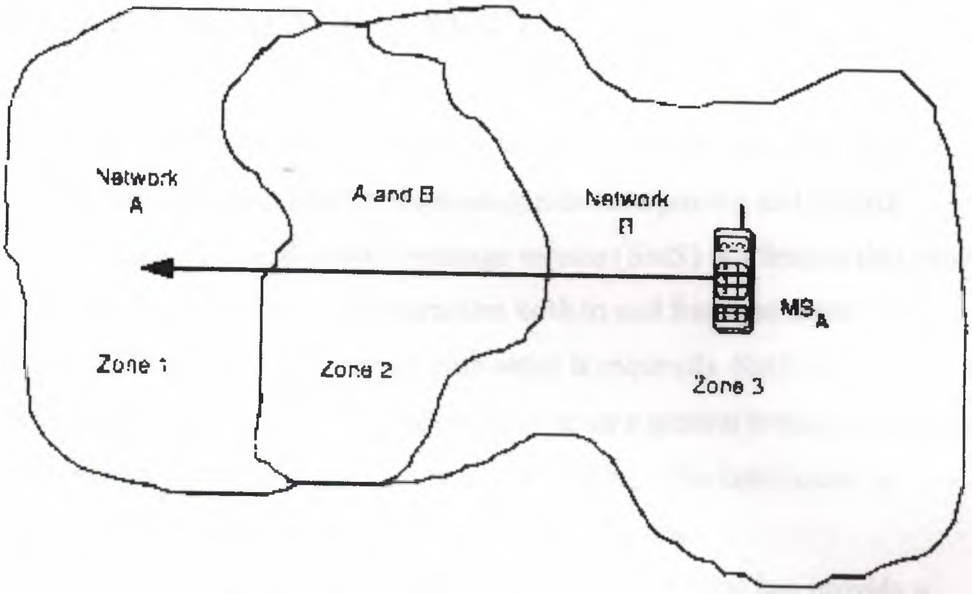


**Figure 4.3** Natiol roaming

Three zones are defined by the respective location areas of each network. A mobile station belonging to network A (MSA) starts a journey in zone 3. It is located in a 1ocation area in zone 3 and receives service from network B. When MSA moves into a location area of network A in zone 2, where coverage is available from networks A and B, the request by MSA to network B to update the location area is rejected, causing the mobile to search for and to access its home network. This is the key step; without the national roaming enhancements, the mobile would remain on the visited network B until it lost coverage from it, that is, until it reached the boundary between zones 1 and 2. While MSA remains in zones 1 and 2, it continues to receive service from its home network. These operations take place without intervention from the user and extend the coverage for MSA by the area of zone 3.

This type of operation reflects one of the underlying principles of GSM/DCS 1800 that, wherever possible, a mobile should receive service from its home network, that is, the one subscribed to by the user. In areas where coverage is available from more than one network, the aim is to minimize the time that a mobile is not served by the home network and as part of the network of the phase 2 and phase 2+ standards programs, new procedures are being defined to achieve that aim optimally.

## 4.7 SHORT-MESSAGE SERVICE

The DCS 1800 standard provides a structure for delivering a full range of telecommunications voice and data services using modem signaling and control structures. In addition to this, the short-message service (SMS) is a feature that provides for delivery of messages of up to 160 characters both to and from the mobile in a connectionless manner (that is, no speech path setup is required). SMS may be delivered both to addressed mobiles (point-to-point service) or on a general broadcast basis from individual or groups of base stations (cell broadcast mode). This latter mode is particularly useful for general or localized informafion services.

In the PCN environment, messaging (both voice and data) can provide a powerful complement to the high-quality voice mobile service. SMS functionality, linked to voice messaging systems, opens up a new vista of service opportunities and will be a major feature of the DCS 1800 service offerings in the future. One simple example is the delivery of a voice message waiting signal to the mobile, which is sent when the mobile reacfivates into the network, indicating without intrusive interruption that a message has been left while the mobile was unavailable. Such a feature-and there are many variations of voice and data messaging that can be exploited-begins to put into customers' hands a telecommunications product over which they can exert control and yet be given the assurance of being contactable.

## 4.8 IMPLEMENTATION OF PCN

Although the elements of a mobile cellular network and PCN are similar, the ways in which the networks are implemented can vary significantly in order to create their different market objectives. Traditionally cellular networks were initially deployed with as few cells as possible to provide coverage just over areas frequently visited by mobiles,for example, city centers and motorway corridors. Cellular tariffing has little call-distance structure and comparatively high charges, and it is positioned as a premium service ideal for those requiring wide-area mobility. As the business develops, enhancement of coverage quality and capacity can be financed by the revenue from the existing customers. The better coverage increases suitability for handportable users. Eventually the network can be used for other types of customer, for example, someone desiring occasional emergency service can be offered a package with lower ownership charges and very high usage charges, because the network build costs have already been paid for by the principal users.

PCN operators seek to offer high-quality communications with a customer base requiring contiguous coverage over the community of interest where the service is being sold. In general this community is at least a city plus commuter environs covering hundreds (possibly thousands) of square kilometers. PCN requires a very large initial investment to ensure that the network quality meets the marketing requirement from launch. By building the "final" network at the outset, the total costs are less due to economies of scale in manufacturing and deployment and also due to avoiding the need for expensive upgrading, cell splitting, cell replacement, and replanning commonly experienced in evolving cellular networks. However, because none of the initial network can be financed by revenue from users, PCN requires long-term investment commitment from its backers and recognition of the considerable period before profitability.

The tariffing of PCN must be suitable for a mass market. Although a premium is possible for its mobility advantages over the fixed phone, when used near the user's home the increment over PSTN rates should be small while local and trunk rates should be supported. This requires interconnection between the PCN and the PSTN at sufficient points to access the different tariff bands. Interconnect rates have to be agreed on by the PSN and PSTN operators such that they can cover their costs for their parts of delivering calls across the two networks. By deciding to make only a small profit margin per call or by offering innovative tarif packages such as free off-peak local calls, PCN rates can encourage high usage and achieve profitability from volume.

DCS1800 has provided telecommunication operators with an opportunity for the initial step into the PCN marketplace:

1- The core network and mobile elements were based on the GSM 900 technology, which was in production and entering public service.

2- Radio technology to implement the 1 800-MHz operating frequency was available.

3- The DCS 1800 standard was optimized around the handportable product with both low-power portables and base station technology.

4- The characteristics of the 1800-MHz operating band results in a small cell structure that is compatible with the PCN concept.

5- The 1800-MHz band is, in general, occupied by fixed radio links for which alternative technologies exist, and clearance of the band could be more readily effected than attempting to manage coexistence and transition between first- and second-generation cellular systems at around 800 MHz to 900 MHz.

The DCS 1800 standard represents the technical foundation for the implementation of the network, and as such it provides for a wide range of options and design variants suitable for PCN. However, the specific network design and implementation are equally important in determining the quality and type of service actually offered to customers. A comparison of the different implementation provisions between "traditional" mobile cellular radio and PCN is shown in Table 4.1.

## 4.9 PCN RADIO NETWORK DESIGN

The initial implementation of PCN is based on provision of a high-quality small-cell network (cell radius from less than 1 km in a dense urban environment to 5 km in a rural environment). Radio coverage and system parameters are optimized for the low-power handportable, and emphasis is on generally providing a significantly higher statistical call success and quality level for the handportable than current cellular networks can provide. Coverage targets are set for both indoor and outdoor usage.

The radio cellular design requires the establishment of a suitable radio link path budget; a typical calculation for DCS 1800 is set out in Table 4.2. A 1W (peak) handportable

### Table 4.1

Comparison of Traditional Cellular and PCN Implementation

| Tradional cellular | PCN |
|---|---|
| Optimized to mobile | "Phones for people"<br>Mass market economies of scale<br>Handportables<br>-Network build<br>Greater self-provision of links<br>Common handset specification<br>-Prioritizing market offering<br>Advanced but simple-to-use features |
| Wide-Area outdoor service | Combination of cordless and cellular attributes<br>In-building and outdoor coverage<br>Microcellular techniquesfor high capacity |
| Trunk PSTN intrconnection | PSTN interconnection aligned with coverage |

**Table 4.2**

Typicall DCS 1800 Radio Link Budget

| | |
|---|---|
| Mobile peak output power (1W) | +30 dBm |
| Effective mobile antenna gain | -3 dBi |
| BTS antenna gain (sector) | +17 dBi |
| BTS feeder loss | -2 dB |
| - (BTS receiver sensitivity) | 104 dBm |
| Overall (nonfading) path loss | 146 dB |

is assumed, and the "effective" mobile antenna gain reflects the relatively low gain and efficiency obtainable from the antennas of small handportable transceivers.

