5

Mobile Communications

The major application for wireless communications has been speech. Radio telephones have been around for many decades, but the capacity of these systems has been very limited. These radio telephone networks consisted of only a few *base stations* (BSs) with which mobile units communicate, and each BS covered a large geographical area. The number of simultaneous calls inside the area covered by one BS was restricted to the number of channels available for this BS. Therefore, the capacity of these systems was low and the radio telephone service was available only to professionals.

During the 1970s, the development of digital switching and information technologies made modern cellular telephone systems feasible. The cellular principle offered a solution to the capacity problem. Different analog cellular standards were developed in Nordic countries, the United States, and Japan at the end of 1970s.

In this chapter we introduce first the idea and operation of cellular radio systems in general. The common principles of cellular systems are valid for any public land mobile network. Then we will review other mobile systems such as paging systems, cordless telephones, and WLANs. In the last section of this chapter, we review the structure and operation of the GSM network. Our goal in this chapter is to provide the reader with an understanding of what is required of the network to enable someone to receive or initiate a call anywhere in the world. The natural requirement for this is that compatible service be available. We use GSM as an example of a digital cellular system because it is currently the dominant global digital technology.

5.1 Cellular Radio Principles

The main problem of conventional radio telephone networks was low capacity because of the limited frequency band available for this service. Cellular networks provide a solution for this by using the same frequencies in multiple areas inside the network. This principle of frequency reuse with the help of a cellular network structure was invented at Bell Laboratories during the 1960s. The technical development of radio-frequency control, the microprocessor, and software technologies made cellular networks feasible by the end of 1970s. Here is a list of the most important common characteristics of cellular systems:

- Frequency reuse provides a much larger number of communication channels than the number of channels allocated to the system.
- Automatic intercellular transfer, or a handover, ensures continuity of communication when there is a need to change BSs.
- Continuous monitoring of communication between the mobile and BS verifies the quality and detects the need for a cell transfer.
- Automatic location of mobile stations within the network ensures that calls can be routed to mobiles.
- Mobile stations continuously listen to a common channel of the network in order to receive a call.

Figure 5.1 presents the basic elements of a simplified cellular network. BSs are radio transmitter/receivers by which the *mobile stations* (MSs, such as telephones) are connected to the wire-line network. The BSs are connected to the *mobile switching center* (MSC) by primary rate digital connections. The MSC acts as a local exchange in the fixed network. In addition to the switching and other functions of an ordinary telephone exchange, the MSC also keeps track of the subscribers' locations with the help of location registers. We discuss this equipment in the following section.

Note that all cellular networks are designed to act as access networks. Their main purpose is to make mobile subscribers accessible from the global (fixed) telecommunications network. The mobile cellular networks always rely on a fixed network. They have no switching hierarchy similar to that of a fixed network (see Chapter 2) and international calls are connected via a fixed network.

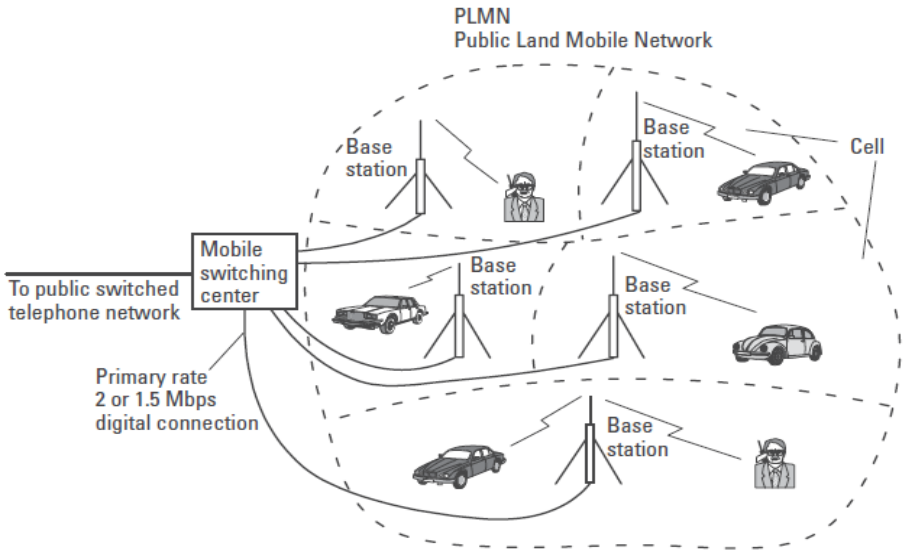

Figure 5.1 Basic structure of a cellular radio network.

5.2 Structure of a Cellular Network

This section reviews the structure of a general cellular network. The detailed structure of a cellular radio network, the terminology of network elements, and their detailed functions are dependent on the network technology in question.

5.2.1 Cellular Structure

Instead of covering an entire area with high-power fixed radio stations, the way older generation radio systems had to, the area of a cellular network is divided into small cells of only a few kilometers or less across as shown in Figure 5.2. Areas where subscriber density is high are covered by smaller cells than areas where subscriber density is low. The power BSs and MSs are automatically decreased with the decreased cell size.

The BSs and MSs (telephone) are controlled to keep their transmission power as low as possible. This low-power transmission does not interfere with other users of the same frequency (reuse of frequencies) some cells away from this cell. This is how each frequency channel can be used again and again and, in principle, a network operator can increase capacity without

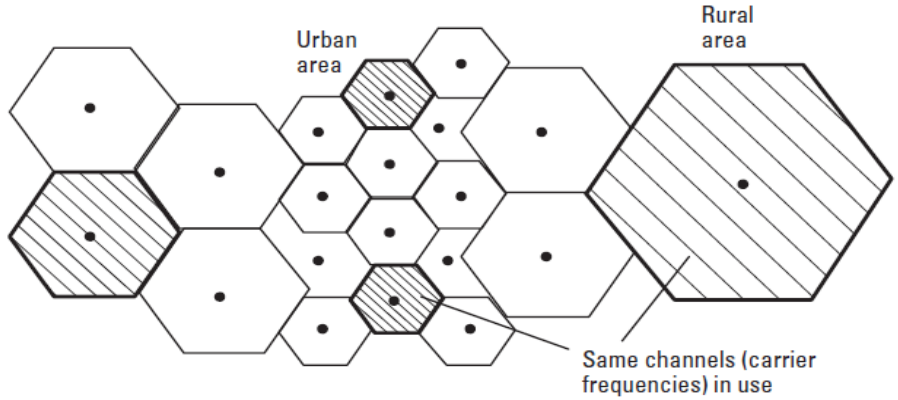

Figure 5.2 Cellular structure of a mobile radio network.

limit by reducing cell size. Naturally, this requires investment in additional BS sites. How often each carrier frequency is used is termed the *frequency reuse factor* and it depends on the system. Note that in the CDMA cellular system, which is introduced in Section 5.4.5, neighbor cells may use the same carrier frequency and there channeling is based on the spreading code instead of frequency (and time slot).

The consequences of reduced cell size are handier and less expensive telephones as well as longer operational life for the battery. Low transmission power also provides a safety improvement from the users' point of view. Because of public concern about handheld terminals and their adverse effects on health, low transmission power has become increasingly important.

In a conventional fixed network, telephone calls are always routed to one fixed telephone socket, as we saw in Chapter 2. In a cellular network a subscriber is located in one cell at a time. Now the network has to include additional intelligence to be able to connect a call to the cell where the called subscriber is available at that time. To succeed at this, the cellular networks have two databases or registers, a *home location register* (HLR) and a *visitors location register* (VLR), and with them the network is able to manage the mobility of its subscribers.

5.2.2 HLR and VLR

When subscribers purchase a mobile telephone, they are registered in the HLR of their own mobile telephone operator. The HLR stores their up-to-date subscriber information such as where (in the area of which VLR) they

are located presently, what services they have the right to use, and a number where she has transferred calls. The HLR is the global central point where their information is available wherever they are located. When a call is routed to them, the dialed subscriber's telephone number tells the network where their HLR can be found.

VLR stores information about every subscriber in its area. The VLR informs the HLR when a new subscriber arrives in its area. It also contains more accurate information of where (to which cell or group of cells) to connect incoming calls directed to a certain subscriber. The VLR is usually integrated into a mobile telephone exchange but the HLR is usually a physically separate efficient database system.

5.2.3 Radio Channels

Each BS provides two main types of channels, as shown in Figure 5.3: the common control channel and the dedicated channels. In the downlink or forward direction (from network to mobile stations) information such as network identification, location information, designated power level, and paging for incoming calls is sent on the common control channel of each cell. When MSs are in idle mode (no ongoing call) they are continuously listening to the common control channel of one cell. In the uplink or reverse direction of the common control channel the MSs send, for example, call-request messages in the case of outgoing calls and location update messages when they notice that they have arrived in a new location area.

One dedicated user channel or a traffic channel is allocated for each call. During an call, a MS is said to be in dedicated mode. Each dedicated channel requires the transmission of control information in addition to speech transmission. This is needed for transmission power control of mobile stations and for transmission of performance monitoring information from MSs to the network. When the call is cleared the dedicated channel is released and available for other users.

In Figure 5.3 we see that BSs are connected to the mobile switching center by a radio relay system or by a cable line (optical or copper cable). Especially in rural areas microwave links are attractive because cables are usually not available for BSs and they are very expensive to install. Microwave radio requires and antenna but this is not a problem—an antenna tower is always available because it is needed for the BS antennas.

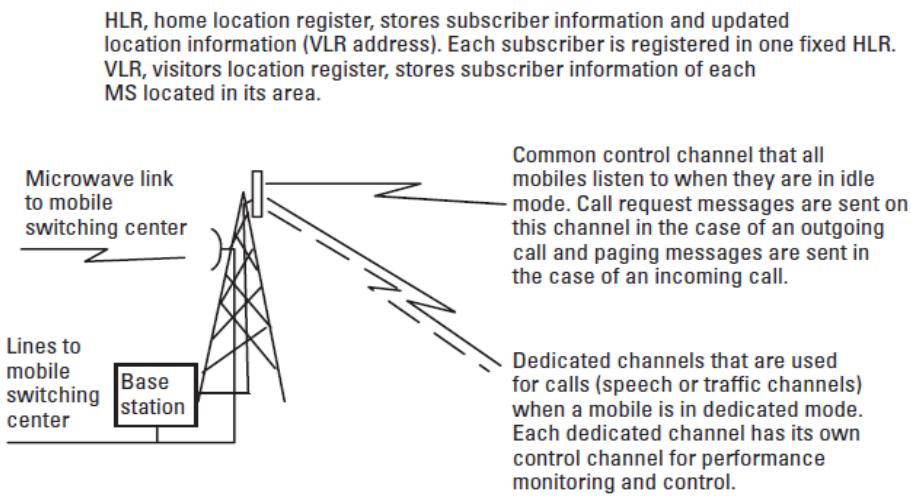

Figure 5.3 The main types of radio channels.

5.3 Operating Principle of a Cellular Network

In the fixed telephone network each subscriber is identified by the number of a certain subscriber loop that is connected to a certain telephone socket. In the case of a cellular telephone the identification is in the telephone set (MS) itself. The cell structure of the network and the mobility of the user require the cellular network to keep track of the location of each MS in order to be able to route a call to the destination.

We now review the principles of how the cellular network manages the mobility of users and how calls are initiated and received. We introduce the operation of a cellular network in general; therefore, the terms and operation presented may not be consistent with the terms and detailed operation of a particular network technology.

5.3.1 MS in Idle Mode

The MS is preprogrammed to know the frequencies of the control channels. When it is switched on, the mobile scans these frequencies and selects the BS with the strongest common control channel. Then the MS transmits its unique identification code, which may be its telephone number (or other identification code depending on the system), over the control channel in order to inform the VLR. The VLR, with the help of the identification of the MS, determines the address of the subscriber's home country and the home network. Then the MSC/VLR transmits the signaling message toward the

home network. The message is then routed to the HLR, which is then informed that this specific subscriber is now located in the area of a certain VLR. The HLR stores this information. Now the HLR is able to route the calls to the right MSC/VLR, which routes it further to the mobile subscriber.

The MS then continuously listens to the common control channel and, if necessary, transfers to the control channel of another cell (Figure 5.4). Each network is divided into small location areas that contain a group of cells. All BSs inside a certain location area send the same global code dedicated for that location area on the common control channel. If the MS moves, changes the channel and the location information sent by the network changes; the MS notices it and informs the network, which then updates the location information stored in the VLR and HLR (if needed).

5.3.2 Outgoing Call

The number that a user wants to call is entered into the memory of the mobile telephone through its keypad. When the user presses the Call button, the mobile telephone sends a set of signaling messages to the BS via the common control channel, as shown in Figure 5.4. These messages contain the dialed digits, which the BS passes to the MSC for routing.