The radio network designer depends on the diversity capability of the DCS 1800 system with its combination of time and diversity to frequency diversity within the scope of the standard and the effectiveness of BTS antenna spatial cope with the fading environment that the mobile experiences.

In the dense urban environment, cell implementation is best effected using traditional sectorized structures typically using 120-degree sector configuration; this generally provides for optimal radio coverage with a high-gain directional sector antenna. Spatial diversity on the BTS receive antenna is necessary to provide a balance between the higher-power BTS dowlinknk and the mobile uplink. Frequency efficiency is also optimized with the sectorized structure. DCS 1800 has a carrier-to-interface ratio (C/I) of around 12 dB for a good-quality speech, significantly better than existing first-generation analog systems. As a result, more efficient frequency reuse structures can be implemented. A theoretical cell frequency repeat pattern approaching four is within this

C/I capability, and with the application of frequency hopping even tighter reuse may be contemplated. It is likely,however, that the practical issues of BTS location and interference propagation characteristics are such that the deployment of such tight reuse arrangements will be impossible in the PCN small urban cell environment. Microcell arrangements can, however, be used, creating exceptions to frequency reuse structures with both base station and mobile operating at lower than normal power levels.

Microcells are small cells whose base station antenna is below rooftop height, so that the RF coverage is confined to a small area. The next stage of evolution may include such microcell structures for coverage and capacity enhancement into buildings where large numbers of people gather, such as airport terminals, railway stations, and shopping malls. A forther development would then be the exploitation of "private" cells within offices to provide internal business communications.

Ubiquitous deployment of microcells in a PCN environment requires a very fast handover-processing capability, which was not initially available on DCS 1800. However,it is practitable within the first phase of the standard to exploit isolated microcells within the general macrocell environment by careful attention to handover parameter selling, that is, only allowing calls to originate within the microcell and using the overlaying macrocell as the single target handover candidate.

High-quality coverage and grade of service demand advanced, efficient radio network techniques as well as a sufficient spectrum allocation. The air-interface is in effect a traffic concentrator where blocking can occur just as in other parts of the fixed network. Layered cell hierarchies in which a layer of macrocells is overlaid by a layer of microcells located at traffic peaks cap offer substantial increases in traffic capacity [2]. This approach makes efficient use of the scarce radio spectrum and, when allied to the 2 x 75-MHz potentially to PCN, will provide for very high capacity systems.

The microcell can be used to increase the capacity of the network because it permits greater frequency reuse and can provide many channels in a small area. However, for contiguous coverage a layer of macrocells is also required. Before microcells can be implemented, they need the development of small base stations and new design techniques, which require advances in technology and enhancements to the standards. The classic problem is the risk of dropping calls from high-speed mobiles when they leave the microcell's coverage, for example, when they turn a corner and become shadowed by a building.An enhancement has been developed for Phase 2 of the

DCS 1800 standard whereby stationary and slow moving mobiles are encouraged to access the microcell, mobiles while ensuring that fast-moving mobiles remain served by macrocells, as shown in Figure 4.4.

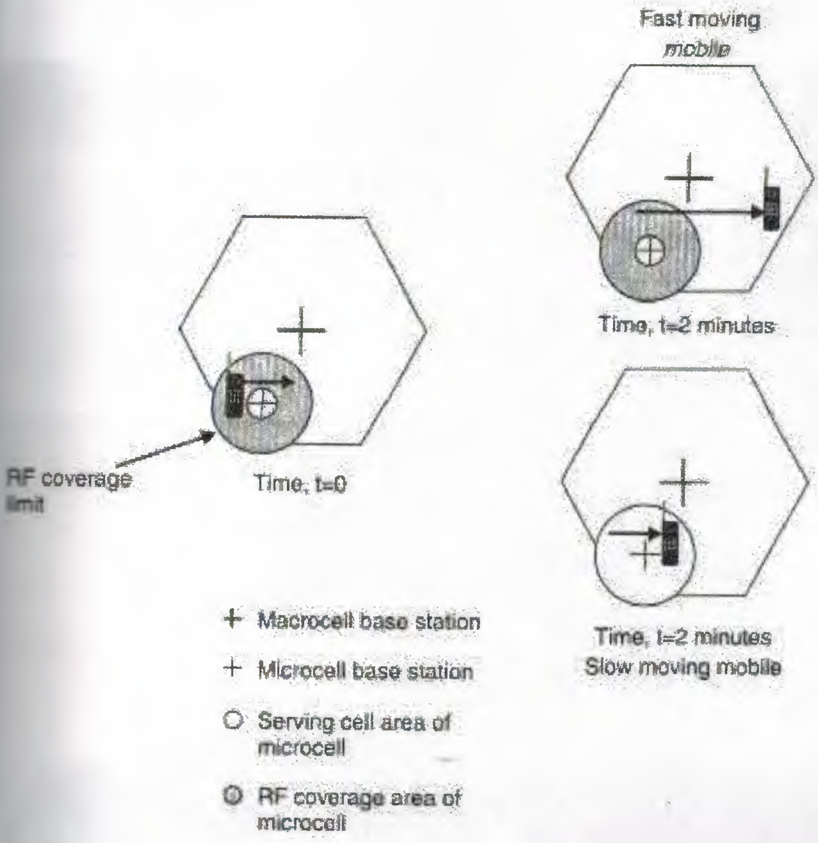


**Figure 4.4** Microcell handover

A timer mechanism is implemented in the mobile such that when the mobile first receives radio coverage from the microcell, the effective serving cell area is deliberately minimized. If the mobile is still within the microcell coverage area after a penalty time of ,for example, 2 minutes, the serving area is increased. In the case of the high-speed mobile, it has already left the coverage area of the microcell and therefore continues to be served by the contiguous macrocell coverage layer.
However, the slow-speed mobile is still within the microcell coverage area and it selects the microcell for its service. This simple mechanism distinguishes the majority of high-speed from slow-speed mobiles.

**Figure 4.5** Typicall antenna

Outside the urban environment, the same pressures on capacity and frequency efficiency do not apply. In addition, environmental considerations relating to antennas and towers are increasingly a consideration for planners. An omnidirectional antenna arrangement is likely to provide the most effective solution, and technology is now able to provide relatively high-gain (12 dBi) omnidirectional antennas with good beam patterns. Lightweight towers can be used in "green field" situations, and a solution providing excellent radio performance may now be combined with an environmentally acceptable implementation, an example of which is shown in Figure 4.5. Two antennas are used for receiving diversity with a duplexer to permit one antenna to also serve as a transmitting antenna. The spacing of around 5m gives adequate transmit-receive isolation and sufficient separation for spatial diversity in the multipath conditions of rural areas.

## 4.10 PCN TRANSMISSION NETWORK

A transmission network is required to link radio cells to the BSCs and MSCs. The network should provide a sufficiently high availability to achieve a high-quality network. On a link-by-link basis, the required availability level differs since it is clearly less important to lose a single cell for a short period than a considerable portion of the network. The simplest method of providing connectivity is a tree-and-branch structure, but this leads to the network being very susceptible to failure of the higher multiplexed links.Resiliency can be improved by hot standby parallel paths or ring structures, although these must be of greater capacity and include equipment capable of rerouting.

If microwave links are designed to have an availability of 99.99%, then on average all links will be unavailable for 1 minute per week. The unavailability is primarily due to propagation outage, which in reality means there will be a 5- to 10-minute outage about six times a year spread over a 4-month yearly cycle (e.g., wet snow in January and February and thunderstorms in July and August) with a few random events at unpredictable times.

With its proportionately greater number of cells than a traditional cellular network the PCN network is particularly sensitive to transmission costs. Even if the costs of cabling to PCN cell sites were not prohibitive, availability of duct space is generally not enjoyed by new PCN operators. Key, therefore, to the implementation of PCN is access by the operator to high-frequency microwave and millimeter wave radio capacity for linking cell sites back to switching centers.

The macrocell and microcell dimensions are such that, rather than laying costly underground cable links, millimeter-wave hops become an attractive proposition.In the United Kingdom, the DTI is allowing PCN operators to use the 38-GHz and potentially 55-GHz bands for this purpose. These links can be used for ranges up to a few kilometers. The general architecture of the PCN transmission network is shown in

Figure 4.6.Cell sites are linked to higher-order nodal points by "daisy-chain" or star configurations. Clearly, the most cost-effective solution is to use the cell sites wherever possible as the first-stage transmission nodal point, and the selection and implementation of cell sites should be driven as much by the transmission connectivity (e.g., line of sight) needs as by the cellular radio engineer's requirements for radio coverage.

Point-to-point radio link equipment operating at 38 GHz is now available at low cost, and this provides the most cost-effective solution to the first stage "hop" from a cell site. Such equipment can operate on links of a few kilometers, with small (30 to 60 cm) dish radii-again, compatible with the environmental considerations of cell-site implementation.

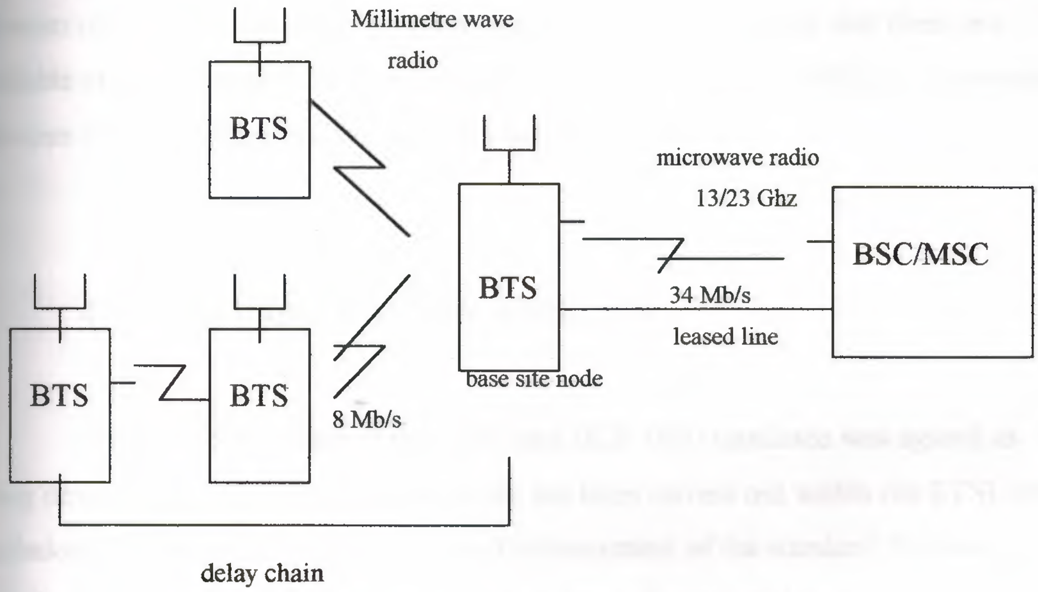


**Figure 4.6** Transmission network architecture

Because of the short-range nature of the links and the imperatives on low-cost implementation, relatively simple digital radio link equipment is used. Simple 2- and 4-level FSK/PSK modulation systems, while not the most bandwidth efficient, provide high reliability and low cost because of their simplicity. Link frequency planning is a challenge because of the regular grid nature of the cellular network, although in general the natural distortions of the grid due to practical site location issues diversifies beam patterns sufficiently to enable effecfive frequency reuse to be achieved.

With the DCS 1800 speech coder, each transceiver requires only three 64-bit/s time slots including signaling needs. Thus, transmission links from a cell site supporting up to 9 transceivers (around 66 full-rate speech/data channels) at 2 Mbit/s or 36 transceivers at 8 Mbit/s can be implemented. Using 38-GHz radios, a channel of 7 or 14 MHz is required and experience to date has shown an overall bandwidth requirement of around 2*200 MHz for a large city and its surrounding commuter environs is adequate for links to connect the radio cells.

In a tree-and-branch architecture, there is no route diversity from any network node, although resiliency can be improved by 1+1 hot-standby radio equipment. However, due to radio outage being primarily due to occasional adverse propagation conditions, an alternative to radio is the best means of improving network resiliency. By adding route diversity fiber (typically leased from a public telecommunications operator, or PTO),extremely reliable paths can be created due to the lack of correlation between route failure mechanisms. However, it is difficult to ensure that fibers are available at each critical node. Transmission network planning is a difficult compromise between the requirements of low cost and yet high resiliency.

## 4.11 DCS18OO ENHANCEMENTS

A common evolution of the GSM and DCS 1800 standards was agreed as being desirable,and a joint program of work has been carried out within the ETSI SMG Technical Commttee for the evolution and enhancement of the standard. Priority tasks included completion of work on desirable features and services that were not completed as part of the Phase 1 activities, particularly for support of a Group 3 facsimile service.New supplementary services, including call waiting, call hold, multiparty, line identification and closed user group, are being developed that will improve the PCN service offering.Optimization of the standards is taking place as results from early GSM operatio nal systems are becoming available. The trend toward smaller cells to increase capacity  particularly in dense urban areas, requires new techniques to support microcell environments. In addition enhancements have been proposed to the national roaming mechanism to make its implementation more cost effective.

The PCN operators have also supported the development of a half-rate speech coder which is a key component for still higher capacity networks. Two candidates have emerged with quality and delay similar to that of the full-rate 13-kb/s RELP GSM/DCS18OO codec but with implementation complexities around three times as great. It is predicted that this additional complexity will be matched by the anticipated advances in semiconductor technology in the next few years.

Third-generation systems should continue the move toward systems that fully meet the requirements of personal communications by offering services and features that are demanded by the market and that can be offered economically and competitively.Developers of standards for third-generation systems have opportunities to provide technical solutions to respond to the emerging and projected market needs but will also need to take into account the significant investments that many will have made in digital infrastructure for personal, mobile, and fixed network services. Consideration should be given to exploiting the reuse of existing standardization work and systems infrastructure where this is appropriate, particularly bearing in mind the expected large populations of personal communications terminals that will be in use at the time of the introduction of the next generation of systems. ETSI has acknowledged the need for a third-generation standard and is setting requirements as the initial step toward the standardization of a universal mobile telecommunications service (UMTS).

## 4.12 THE PCN VISION

It is generally accepted that the PCN vision is the provision of affordable communications with total freedom and mobility, ubiquitously available, and provided in a manner that puts the users in control of their communications. DCSI8OO provides a standard to deliver the PCN vision and has enabled Mercury One-2-One to launch the world's first PCN in London during 1993 with plans to continue its implementation over the whole of the United Kingdom by around the turn of the century.

## CHAPTER 5

# Personal Communication Services in the U.K. Cellular Enviroment

The present development of a wide range of public mobile telecommunications services in the United Kingdom is firmly based on the success of the two competing cellular telephone networks, which commenced operation in January 1985. Since that time both Cellnet and Vodafone have experienced phenomenal growth; at the beginning of 1994 they had over 1.9 million subscribers between them and were two of the largest mobile phone operators in the world. The competitive market has led to some of the lowest prices in Europe, with tariffs held constant outside London since service began.

The existing cellular networks are based on analog mobile radio technology developed by Bell Laboratories in the United States during the 1970s. This technology was adopted, with minor modifications to suit European frequency allocations around 900 MHz, as the U.K. total access communication system (TACS). As originally designed, the system was intended to support relatively high-powered mobile equipment installed in vehicles. From the earliest days in the United Kingdom it was anticipated that portable equipment would be increasingly used on the network. As the networks have expanded, handportable equipment has become much more compact, to the point that truly pocketable phones have become available at decreasing prices. The demand for portable equipment is such that 40% of phones in use are now portables, and the number of portables registered on the Vodafone network is actually increasing faster than the total number of subscribers.

*As the networks have expanded, cell sizes have decreased such that portable* equipment is adequately served over a large proportion of the country. In early 1994, the Vodafone network had about 800 (analog) cell sites with more than 30,000 voice channels service.

Although the cost of using a mobile phone continues to fall in real terms, it is still considerably greater than that of using a fixed telephone. The existing cellular networks serve a subscriber base consisting largely of business users, for whom the additional cost is justified by the benefit of mobile Communication.