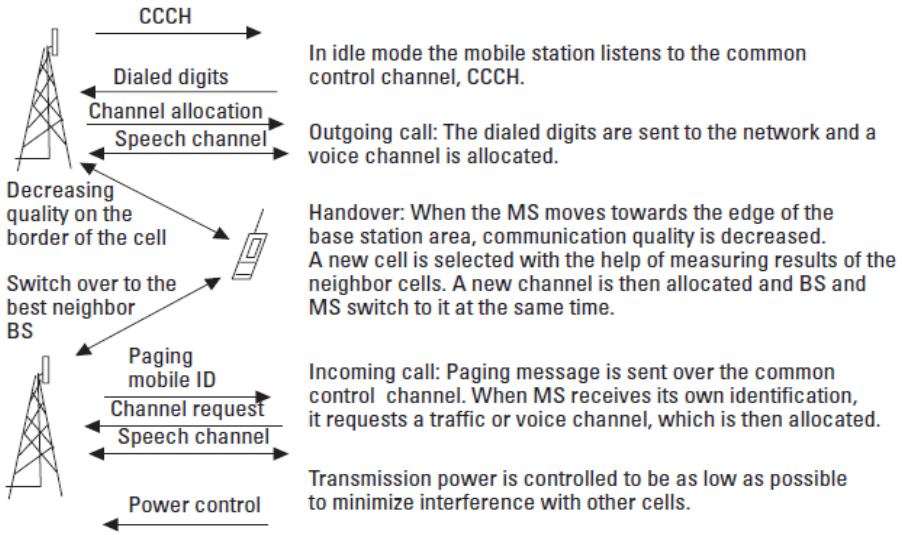

Figure 5.4 Basic operation of the cellular network.

The MSC analyzes the dialed number, passes the digits to the public telephone network for call establishment through the PSTN, and requests a BS to allocate a dedicated speech channel for the calling mobile. The MS and BS switch to this channel when the called party answers and the conversation is allowed to start (Figure 5.4).

5.3.3 Incoming Call

When a call is to be connected to the MS, the HLR determines to which VLR address the call should be routed. This address is global, containing the country and network codes according to international telephone numbering scheme. The call is then routed to the MSC/VLR, which knows the more exact location (the location area) of this specific subscriber inside its area. A paging message with MS identification is sent on the common control channel of all BSs in that area where the subscriber is currently located. The receiving MS continuously listens to this channel and when it receives the message containing its own identification it requests a speech channel and a channel is allocated for this call. The BS and MS switch to the allocated channel, the telephone rings, and when the subscriber presses the Call button, the call is connected.

5.3.4 Handover or Handoff

During a call the quality of the connection is continuously monitored and the transmission power of the MS and BS is adjusted to keep the quality at a sufficient level while at the same time keeping the transmission power as low as possible. When an MS moves close to the border of a cell, the transmission power is adjusted to the maximum allowed for that cell. As an MS moves further away from the BS, the S/N of the channel decreases and the error rate increases. If the quality falls below a predetermined level, a new channel is allocated in a neighboring cell and both the BS and the MS are requested to switch to the new channel at the same time instant. The cellular network has analyzed the measuring results before the switch and estimated the quality between the MS and neighbor cells. The best alternative is selected for a new cell.

5.3.5 MS Transmitting Power

During the planning phase of a cellular network, the maximum transmitting power for each cell is defined. This power is dependent on the desired cell size and on geographic conditions. The transmitting power of the common

control channel of the BS is adjusted to a level that is high enough to cover the cell area but not higher than necessary. During a call the network, to minimize interference between cells that use the same frequency, continuously controls the transmitting power of the MS and the BS. This also saves the battery of the MS.

5.4 Mobile Communication Systems

So far we have looked at the generic operation of cellular mobile radio systems because of the importance of these systems. However, there are many other important mobile communication systems, and we briefly introduce some of them in this section.

5.4.1 Cordless Telephones

Cordless phones were originally developed for the residential market and they were designed to cover only one local area such as a house and garden. They support only local mobility and should not be considered competitors for cellular mobile networks. We now look at the most important applications of cordless telephones.

5.4.1.1 Residential Use

The only advantage of cordless telephones over fixed telephones in ordinary residential use is a wireless handset that allows some mobility. The BS of a cordless telephone is connected to the fixed telephone socket and only one handset for each base station is typically in use (Figure 5.5). The BS unit contains a battery charger for the handset. Many systems in use are still analog *first generation cordless phones* (CT1).

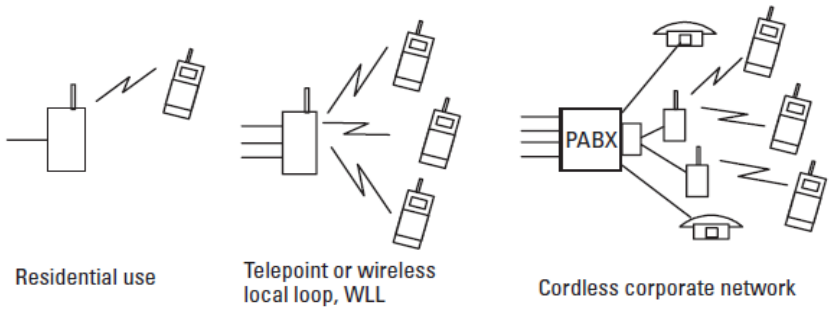

Figure 5.5 Cordless telephones and their applications.

5.4.1.2 Telepoint and WLL

Digital *second generation cordless telephone technology* (CT2) was developed for so-called "telepoint" use in addition to residential markets and offices. Telepoint was a service in which BSs were installed in key locations in a city such as railway stations and airports. A user of this service could take his or her digital cordless telephone from home or office (or rent a cordless telephone) and make a call outside via the telepoint BS. Subscribers were usually not able to receive a call. This service was not successful and most telecommunications network operators have abandoned it. The main reason for this was rapid expansion of cellular mobile service, which allows much better service and mobility.

The latest digital cordless technologies, such as *Digital European Telecommunications* (DECT), are also used in some areas to provide WLL service. With DECT technology a new operator that does not have its own cable network can provide telephone service. The WLL applications were seen to be important to generate competition in the area of traditional fixed telephone subscriber service provision. With the help of cordless technology, a new network operator can efficiently provide a service that is better, in terms of mobility, than the competing fixed telephone service by the operator who owns the cables of the fixed access network. However, the importance of WLL has decreased because of the reduced costs of cellular telephone service.

5.4.1.3 Cordless Corporate Network

In most companies internal wireless communications as well as external communications rely on the public cellular networks. The corporate telephone network is built on the fixed telephone service provided by the PABX/PBX of a company. One attractive application of modern digital cordless technologies, such as DECT, was considered to be cordless corporate networks where the PABX is upgraded to control wireless DECT telephones in addition to wire-line telephones. This technology supports handover and terminals can move freely inside the area of one PABX that controls multiple base stations. Internetwork mobility management functions make it possible to extend the mobility of DECT to other office sites of a corporation and probably even to the local public network if the local public network operator supports DECT technology. The corresponding American technology is called a *personal access communication system* (PACS).