The challenge for the future is to bring mobile communications to the mass market. The first step in this direction is the adoption of a common standard across Europe for a second-generation digital cellular telephone system. This system is known as GSM, an acronym that began as the name of a European committee and has since been somewhat grandly renamed the global system for mobile communication. This system will gradually replace a wide range of incompatible analog cellular systems across Europe during the 1990s. The European Community set an ambitious target of July 1991 for the opening of service of GSM networks. At the end of 1993, there were 23 working GSM networks in 14 countries serving 1.5 million subscribers. This is a remarkable achievement considering the development work that still remained to be done once the specifications for the system became stable in the late 1980s.

The GSM systems will operate in the same part of the spectrum around 900 MHz currently used by the TACS system. The initial allocation in the United Kingdom is of 2 x 10 MHz, expanding to 2 x 25 MHz when the analog networks are finally phased out in the next century.Already, some countries have identified a potentially greater demand for spectrum, and another 2 x 13 MHz is being suggested as an expansion band for GSM in the future.

Before the GSM systems had even begun operation, the U.K. government had licensed three operators to provide personal communications services, using a spectrum allocation of 2 x 75 MHz at around 1800 MHz. After some discussion about the technology to be used, the operators settled on a system firmly based on GSM technology, now standardized in Europe and known as DCS1800.

So what is the difference between a PCN and a GSM cellular network? In the remainder of this chapter, we will consider the similarities and the differences and the way that personal communications services will be provided by the existing cellular operators.

## 5.1 GSM and DCS18OO: SIMILARITIES AND DIFFERENCES

The differences in technical specifications between the GSM 900 and the DCS

1800 systems are relatively small. Both are based on identical modulation and signal processing functions and can potentially offer the same range of services. The most significant differences are summarized in Table 5.1.

It can be seen that the greatest difference is in the increased spectrum available to the personal communications network (PCN) operator. This gives tile operator greater flexibility in frequency planning compared to a GSM network and potentially a capability to serve a larger customer base in the long term. The GSM specification supports a range of equipment from low-power handheld to high-power mobile. The DCS1800 system has been specified from the start to support only low-power handportable equipment. This

**Table 5.1**

Major Differences in GSM 900 and DCS 1800 Specifications

| | GSM 900 | DCSI8OO |
|---|---|---|
| Mobile TX band | 890-915 MHz | 1710-1785 MHz |
| Mobile RX band | 935-960 MHz | 1805-1 880 MHz |
| Mobile TX peak power (maximum) | | |
| Class 1 | 20W (+43 dBm) | 1W (+30 dBm) |
| Class 2 | 8W (+39 dBm) | 0.25W (+24 dBm) |
| Class 3 | 5W(+37 dBm) | |
| Class 4 | 2W (+33 dBm) | |
| Class 5 | 0.8W (+29 dBm) | |

| | | |
|---|---|---|
| Mobile TX peak power (minimum) | | |
| Class 1 | +13 dBm | +10 dBm |
| Class 2 | +13 dBm | +4 dBm |
| Class 3 | +13 dBm | |
| Class 4 | +13 dBm | |
| Class 5 | +13 dBm | |
| RX sensitivity<br>(portable phone) | -102 dBm | -100 dflm |

removes a degree of flexibility in the range of services that can be provided compared a to GSM network. For example, a GSM network could be designed to allow handheld coverage in urban areas but full countrywide service in rural areas via the use of a power- boosting car adaptor. The slightly greater power control range of the DCS 1800 equipment and other detailed differences in transmitter and receiver performance specifications too numerous to mention here give the DCS 1800 system a small performance advantage when operating with a high density of subscribers.

Another small advantage of the DCS 1800 system is due to the fact that multipath fadding occurs more rapidly at the higher frequency for a given speed of the moving subscribers.Because the error correction system inherent in GSM and DCS 1800 is better at correcting randomly spread errors than bursts of errors, it is enhanced by an interleaving system that spreads out bursts of errors. This is made more effective at the slow speeds of a pedestrian by the higher fading rate at 1800 MHz.

In contrast, the GSM operator has a considerable advantage in path loss capability, and thus in the maximum cell size that can be achieved. The free-space path loss between isotropic antennas increases by 6 dB for a doubling in frequency. Additional losses due to diffraction also increase with frequency. The empirical propagation model derived by Hata [1] suggests an additional path loss of 7.7 dB at 1800 MHz. Since the release of spectrum for mobile applications is around 1800 MHz, many organizations have carried out comparative trials at 900 and 1800 MHz. Simultaneous trials in Aalborg, Denmark (2) showed a mean additional loss of 9.8 dB. Similar trials in Mannheim and Darmstadt, Germany, yielded a mean difference of 11 dB, although in one industrial area with large buildings and little vegetation the difference was only 6.4 dB. The difference in path loss in open rural areas will be lower; Hata [1] suggests 4.2 dB, but the penetration loss of trees in wooded areas will again increase the loss at 1800 MHz. So far, we have considered only outdoor coverage, but an important aspect of any truly portable service is coverage inside buildings. Data on building penetration loss at different frequencies have been gathered by many organizations. The vast variety in building construction methods, shapes, and sizes leads to a large body of data from which it can be difficult to draw clear conclusions. On balance, it seems that there is little to choose between the two frequency bands.

Overall, it is reasonable to conclude that a network operating at 1800 MHz will have a disadvantage of around 10 dB in path loss. Although some of this disadvantage can, in theory, be regained by the use of higher-gain antennas for a given physical size, this advantage will be difficult to achieve in practice. In a portable equipment it is difficult to achieve any significant gain, because the orientation of the antenna cannot be controlled. The large collinear arrays already used for base station antennas at 900 MHz typically consist of up to 8 dipoles. Any larger array would have an excessively narrow vertical radiation paflern and would have to be carefully manufactured to have more than a 1- to 2dB  advantage. The reduced receiver sensitivity of the DCSl8OO equipment is no disadvantage, because the base station power can be increased to compensate, the uplink power budget from the low-power handheld being the limiting factor. On the uplink, a class-1 DCS 1800 phone has a 1dB advantage over a class-5 GSM phone.

In conclusion, since a path loss reduction of 10dB corresponds approximately to a doubling of range, the reduced path loss at the lower frequency will allow a cellular network operating at 900 MHz to provide coverage to portable equipment with considerably fewer base stations than would be required at 1800 MHz. This is of considerable advantage to an operator attempting to roll out a network at minimum cost. It can be seen that although there are important differences in spectrum available and in the maximum cell size achievable, the two systems are technically very similar. What then is the difference between a "personal communications" service (PCS) and a "cellular" service, when even the existing analog networks provide substantial support for pocket portable phone users? The biggest differences between PCN services and cellular services and between different PCN services will be in the markets the operators choose to address and the way they target coverage and tariffs. The same technology can be used to provide a nationwide mobile service, a localized portable service, a system whose main aim is to bypass the local loop in supplying telephone service to domestic subscribers at home, or some combination of all three.

## 5.2 PERSONAL COMMUNICATIONS SERVICES

Stimulated by competition from the PCN operators, it is inevitable that both Cellnet and Vodafone will want to offer a range of GSM-based services targeted at different groups of customers, from the business user to the domestic telephone subscriber. The PCN operators will be aiming at the potentially large but highly cost sensitive domestic market, by offering a lower-cost service than the traditional cellular systems. The key to success for the cellular network operator will be the ability to offer a variety of services with different characteristics and different tariffs. Some of these services will compete head-on with the PCN operators, while others will offer additional facilities for premium prices. The different services may be characterized by different coverage areas, regional and local tariffs, or even different grade of service, measured in terms of the probability of being able to make a call.

There are three fundamental requirements in the system infrastructure to support flexibility in services and tariffs.

The first requirement is a means for on-line checking of subscription information, so that at the time of access the network can determine the level of service to which a particular subscriber is entitled.

The second is an on-line method of informing the user of the cost of a call before it is made. It is not unreasonable that most consumers expect to know the cost of something before they commit to buying it. In a fixed network, the operator can publish a fixed tariff, and the user is always able to determine the cost of a call in advance. If a user is in any doubt, for example, of which calls are carried at the local rate, he or she merely has to look up a list of exchanges in a telephone directory. In contrast, in a mobile network, a it may be desired to set a tariff in which the calls that are charged at a local rate depend on the cell that is currently serving the subscriber. It is not practicable to publish a definitive map showing the area served by each cell, and even if it were, the user would not want to keep consulting it. If subscribers are not to become frustrated by receiving bills for expensive calls that they reasonably expected to have been cheaper, they must be able to determine the tariff for each call in advance. Once this facility is available, it will offer the network operator an enormous flexibility in selling tariffs. The operator might, for example, dynamically increase the price when a cell is heavily loaded. This represents a highly responsive method of market pricing; if the user dislikes the offered price, he or she can try again later when the congestion has been relieved and the price has dropped.

The third requirement is a suitable off-line billing system that can generate the appropriate entries in the customer's bill from a limited quantity of data logged when the call was made.

To consider the way in which some of these requirements will be achieved, we will look at a practical example. At the Communications 91 exhibition in Geneva, Vodafone announced plans for a PCS service as a microcellular network (MCN); the service has since been launched under the name MetroDigital. The following section describes the features of that network, and the way it is integrated into the full Vodafone GSM cellular system.

## 5.3 THE VODAFONE MCN SERVICE

The MCN service to be offered by Vodafone will be designed to offer an economical service to the user of a lightweight, class-5 GSM portable phone. The service will be available in any significant built-up area, identified as the areas shaded in yellow on an ordinance survey route planning map. At the opening of service in 1993, the southeast of England was fully covered, with rollout to most of the country over three years.

MCN tariffs will be at three levels. The "home local" tariff will apply to all calls made from a small area surrounding an address that the user nominates as his or her home location. This will usually be a home address but may be a business address. The "roamed local" tariff will apply when the user is away from his or her home location but makes a call to a nearby fixed subscriber. For example, a user whose home location is in London but who is currently in Portsmouth would pay the roamed local rate for a call to Southampton. Any other calls will be at the "national" rate, which will still be lower than the rate for all calls on the full GSM network.

The full GSM network will provide almost nationwide coverage, as the TACS networks do today, although not all areas will be covered adequately for portable phone users. The full GSM network will be available to an MCN subscriber who selects the GSM network manually or clips the phone into a car adaptor kit incorporating a power booster. Calls made in this way will be at the "GSM upgrade" tariff, which will be more expensive than what a subscriber to the full GSM service would pay for the same call.

The GSM and MCN services are, therefore, complementary. Users who make calls mainly within towns or villages with MCN coverage and only occasionally use their phones while traveling between populated areas would select the MCN service, but they do not sacrifice the availability of nationwide coverage when they really need it. Users who make frequent calls while on the road would find it cheaper to subscribe to the GSM service, with the full network available to them at all times. Users of either network will of course, have full access when traveling abroad to the range of GSM services that will cover the majority of Europe during the 1990s. An MCN or GSM subscriber can, therefore, be reached on a single number whenever he or she is within range of a GSM network anywhere in Europe. As with any GSM subscriber, incoming calls to a user outside the home country will be charged to the caller at the normal rate for a call to the home mobile network.The additional cost due to the subscriber being abroad will be charged to the subscriber receiving the call.

## 5.4 GSM AND MCN INFRASTRUCTURE

The two networks will be supported by three different types of cell sites, which will be known as:

- GSM macrocells;
- Shared macrocells;
- Shared microcells.

GSM macrocells will be large cells, generally covering rural areas, and available only to subscribers to GSM service or MCN subscribers who have temporarily elected to use the GSM network while paying a premium rate. Shared macrocells are cells that form part of the main GSM network but that provide adequate coverage to handportable equipment over part or all of a built-up area. MCN subscribers will treat these cells as part of the MCN network. Macrocells may be either omnidirectional, in which one site feeds one cell, or sectored, in which three different cells are fed by directional antennas from a single site. The vast majority of macrocells will be located at sites already used for the analog TACS network, so rollout can be rapid. Shared microcells are cells constructed specially to support handportable coverage of built-up areas not already covered adequately by a macrocell. They will generally be omnidirectional, serving an area within a radius of about 2 km in suburban districts.

To provide portable coverage of most built-up areas of the United Kingdom, it is anticipated that approximately 2,500 shared microcells will augment the approximately 1600 macrocells fed from 750 sites.

To allow rapid installation of microcell equipment, a standard cell configuration has been designed, which uses a sufficiently small mast to minimize environmental impact and avoid the need for planning permission. Figure 5.1 shows a typical microcell site.The mast is about 15m high and will support two omnidirectional antennas. One antenna will be used for transmission, and both will be used for diversity reception.

Diversity reception helps to mitigate the effects of multipath fading and is particularly important in a system designed for portable use. Without diversity, a static or slowly moving user might pause at a point where the signal on the uplink (mobile to base station) faded into a deep null. Because the fading on the uplink and downlink frequencies is not correlated,the user may be hearing a perfectly good signal on the downlink, but the call may be dropped. The use of diversity reception greatly reduces the probability of this happening.

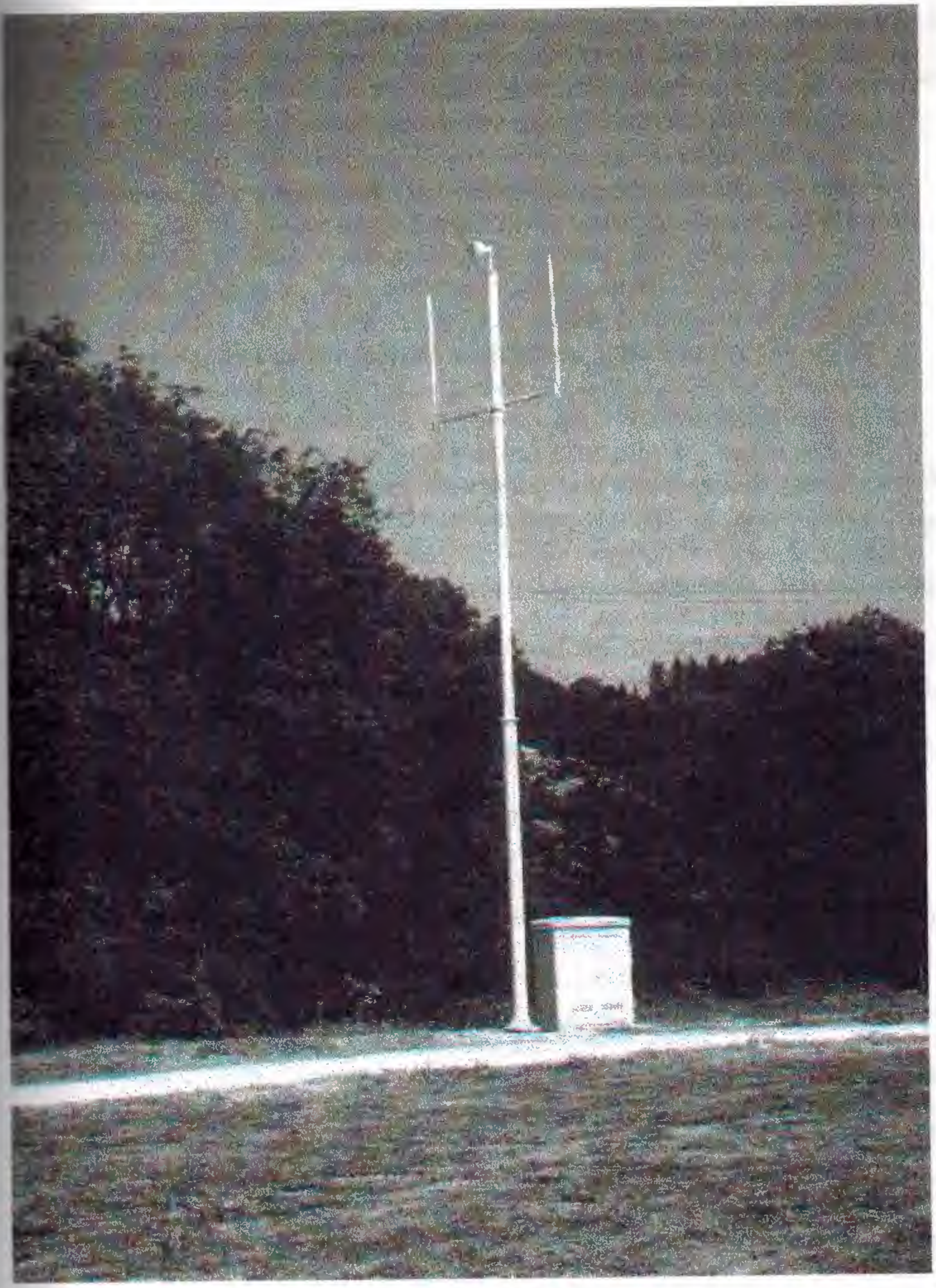


**Figure 5.1** Typicall microcell site

The mast will also be capable of supporting one or more microwave dishes. Wherever possible, microcells will be connected to a nearby macrocell site by microwave link, to minimize link costs. In selection of potential microcell sites, the availability of a line-of-sight path to a nearby macrocell will be an important consideration. The base station transceivers,baseband equipment, microwave link, operations and maintenance systems, control equipment, and a battery backup power supply will all be contained in a single environmental cabin that will be sited near the bottom of the mast. All the equipment will be factory commissioned, so that on-site installation work involves little more than mounting the cabin on its concrete base and connecting up power and anlennas. *In urban areas where a substantial proportion of buildings exceed a height-of* 15m, a similar package will be rooftop mounted on a suitable building.