5.5 GSM

As an example of a digital cellular network, we introduce the structure and operation of the GSM network. The European digital cellular system GSM was developed by CEPT during the 1980s, and this work was continued by ETSI. The acronym GSM came originally from the standardization working team, but GSM is presently understood to mean Global System for Mobile Communications. Two other cellular networks are based on GSM technology: the European DCS-1800, which operates in the 1.8-GHz band, and the American GSM-1900, which operates in the 1.9-GHz band. Our discussion in this section is valid for all of these networks.

In GSM, unlike in analog mobile networks, subscription and mobile equipment are separated. Subscriber data are stored and handled by a *subscriber identity module* (SIM), which is a smart card belonging to a subscriber. With this card the subscriber can use any mobile telephone equipment just if it were his or her own. The radio equipment is called *mobile equipment* (ME) and we can say that the mobile station consists of two parts, ME and SIM; that is: MS = SIM + ME.

5.5.1 Structure of the GSM Network

A simplified architecture for the GSM network is presented in Figure 5.9. For a more detailed look at the structure and functionality of the GSM network, the reader should refer to [1, 2].

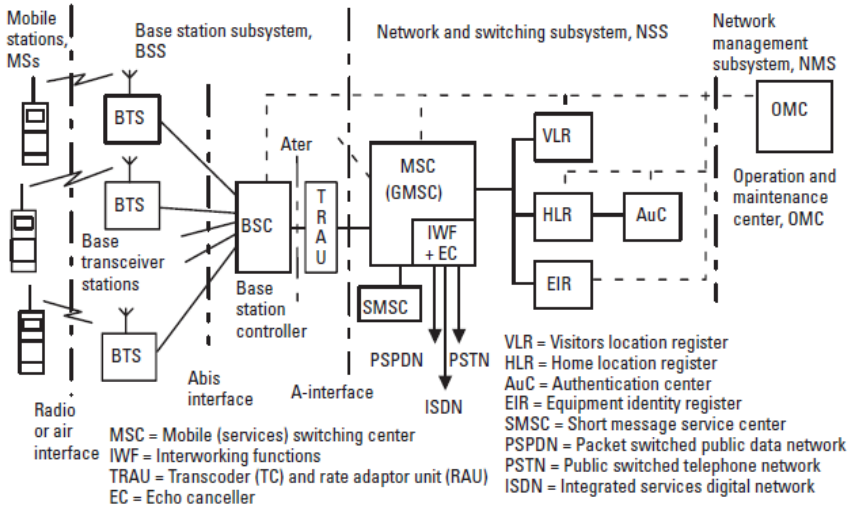

Figure 5.9 Structure of the GSM network.

5.5.1.1 Radio Network

MSs are connected to the mobile switching center (MSC), via a *base station subsystem* (BSS). The BSS consists of a *base station controller* (BSC) and many *base transceiver stations* (BTSs) that are controlled by one BSC. The roles of the network elements are introduced in the following sections.

5.5.1.2 MSC

Like any local exchange, the MSC establishes calls by switching the incoming channels into outgoing channels. It also controls the communications, releases connections, and collects charging information.

As a mobile switching system, the MSC together with the VLR performs additional functions such as location registration and paging. It also transfers encryption parameters, participates in the handover procedure when required, and supports *short message service* (SMS). The SMS is a service integrated into GSM that enables users to transmit and receive short text messages.

In each cellular network there is at least one *gateway MSC* (GMSC) that provides connections to other networks. The MSC in Figure 5.9 performs gateway functions in addition to other MSC functions. The GMSC works as an interface between the cellular network and the fixed networks and it must handle the signaling protocols between the fixed networks and network elements of PLMN. The GMSC also controls echo cancellers, which are needed between the fixed and cellular network because of long speech-coding delays.

5.5.1.3 HLR

All subscriber parameters for each mobile user are permanently stored in one HLR. The HLR provides a well-known and fixed location for variable routing information. The main functions of the HLR are as follows:

- Storage of the subscriber data, for example, services available for this subscriber;
- Location registration and call handling, central store for subscriber location data;
- Support for encryption and authentication;
- Handling of supplementary services (e.g., barring or call transfer);
- Support for the short message service.

The HLR is implemented by an efficient real-time database system that may store the subscriber data of 1 million subscribers.

5.5.1.4 VLR

The VLR provides local storage for all of the variables and functions needed to handle calls to and from the mobile subscribers in the area related to that VLR. The information is stored in the VLR as long as the mobile station stays in that area. The VLR communicates with the HLR to inform it about the location of a subscriber and to obtain subscriber data that includes information about, for example, what services should be provided to this specific subscriber. The main functions of the VLR are as follows:

- Storage of data for subscribers located in its area;
- Management and allocation of the local identity codes to avoid frequent use of a global identity on the radio path for security reasons;
- Location registration and call handling;
- Authentication;
- Support of encryption;
- Support for handover;
- Handling of supplementary services;
- Support for SMS.

The VLR is a database system that is usually integrated in each mobi exchange MSC.

5.5.1.5 Authentication Center (AuC)

The security data of a subscriber are stored in the AuC that contains subscriber-specific security key, encryption algorithms, and a random ge erator. The AuC produces subscriber-specific security data with defined alg rithms and gives it to the HLR, which distributes them to the VLR. PLMN may contain one or more AuCs, and they can be separate netwo elements or integrated to the HLR. The same subscriber-specific key ar algorithms are also stored in SIM. There is no need to send them over t network and on the radio path.

5.5.1.6 Equipment Identity Register (EIR)

The EIR is a database that contains information about mobile terminal equipment. There is a white list for the terminals that are allowed to use the service, a gray list for terminals that need to be held under surveillance, and a black list for stolen mobile terminals. Those terminals whose serial numbers are found on the black list are not allowed to use the network.

5.5.1.7 Interworking Functions

The *interworking function* (IWF) is a functional entity associated with the gateway MSC. It enables interworking between a PLMN and a fixed network, for example, an ISDN, a PSTN, and a public switched data network. It is needed, for example, in the case of data transmission from GSM to PSTN. It converts digital transmissions used inside the GSM network to modem signals for PSTN. It has no functionality with the service that is directly compatible with that of the fixed network.

5.5.1.8 Transcoder and Rate Adapter Unit

A transcoder (TC) is needed to make conversions between GSM voice coding (13 or 7 Kbps) and PCM coding (64 Kbps), which is used in the fixed network. In the case of data transmission, transcoding is disabled. For data, a rate adapter unit (RAU) is needed to adapt SM data service to service provided by the external network. For example, if the GSM user has 14.4-Kbps data access to ISDN, RAU inserts its data into the 64-Kbps data stream of an ISDN B-channel in a specified way so that the other end knows where the user data can be found. The functions of the TC and RAU are often combined into a single piece of equipment called a *transcoder and rate adapter unit* (TRAU).

5.5.1.9 Echo Canceler (EC)

The EC is needed at the interface between a GSM network and the PSTN. The efficient speech coding of GSM introduces such a long delay that echoes reflected by a hybrid circuit in the subscriber interface of the fixed network (see Chapter 2) of the fixed service would be disturbing. The echo canceler eliminates this echo.

5.5.1.10 Short Message Service Center (SMSC)

GSM provides a paging service that is called short message service. The point-to-point SMS provides a mean of sending messages of a limited size to and from MSs. An SMSC acts as a store-and-forward center for these short messages. A short message transmitted by a subscriber is first forwarded through the network to the SMSC of his or her home network operator. The SMSC stores it, extracts the destination telephone number from the message, and forwards the message to its destination. The service center is not standardized as a part of a PLMN, but the GSM network has to support the transfer of short messages between SMSCs and the MSs.

5.5.1.11 Operation and Maintenance Center (OMC)

The OMC is a network management system for the remote O&M of a GSM network. The alarms of GSM network elements and traffic measurement reports are collected there. The O&M system handles features related to system security, faults, and network configuration updates.

5.5.1.12 Interfaces Inside GSM Network

The interface between the MSC and BSC is called the *A-interface* as shown in Figure 5.9. It is standardized and BSSs and MSCs from different vendors at the opposite side of the interface are compatible. Speech is PCM coded (see Chapter 3) at this interface. Another important interface is the *Abis-interface* between the BTS and BSC. At this interface speech is GSM coded, which requires less transmission capacity than the PCM coding. The Abis-interface is not completely standardized and, as a consequence, both BTSs and BSCs have to be purchased from the same manufacturer. The Ater-interface is not standardized either but it is used for terrestrial connections between the BSC and MSC. Speech is GSM coded at the Ater-interface and the transmission capacity needed at the Ater-interface is one-fourth of the capacity of the A-interface.

5.5.2 Physical Channels

The multiple-access scheme used in GSM utilizes two access methods, FDMA and TDMA. Up to eight users may share one of the 200-kHz frequency channels, which is divided into eight time slots.

5.6 Operation of the GSM Network

In this section we introduce the operating principles of a cellular network. To do this, we illustrate the GSM network with a few simplified examples. They show how location update is performed, how a mobile call is established, how handover is performed, and what the security functions of the GSM network are.

Each GSM subscriber is registered into one HLR of his or her home network. This HLR is the central point that provides subscriber information regardless of where he or she is presently located.

5.6.1 Location Update

The cellular mobile network has to be aware of the location of its subscribers at all times to be able to route incoming calls to them. The location update procedure takes place every time a MS moves to another location area or when a user switches her telephone on in a different location than where she was located previously.

The geographical position of a GSM mobile is known at the accuracy of a *location area* (LA), which typically consists of a number of cells. The BTSs of those cells need not be connected to the same BSC. When an incoming call to a mobile subscriber arrives, it is paged through all the cells belonging to the LA where this specific subscriber is known to be.

The MS is responsible for location updates and performs this updating in idle mode, that is, when a call is not connected.

The MS surveys the radio environment constantly and, when it detects that it could be served best in a new LA, performs a normal location update procedure to change the location information in its present VLR and in the HLR (if needed). We say that the mobile station has roamed to another LA. In dedicated mode, during a call, the procedure called handover, which we will discuss later, may be required. If the LA is changed during a call, the location update takes place after the call is cleared.

Location update may take place inside one network when the LA is changed or between different networks that may be located in different countries. The latter case requires a roaming agreement between network operators to allow a subscriber to use the other network in addition to her home network. Figure 5.11 illustrates the location update procedure that

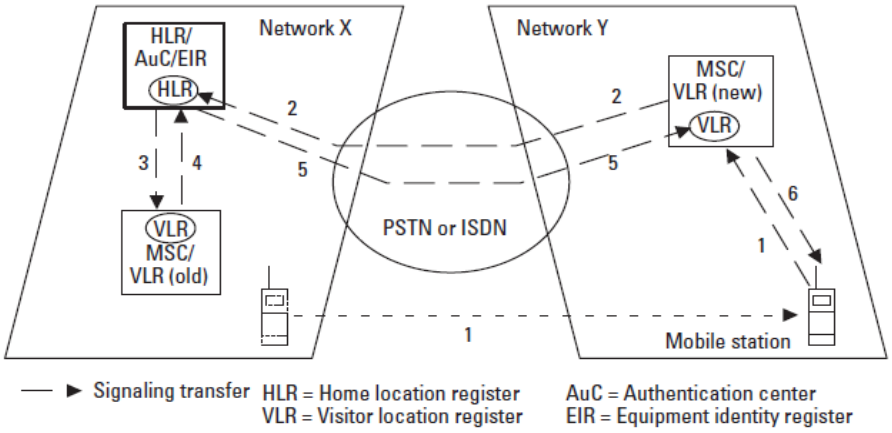

Figure 5.11 Location update in GSM network.

occurs when a mobile station is switched on in another network Y in another country. This example assumes that the mobile station has been switched off in the home network, network X, and that the network operators of networks Y and X have a roaming agreement that allows cellular subscribers to use the services of another network.

For location update the following main operations are carried out (see Figure 5.11):

1. When the MS has roamed to another LA, it scans the common control channels. When it finds a common control channel, it detects the LA code, which contains country and network identifications. If the MS cannot find the same LA code it has stored previously, it requests a location update from the network.
2. The MSC/VLR requests the global identity code of the mobile [*international mobile identity subscriber* (IMSI) stored into SIM, not the same as the telephone number]. With the help of this, the MSC/VLR knows in which country the home network of this mobile is found. The MSC/VLR sends a signaling message via the international CCS7 signaling network toward the home country of this cellular subscriber. The message includes country code, network code, and subscriber identity. The message also includes the address of this new VLR to inform the HLR about the new location of the MS.
3. When the HLR receives the message it requests the former "old" VLR, where this subscriber was previously located, to remove information about the subscriber.
4. The VLR (old) acknowledges and removes the subscriber information from its database.
5. The HLR updates the location information and sends the subscriber information, including security codes, to the new VLR.
6. The (new) MSC/VLR stores the subscriber information, performs authentication of the MS, and acknowledges location update. The MS will now show the name of network Y on its screen.

5.6.2 Mobile Call

Figure 5.12 illustrates how the GSM network routes a call to a subscriber who has roamed to another network. We assume here that both the calling and called subscribers are originally registered in the same home network, network X. Called subscriber B has traveled to another network Y and switched on her MS. Then the location update, which was illustrated in the previous section, takes place. Then mobile user A calls MS B from the home network.

We can identify the following main phases when the call is established from MS A in the home network to MS B located in another network (Figure 5.12).