## 5.5 SERVICE IMPLEMENTATION

Both GSM and PCN networks are based on a common set of standards controlled by the European Telecommunications Standards Institute (ETSI). The ETSI standards specify a minimum set of requirements to ensure that mobiles and infrastructure from different manufaturers can be configured to work together. This alone gives network operators a greater degree of choice in purchasing equipment than with earlier analog systems. In the analog systems the radio interface was standardized to allow competition in mobile manufacture, but the interfaces between base stations and switching equipment were generally proprietary. This meant that once a network operator had chosen a supplier, the operator was commined to that supplier for the life of the network. With DCS 1800 and GSM, it is possible for an operator to mix switches from one supplier with base stations from another.

Although both DCS 1800 and GSM networks are based on the same set of European standards, this does not imply that all networks will be identical. Within the standards there is scope for each manufacturer to develop proprietary strategies for functions such as handover. We will now consider some of the specialized functions that are required to implement an integrated set of mobile and personal communications services based on the GSM standards.

### 5.5.1 Advice of Tariff

We have seen that advice of the cost of the call is an important feature in any system supporting multiple tariffs. There is more than one way in which this might be provided. The simplest wold be by the use of a very short recorded or synthesized voice announcement to the subscriber before a call is connected. An alternative is by the use of the GSM cell brodcast short-message service (CBSMS). This service allows a text message of up to 93 characters to be broadcast to every mobile in a cell. This may be able to be used to deliver some indication of charge rates to the user, who would be able to display the information on the handset. While the CBSMS is a broadcast to all mobiles, GSM also provides for the short-message service (SMS), which allows text messages of up to 160 characters to be addressed to a specific mobile. Unlike CBSMS, SMS uses an acknowledged protocol, so that successful delivery of the message to the mobile is guaranteed. Since a message can be addressed to a specific mobile, use of SMS would allow more coplex tariffs to be applied than use of the broadcast version.

### 5.5.2 Trunk Reservation

Where a range of different services is provided over the same network infrastructure, it is important to ensure that the resources are shared equitably among users of the different services. All telephone systems, whether mobile or fixed, rely heavily on the idea of trunking. If enough telephone lines were provided between London and Manchester for all subscribers in London to make phone calls to Manchester simultaneously, a very expensive resource would be lying idle for most of the time, and telephone calls would be astronomically priced. Instead, the network designer relies on the fact that only a small proportion of Londoners are phoning Manchester at any time. Instead of designing this system for a worst case, which will never occur, the system is designed on the basis of probability. Teletraffic theory enables the designer to calculate how many lines are required, assuming how many Londoners on average will be phoning Manchester,and what probability of being able to make a call will be acceptable to the customer. Such a service would generally be designed so that a call attempt would be successful something like 98% of the time during the busiest hour of the day. Only on one attempt in 50 would the user receive a recorded message saying, "Lines to Manchester are busy, please try later." The probability of a call failing is known as the grade of service, so this system would be described as being designed for a grade of service of 2%. The ratio of the average number of phone calls attempted to the number of lines that must be provide is a measure of the trunking efficiency. Trunking efficiency increases rapidly with the number of lines, especially when the number of lines is small, so that two lines can support far more than twice the number of subscribers supported by one line.

In the initial stages of rollout of a PCS, it is likely that each cell will incorporate only one transceiver, supporting a maximum of seven simultaneous phone calls. As traffic on the network increases, additional equipment will be added to each cell. At 2% grade of service and assuming Erlang B statistics, seven lines can support an average of 2.9 simultaneous phone calls. If this small number of lines were to be split to serve two different services, the total capacity would be greatly reduced. Four lines can support 1.1 calls, three lines only 0.6, so the two services together would support only 1.7 simultaneous calls on average. It can be seen that splitting the lines available between the two services would make inefficient use of the available resources. On the other hand, if the full resource were available to users of either the GSM or MCN service, and the system should become overloaded, there is the possibility that a GSM user who has paid a higher subscription in order to achieve a more comprehensive service might be denied access due to a large volume of traffic generated by MCN users paying lower tariffs.

To solve this problem, Vodafone has patented a system known as Trunk Reservation. This system is designed to control the grade of service offered to users of a number of different services that share the same infrastructure. Let us consider a cell designed to provide n different services, (e.g., service 1 = GSM, service 2 = MCN). If there is a request for the use of a voice channel and a channel in the cell is free, the system will decide whether to grant the request depending on the service requested, the number of channels free, and the value of a random number, R. The random number may be uniformly distributed between 0 and 1. A new random number is generated for each access request. Table 5.2 contains values for $X_{ij}$.

Access to the network is granted only if the random value R is greater than or equal to the value $X_{ij}$, where i corresponds to the number of free channels and j to the service requested. If more than some number of channels Q are free, all access attempts will be granted. With this system, suitable choice of the coefficients $X_{ij}$ enables the operator to adjust the grade of service offered to each service as appropriate.

### 5.5.3 Service Separation

For two or more separate services to be supported on the same network, a means must be provided to allow the network to determrnine which users may have access to any given cell,In the Vodafone network, the system will initially identify a user as requesting MCN or GSM service by that user's classmark. A class-5 phone will receive MCN service,while phones in classes 1 through 4 will receive GSM service. In a GSM network,subscription details are recorded not in the phone itself but in a removable subscriber identity module(sım). This will usually be implemented as a credit card-sized "smart card”. The results of using SIMs containing GSM and MCN subscription information in different mobiles are shown in Table 5.3. The combination of an MCN subscription and a phone in class 1, 2, 3, or 4 may, of course, be obtained either by the MCN subscriber using his or her smart card in a different phone or by inserting a class-

**Table 5.2**

Trunk Reservation Coefficients

| | Service Type | | |
|---|---|---|---|
| Free Channels | 1 | 2 | 3 ... |
| 1 | $X_{11}$ | $X_{12}$ | |
| 2 | $X_{21}$ | X22 | |
| 3 | $X_{31}$ | $X_{32}$ | |
| . | . | . | |
| . | . | . | |
| ? | 1 | 1 | |

*5 phone into a power-boosting car adaptor.*

Mobility management in a GSM network, that is, the ability of a network to know where to find a given mobile, is handled by a procedure known as location updating. The network is broken down into a number of location areas. Each base station radiates a signal containing the location area identity (LAI) of the area to which it belongs. Whenever a mobile camp on a cell with a different LAI, it carries out the location update procedure to inform the network that it has moved into a new area. The size of a location area is determined by a trade-off between the volume of signaling traffic generated by paging requests and the volume of location update traffic. The two extremes of this trade-off are easily understood. If the entire network were treated as a single location area, the network would have no idea where any mobile was located. In the event of an incoming call to the network, a paging message would have to be transmitted in every cell. This would lead to an excessive loading of the control channel with paging traffic. At the other extreme, every cell could be treated as a separate location area. In that case, every time a mobile crossed from one cell to the next, it would generate a location update. Paging

**Table 5.3**

Service Available for Each Subscription and Classmark Combination

| | Mobile Class | |
|---|---|---|
| SIM Subscription Type | 1-4 | 5 |
| GSM | Full GSM service at GSM tariff | Service available only from MCN cells,GSM tariff |
| MCN | Ful GSM service at premium tariff | Service available only from MCN cells ,MCN tariff |

traffic would be minimized, because the network would only have to page a mobile in one cell, but the control channel would be heavily loaded with location update traffic. The practical solution, of course, lies somewhere in between, with a group of cells in each location area.