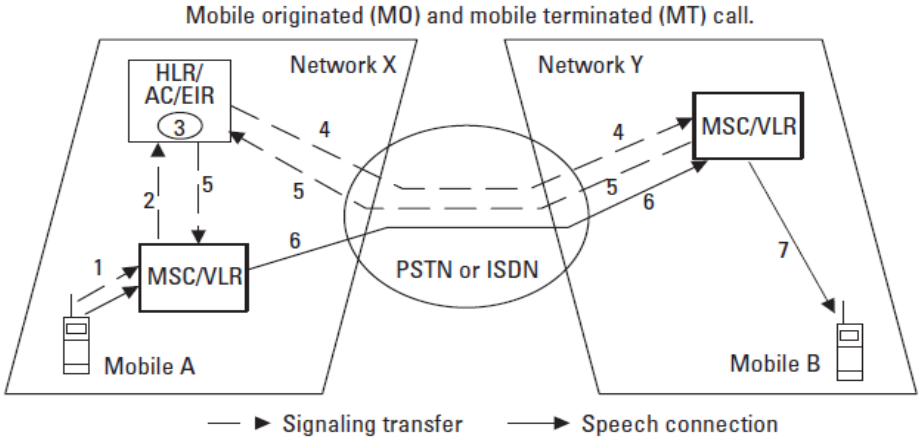

Figure 5.12 Mobile call in a cellular network.

1. MS A initiates a call to MS B, which is currently located in another network. The call connection request and other signaling information are transmitted via the radio path and BSS to the MSC. The telephone number of subscriber B is transmitted to the MSC/VLR.
2. The MSC recognizes mobile B (in this example) as a subscriber of its own network and requests the roaming number from the HLR of subscriber B. The roaming number is a temporary telephone number that is used for call establishment via a PSTN.
3. The HLR of subscriber B knows the identification of the "visited" VLR where mobile B is currently located. When mobile B was switched on, the MSC/VLR of network Y sent its address to the HLR (location update). The HLR builds up a signaling message that includes the identification of called subscriber B together with the address of the visited MSC/VLR.
4. The HLR requests the visited VLR to provide a roaming number.
5. The MSC/VLR of network Y has a pool of roaming numbers that look like the ordinary telephone numbers of that country. The visited MSC/VLR then allocates one roaming number to subscriber B, stores it in its database, and sends it to the HLR, which then forwards it to the MSC/VLR in network X.
6. The MSC/VLR of network X routes the call toward the MSC/VLR in network Y using the roaming number for dialing digits and the call is then routed the same way as any other telephone call.
7. When the MSC/VLR in network Y receives the call identified by the previously allocated roaming number, it associates this with subscriber B and initiates paging toward MS B. The roaming number is then released for reuse.

To keep Figure 5.12 simple, the GMSCs at the border of networks X and Y are not shown as separate network elements. There is always at least one GMSC in each individual GSM network. The GMSC is a signaling interface point to other networks and it is able, for example, to route signaling messages toward the right HLR inside its own network.

The telephone call to a roamed subscriber is currently always connected via the GMSC of the home network, and the roamed subscriber pays for the connection from the home network to his or her present location. Later it may become possible to connect calls directly.

5.6.3 Handover or Handoff

The main reason to perform handover is to maintain call connection regardless of the movement of the MS over cell boundaries. The structure of a GSM network requires the possibility to execute handovers at four levels, as shown in Figure 5.13.

The BSC is responsible for handover because it occurs most often between two cells under one BSC. The handover process should be as quick as possible so that communication is not disturbed. To perform handover quickly, the BSC collects measurement data from MSs and BTSs, processes it, and updates ordered candidate cell lists for handover for all the MSs that have an ongoing call.

Handover is most often necessary between BTSs of neighboring cells, case (b) in Figure 5.13, which are controlled by the same BSC. The BSC controls the handover and performs the channel switch from an "old" cell to a "new" cell. Sometimes there may be a need to switch communication from one channel to another in the same BTS [case (a) in Figure 5.13]. This may be necessary because of temporary interference. Also this handover is controlled and performed by the BSC.

The inter-BSC handover, case (c) in Figure 5.13, occurs if an MS moves to a neighboring cell that is controlled by a different BSC. Now the BSC cannot perform switching. Instead, it has to request the MSC to execute the handover switching to the target cell. When a new connection is

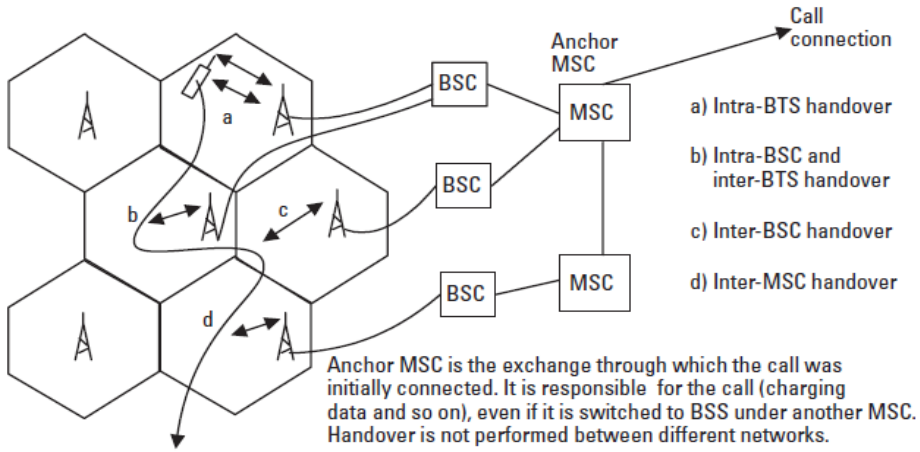

Figure 5.13 The four different cases of handover.

established from the MSC to the new BTS and the MS accesses the new channel, the MSC performs the switching.

When the neighbor cell is located under a different MSC, an inter-MSC handover may be required. Then the BSC requests the anchor MSC to establish the connection with the help of a new MSC to the new cell. The anchor MSC performs the switching. The anchor MSC is the exchange via which the call was originally connected. The anchor MSC controls the call until it is cleared even though it may use other MSCs to maintain the call through handovers.

Handover can also be executed to arrange traffic between cells to avoid unsuccessful calls due to geographically uneven load. In this case the calls of the MSs that are located close to the border of a loaded cell are switched to a neighboring cell that has more free capacity.