The location-updating mechanism can be used to support separation of cells providing MCN service from those that provide only GSM service. GSM-only cells will be given a different location area from shared cells in the same locality. A class-5 mobile attempting a location update on a GSM-only cell will have its location update rejected. This allows the system to restrict MCN users to a subset of cells in the network.The allocation of location areas is illustrated in Figure 5.2.

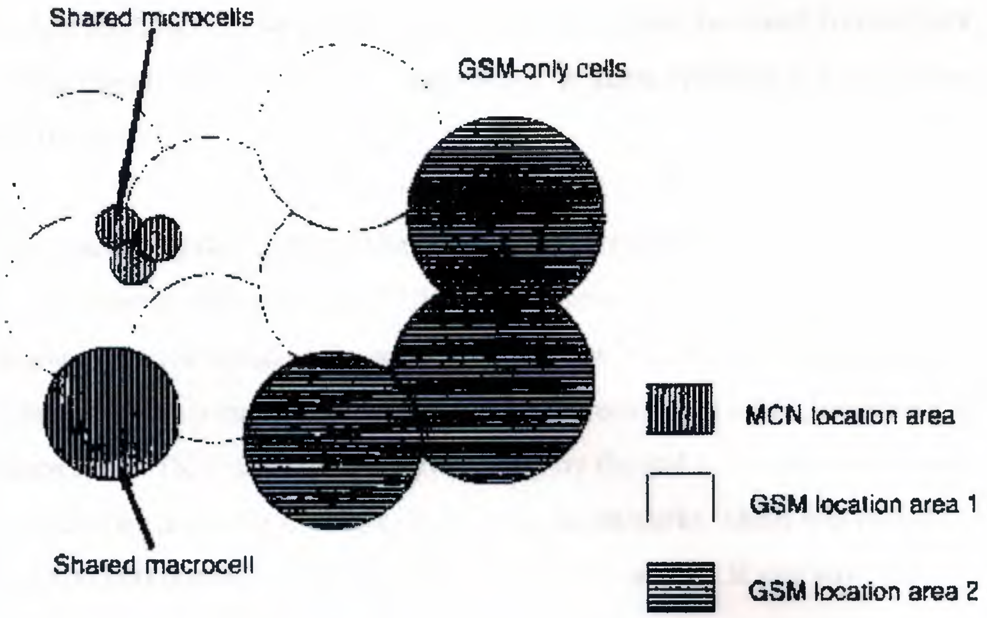


**Figure 5.2** Allocation of location areas.

Use of techniques such as those described here offers the cellular network operator the necessary flexibility to be able to offer a range of personal communications services to suit the needs of its customers and to respond to competition in the fast-changing marketplace for mobile communications in the 1990s.

# CONCLUSION

PCN is really an old marketing term, not a technology. The industry no longer refers to PCN at all, but instead calls it GSM 1800. UK PCN systems are GSM running at twice the frequency. PCN/GSM 1800 is the system that is most recent to the market. The One2one, Virgin and Orange networks use it. Vodafone and Cellnet also have frequencies Allocated in this band, but it is not yet clear how they plan to use them. GSM 1800 was designed and expected to become a mass-market system, and the Orange network is being built with a design capacity for many users. Generally, signal strength inside buildings can be a problem at these frequencies, but more transmitters are improving signal generally as they come on line. In some buildings it works better than 9800, though!

It seems likely that there will be similar 1800 networks built overseas, and "roaming" agreements, allowing use of UK phones abroad, are likely. Roaming at 1800 MHz in many countries including France, Germany, The Netherlands, Switzerland, Thailand and Malaysia is currently available. An EC directive has made governments issue licenses for an 1800 network in every country by the end of the decade, but less populated countries may take a while to roll out these networks. Many will probably use dual-band 1800/900 phones, which are now commonly available. If you have the choice, getting a dual-band handset seems to make sense.

## ABREVATION

The following is a list of abbreviations and terms frequently used in the GSM literature.

| | |
|---|---|
| A | interface between MSC and BSC |
| Abis | interface between BSC and BTS |
| AC | authentication center |
| ADC | analog-to-digital converter |
| AGC | automatic gain control |
| AGCH | access grant channel, used by BTS to allocate initial signaling channel |
| AM | amplitude modulation |
| AMPS | advanced mobile phone system, U.S. cellular standard |
| ARFCN | absolute radio frequency channel number |
| ASIC | application-specific integrated circuit |
| ASK | amplitude-shift keying |
| BCC | base station color code |
| BCH | broadcast channels |
| BCCH | broadcast control channel, base channel from BTS |
| BCF | base station control function |
| BDM | bit demodulator |
| BER | bit error rate |
| BFI | bad frame indication, used when a speech frame is corrupted |
| Bm | bearer-mobile channel |
| bps | bits per second |
| BPSK | binary phase-shift keying |
| BS | base station |
| BSC | base station controller |
| BSIC | base station identity code, contains identity and TSC |
| BSS | base station system |
| BSSMAP | base station system management part |

| | |
|---|---|
| BTS | base transceiver station |
| CAI | common air interface |
| CBCH | cell broadcast channel, used for point-to-multipoint SMSs |
| CC | call control entity |
| CCCH | common control channel, can be AGCH, PCH, or RACH |
| CCITT | Commitê Consultatif International de Têlêgraphique et Téléphonique, International Telegraph and Telephone Consultative Committee |
| CDMA | code-division multiple access, a broadband radio technology |
| CDVCC | coded digital verification color code |
| CELP | code excited linear predictive coding |
| CEPT | Conference Européenne des Administrations des Postes et des Télécommunications, European Conference of Posts – and Telecommunications Administrations |
| C/I | carrier-to-interference ratio |
| C/R | commandlresponse |
| CRC | cyclic redundancy check |
| CM | connection management |
| CW | continuous wave |
| DAC | digital-to-analog converter |
| DAI | digital audio interface |
| D-AMPS | Dual-mode AMPS, U.S. analog and digital dual-mode cellular system |
| DAMPS | another abbreviation for D-AMPS |
| DCCH | dedicated control channels |
| DCS 1800 | digital cellular system, 1800-MHz band, used for PCN Networks |
| Dm | data-mobile channel |
| DQPSK | differential quadrature phase-shift keying |
| DSP | digital signal processing |
| DTAP | direct transfer application part |
| DTC | digital traffic channel |
| DTMF | dual-tone multifrequency, (touch-tone) addressing of |

| | |
|---|---|
| | numeric keypad |
| DTX | discontinuous transmission, optional transmission mode of a mobile station, which is used when no voice activity is detected |
| DUT | device under test |
| EAMPS | expanded AMPS, a form of AMPS with more RE Channels than the 666 channels in AMPS |
| E-GSM | extended GSM |
| EIA | Electronics Industries Association |
| EIR | equipment identity register, network register for mobile Terminal equipment |
| EPI | protocol indicator |
| EQ | equalizer |
| ESN | electronic serial number |
| ETS | European telecommunications standards |
| ETSI | European Telecommunications Standards Institute |
| FACCH | fast associated control channel |
| FCCH | frequency-correction channel, BTS to MS |
| FDD | frequency-division duplex |
| FDMA | frequency-division multiple access |
| FEI | frame erasure indication |
| FER | frame erasure rate |
| FN | frame number |
| FM | frequency modulation |
| FOCC | forward control channel |
| FPLMTS | future public land mobile telephone system |
| FSK | frequency-shift keying |
| FTA | full type approval, mobile equipment approval |
| FVC | forward voice channel |
| GMSC | gateway mobile switching center |
| GMSK | Gaussian minimum-shift keying, modulation scheme used in the GSM |
| GSM | Global system for mobile communications (formerly: |

| | |
|---|---|
| | groupe |
| | Spéciale Mobile, now 5MG) |
| HLR | home location register, network register for home |
| | Subscribers |
| HSN | hopping sequence number, frequency-hopping parameter |
| HT | hilly terrain |
| HWC | hardware controller |
| IE | information element |
| IEI | information element identifier |
| I-ETS | Interim European Telecommunications Standards |
| IF | intermediate frequency |
| IMEI | international mobile equipment identity |
| IMSI | international mobile subscriber identity |
| IMTS | improved mobile telephone service |
| IS | interim standard |
| ISDN | integrated services digital network |
| ISO | International Standards Organization |
| ITA | interim type approval, mobile equipment approval before |
| FTA | was available |
| JDC | Japanese Digital Cellular, also PDC |
| JTACS | Japanese TACS |
| kbps | kilobits per second, a thousand bits in one second |
| kHz | kilohertz, 1,000 Hertz or cycles per second |
| LAC | location area code |
| LAI | location area identity, contains LAC, MCC, and MNC |
| LAPD | link access protocol digital |
| LAPDm | link access protocol digital mobile |
| Lm | low-mobile channel |
| L2ML | Layer 2 management link |
| LMT | local maintenance terminal |
| LPC | linear predictive coding, speech coding |
| | Unction |
| LPD | link protocol discriminator |