As an example we now look at how the most complicated handover, inter-MSC handover, is performed. The handover procedure between two MSCs, shown in Figure 5.14, includes the following main phases:

1. The mobile station moves across the cell border and the BSC (old) decides to initiate handover to another cell (new). The decision is based on the measurement information sent by the mobile and by the BTS. The measurement information includes, in addition to traffic channel measurement results, identifications of neighboring cells and the measurement results of them. The mobile station continuously measures the common channel of each neighbor cell in addition to the traffic channel in use for the call.
2. The BSC (old) notices that the best cell candidate is not under its control and requests the MSC (old) to begin handover preparation to the new cell. The MSC (old) recognizes that the proposed cell (new) is connected to another MSC.
3. The MSC (old) requests a handover number from MSC (new). The handover number is a temporary telephone number that is used to establish a connection via PLMN, ISDN, or PSTN for the handover.
4. The new MSC requests allocation of a traffic channel from the BSC (new).
5. The BSC (new) allocates the channel and informs the MSC (new).
6. The MSC (new) allocates a handover number and sends it to the MSC (old).
7. The MSC (old) routes a call toward the MSC (new) using the handover number as dialed digits.
8. When the routing is complete and channel is established from the anchor MSC to the new cell, the new MSC/VLR commands the mobile station, via the MSC (old), to switch to the new traffic channel (frequency and time slot of the new cell) and MSC (old) to perform switching.
9. The old MSC switches to the new channel and the new MSC and BSC connect the speech path through the reserved channels in the new cell. Notice that the call is still controlled by the old MSC, which has the role of anchor MSC and it, for example, produces charging records. Finally, the channel of the old cell is released.

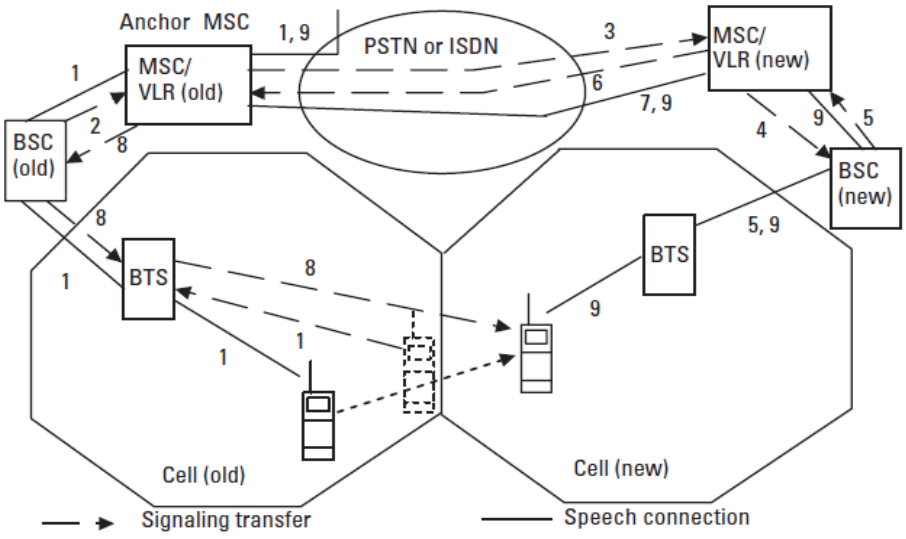

Figure 5.14 Handover or handoff between two MSCs.

5.6.4 GSM Security Functions

In the GSM special attention is paid to security aspects, such as security against forgery and theft, security of speech and data transmission, and security of the subscriber's identity. Use of a radio transmission makes the PLMNs particularly sensitive to the misuse of resources by unauthorized persons and the eavesdropping of information exchanged on the radio path.

For security functions the AuC delivers random numbers and precalculated keys for authentication and ciphering to the HLR. It then sends them with other subscriber information to the VLR, where location update is performed.

We now review the four most important security functions of GSM network, which are shown in Figure 5.15. In addition to these functions, the GSM SIM card is protected by a *personal identity number* (PIN), similar to a credit card "password." The ME may also provide additional security features.

5.6.4.1 Authentication

For authentication AuC provides authentication triplets to the VLR via the HLR. These include a signed response, random number, and ciphering key. Each triplet is used only once and AuC delivers new triplets on demand.

The principle of authentication is to compare the subscriber authentication key Ki in the authentication center and in the SIM without ever sending the Ki on the radio path. For authentication the network sends a random number to the mobile at the beginning of each call. The SIM then uses an algorithm, A3, to process a response that is dependent on the random number as well as on the secret subscriber specific key stored in the SIM. The AuC has also computed this response, called *signed response* (SRES), and delivered it in the authentication triplet to the VLR. The VLR performs a comparison and if they match, the MS is allowed to use the network.

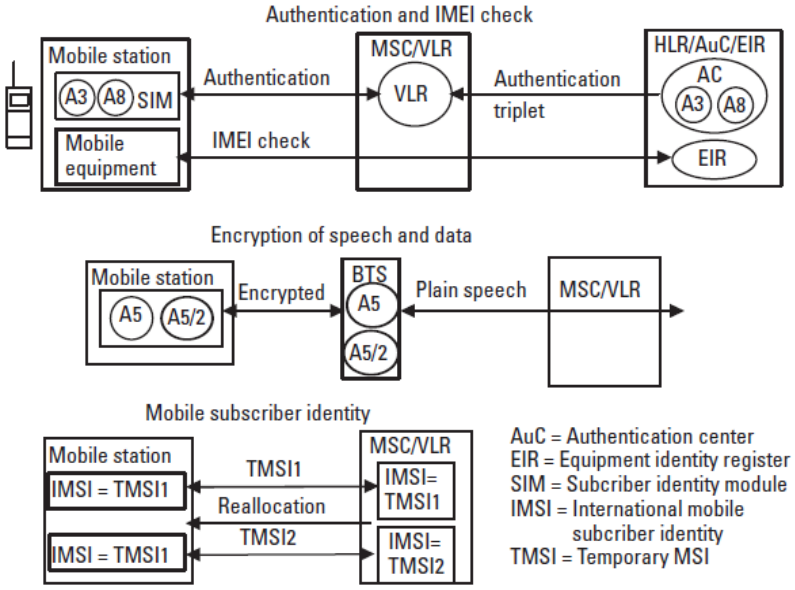

Figure 5.15 The security functions of GSM.

5.6.4.2 IMEI Check

The *international mobile equipment identity* (IMEI) check procedure is used to ensure that the mobile equipment does not belong to the black list where the EIR stores the serial numbers of stolen mobiles. If an IMEI is found on the black list, a connection cannot be established. The IMEI is a manufacturer-specific code that is stored in each piece of mobile equipment when manufactured.

5.6.4.3 Encryption of Speech and Data

Speech and data are encrypted before forwarding the radio or air interface. The main algorithm for ciphering is A5, which defines how the ciphering sequence is generated. For encryption an exclusive-or operation is performed with data and the ciphering sequence. An encryption algorithm uses the ciphering key that is calculated by the authentication center and by the SIM. The ciphering key depends on the subscriber-specific key together with the random number that is given to the mobile station at the beginning of each call.