| | |
|---|---|
| LTP | long-term prediction, speech coding function |
| MAHO | mobile-assisted handoff |
| MAIO | mobile allocation index offset, indicates at which frequency within the hopping sequence the MS and BS will start to hop |
| MAP | mobile application part, network Unctionlentity |
| MCC | mobile country code, country code of GSM network, three digits |
| ME | mobile equipment, terminal not fitted with a SIM |
| MF | mandatory fixed length |
| MHz | megahertz, 1,000,000 Hertz or cycles per second |
| MIN | mobile identity number |
| MM | mobility management |
| MMI | man-machine interface, user interface |
| MNC | mobile network code, identifies a GSM-network within a country, two digits |
| MOC | mobile-originated call |
| MoU | Memorandum of Understanding, within a group of GSM operators |
| MS | mobile station, terminal (hardware) equipped with a SIM |
| MSC | mobile (services) switching center, GSM switch |
| MSIC | mobile subscriber identification number |
| MSK | minimum-shift keying |
| MT | message type |
| MTC | mobile-terminated call |
| MTP | message transfer part |
| MTS | mobile telephone service |
| MV | mandatory variable length |
| NADC | North American Digital Cellular |
| NAMPS | narrowband AMPS |
| NCC | national color code |
| N-CDMA | narrowband CDMA |
| NMT | Nordic mobile telephone system, Scandinavian analog cellular |

| | |
|---|---|
| | standard for *450* and 900 MHz |
| NTACS | narrowband TACS |
| OF | optional fixed length |
| O&M | operation and maintenance |
| OMC | operations and maintenance center, network entity for network operation and management |
| OML | operation and maintenance link |
| OQPSK | offset quadrature phase-shift keying |
| OSI | open systems interconnection, functional interconnect model |
| OV | optional variable length |
| PAD | packet assembler/disassembler |
| PCH | paging channel, used to call a mobile station |
| PCM | pulse code modulation |
| PCN | personal communications network |
| PCS | personal communications system, U.S. |
| PD | protocol discriminator |
| PDC | personal digital cellular (JDC, Japanese personal communication system), 800/1,500 MHz |
| PIN | personal identification number, to be presented when using a GSM phone/SIM |
| P/F | poll/final |
| PLMN | public land mobile network |
| PM | phase modulation |
| PRBS | pseudorandom bit sequence |
| PSK | phase-shift keying |
| PSTN | public switched telephone network |
| PUK | personal unblocking key |
| RVC | reverse voice channel |
| QPSK | quadrature phase-shift keying |
| RA | rural area |
| RACH | random access channel, used by MS to access a GSM network |
| RBER | residual bit error rate |
| RCC | radio common carrier |

| | |
|---|---|
| RECC | reverse control channel |
| RPE | regular pulse excitation, speech coding function |
| rms | root mean square |
| RR | radio resource management |
| RSL | radio signaling link |
| RSSI | received-signal strength indication |
| RX | (radio) receiver |
| SABM | set asynchronous balanced mode, Layer 2 command |
| SACCH | slow associated control channel, associated with TCH or SDCCH |
| SAP | service access point |
| SAP(I) | service access point (identifier) |
| SAT | supervisory audio tones |
| SC | signaling controller |
| SCCP | signaling connection control part |
| SCH | synchronization channel, used by BTS to transmit BSIC and time stamps (frame/multiframe counters) |
| SCM | station class mark |
| SDCCH | standalone dedicated control channel, signaling channel |
| SDMA | space-division multiple access |
| SFH | slow frequency hopping |
| SID | silence descriptor (frame sent when no voice activity) |
| SID | system identification number |
| SIM | subscriber identity module, smart card |
| SINAD | signal + noise and distortion |
| SMG | Special Mobile Group, ETSI standardization groups for GSM |
| SMS | short-messages services, transmission of alphanumeric infortion, point-to-point (dedicated) or point-to-Multipoint (CBCH) |
| SMT | surface-mounted technology |
| SNR | signal-to-noise ratio |

| | |
|---|---|
| SS | supplementary services |
| SSN7 | signaling system no. 7, CCITT standard |
| TACS | total access cellular system, U.K. analog cellular standard |
| TCH | traffic channel, for speech or data |
| TCH/FS | traffic channel/full-rate speech |
| TCH/HS | traffic channel/half-rate speech |
| TDD | time-division duplex |
| TDMA | time-division multiple access |
| TEI | terminal equipment identifier |
| TI | transaction identifier, Layer 3 parameter |
| TMSI | temporary mobile subscriber identity |
| TN | time slot number (0,1,..., 7) |
| TRAU | transcoder rate adapter unit |
| TRX | (radio) transceiver |
| TS | time slot |
| TSC | training sequence code (0, 1, ..., 7) |
| TTL | transistor-transistor logic |
| TU | typical urban |
| TX | (radio) transmitter |
| UI | unnumbered information |
| Um | GSM air interface (radio interface) |
| UMTS | universal mobile telephone system |
| UUT | unit under test |
| VAD | voice activitx detection |
| VCO | voltage-controlled oscillator |
| VLR | visitor location register, network register for visiting subscribers always associated with an MSC |
| VLSI | very -large-scale integrated circuits |
| WP | working party |

# REFERENCES

1) SIEGMUND M.REDL, MATTHIAS K. WEBER, MALCOLM W. OLIPHANT
1995, "AN INTRODUCTION TO GSM", Norwood, Artech House, INC.

2) Mouly, M., and B. Pautet, 1992, "The GSM System for Mobile Communications" , Palaiseau, pp. 28—32.

3) Schmitt, G., Nov 1993, "GSM, a Success in Europe, an Opportunity for the Middle East and the Arab World", Proc. IBC Middle East and Gulf Mobile Communications Conf., Dubai, Press: IBC Technical Services Ltd., London.

4) Twingler, J., Nov 1993, "The GSM Standard in the Present and in the Future," Proc. IBC Middle East and Gulf Mobile Communications Conf., Dubai, Press: IBC Technical Services Ltd., London.

5) Sophia Antipolis, "GSM Technical Specifications", ETSI, Vols. 02.01 to 02.05.

6) JOHN GARDINER, BARRY WEST,1997, "PERSONAL COMMNICATION SYSTEMS AND TECHNOLOGIES", Norwood, Press:Artech House, INC.

7) Akerberg,D.,et al., Jan 1991. "A Business Cordless PABX Telephone system,IEEE Comminications Magazine" ,Vol.29,NO.1.

8) ETSI,European Telecomminication Stadandard,DECT,ETS 300 175 ,Parts 1-9 , and ETS 300 176.

9) Hoek,H.B.van der, 1993 , "DECT,European Comminications"

10) Trivett ,D., 1997 , "DECT,Datapro Publication",
Press:McGraw-Hill.

11) Sophia Antipolis ,1997, "Recommendations for GSM 900/DCS 1800" Published by ETSI, ,
European Telecommunications Standards Institution, Cedex, France.

12) Raxnsdale, P. A., and W. B. Harrold, Oct 1992 , "Techniques for Cellular Networks Incorporating Microcells" IEEE Conf. PIMR 92 , Boston.

13) Hata, M., Aug 1980, "Empirical Formula for Propagation Loss in Land Mobile Radio Services," IEEE Trans. on Vehicular Technology, Vol. VT-29, No. 3, pp. 3 17—323.

14) Morgensen, P.E., P. Eggars, and C. Jensen, Apnl 15-18,1991, "Urban Area Radio Propagation Measurements for GSM/DCSI800 Macro and Micro Cells," Proc. 7th mt. Conf Antennas and Propagation
Press: lEE Conference Publication No. 333, IEE,pp. 500—503.
City:London

15) http:\\www.gsm1800.com

16) http:\\www.pcn.com