5.6.4.4 Mobile Subscriber Identity

The MS is normally addressed over the air interface by using a *temporary mobile subscriber identity* (TMSI), which is allocated for each mobile located inside an LA. The global identity of the mobile, *international mobile subscriber identity* (IMSI), which is stored into SIM, is very seldom sent over the air interface to prevent eavesdropping devices from using it as trigger information. A new TMSI is allocated for the next call when communication is in ciphered mode.

IMSI is a global subscriber identification but it is not the same as the telephone number. A subscriber may have several telephone numbers, for example, one for telephone and one for fax, connected to one IMSI in the HLR. He or she may also change SIM (IMSI is changed) but keep the same telephone number.

5.7 GPRS

GPRS will surpass HSCSD because it provides optimum service for data users. It is a genuine packet-switched system in which the radio channel is

reserved only for the time during which data transmission takes place. It supports asymmetrical transmission and radio resources in uplink and downlink directions are assigned independently. The radio channel is reserved only for the time of transmission although a virtual connection (see Section 6.2) exists at all times for each GPRS subscriber.

GPRS users share physical channels allocated for packet-switched service. It offers a real packet access method and supports charging based on the amount of transferred data.

5.7.1 GPRS Network Structure

Because GSM was originally designed for circuit-switched service, the introduction of packet-switched transmission requires some significant functional and operational changes. GPRS introduces two new network nodes, *GPRS support nodes* (GSN) to support end-to-end packet transfer. They are *serving GPRS support node* (SGSN) and *gateway GPRS support node* (GGSN), which are shown in the simplified network architecture in Figure 5.16. To keep the figure simple, many GSM network elements, such as EIR and SMSC, have been excluded. Circuit-switched calls are routed from the BSC via the MSC to PSTN.

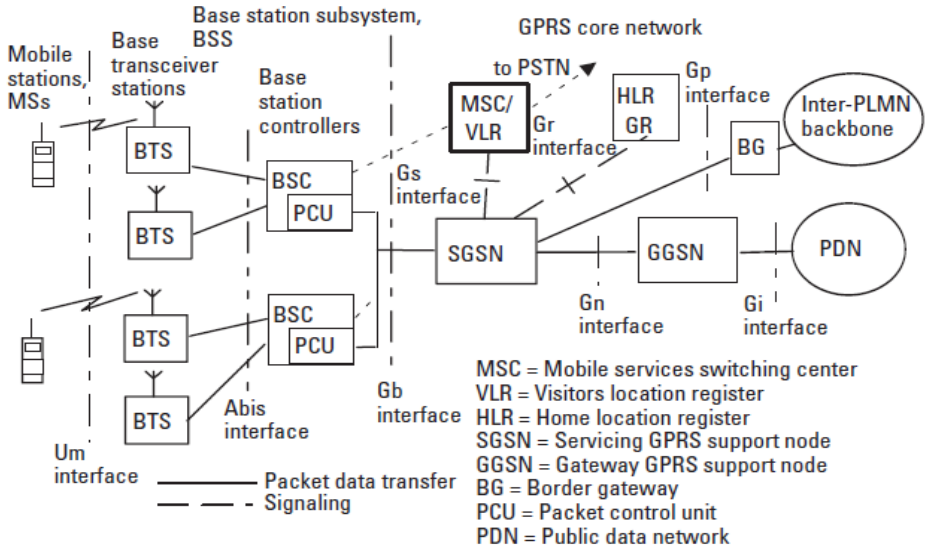

Figure 5.16 GPRS system architecture.

For GPRS operation the HLR is enhanced with GPRS subscriber data and routing information. The HLR is to be updated to include *GPRS register* (GR), which stores packet user related data, such as IP address of the present SGSN. The GR stores routing information (SGSN address) and maps IMSI to one or more *Packet Data Protocol* (PDP) addresses if addresses are permanently assigned to subscribers. Typically, an *Internet Protocol* (IP) address is assigned for a subscriber on demand, that is, when she attaches GPRS. Dynamic address is released in GPRS detach, when the MS is disconnected from the GPRS network. The major upgrades in the BS subsystem are new channel coders in BTSs and *packet control units* (PCUs) in BSCs. PCUs take care of the packet transmission between MSs and SGSN.

5.7.2 GPRS Network Elements

GPRS is designed to leave BSSs almost unchanged. A PCU is added to the BSS and it routes packet-switched data to a separate GPRS core network. The roles of the new network elements are introduced below.

5.7.2.1 SGSN

The SGSN support node is responsible for the delivery of packets to all MSs within its service area. SGSN plays the same role in GPRS as MSC/VLR in the circuit-switched GSM network. It detects new MSs in its area, performs authentication, ciphering, and IMEI check, and it sends and receives packets to and from the MS. It also collects *charging data records* (CDRs), performs session and mobility management, and supports SMS. Mobility management contains GPRS attach/detach, routing area update, location area update, cell change (in ready mode), and paging. Cell change corresponds to handover and for that SGSN takes care that unacknowledged packets are routed to a new cell and possibly to the new SGSN if the new cell is under different SGSN. Session management contains PDP context activation, deactivation, and modification. PDP context activation means establishment of a "virtual circuit" between the MS and GGSN for IP packet transfer. The SGSN handles protocol conversion between the IP protocol and the LLC protocol that is used between SGSN and MS. The SGSN performs TCP/IP compression according to RFC 1144 to save radio capacity [3].

5.7.2.2 GGSN

The GGSN support node acts as a logical interface to external packet data networks. GGSN acts as a router and hides the GPRS network infrastructure from the external networks. GGSN remains an anchor point when SGSN is

changed due to a cell change. When the GGSN receives a packet addressed to a specific user, it checks its database to determine if the address is active. If it is, GGSN uses its PDP context (containing SGSN address for tunneling) to forward the packet to the relevant SGSN. If the address is not active, the data are discarded. GGSN collects charging information based on usage of network resources.

The GGSN corresponds to the GMSC in circuit-switched operation. The main function of GGSN is to handle interactions with external data network. It acts as a router hiding the GPRS network from the external network, typically the Internet. GGSN updates the location of the MS according to the information from SGSNs and routes packets to and from the SGSN, which serves the destination MS.

Within the GPRS network, PDUs or packets are encapsulated at the originating GSN (either SGSN or GGSN) and decapsulated at the destination GSN. In between the GSNs, IP tunneling is used to transfer PDUs. This means that a user data packet is inserted into an IP packet, which contains the IP address of the destination GSN (see Section 6.6.4). The GGSN maintains routing information used to tunnel packets to the SGSN that is currently serving the destination MS. All GPRS user-related data, needed by the SGSN to perform the routing and data transfer functionality, are stored within the GR/HLR.

5.7.2.3 PCU

The BSC is upgraded with a PCU, which supports all GPRS protocols and controls and manages most of the radio-related functions of GPRS. It splits up long LLC frames into short RLC frames for ratio transmission. The PCU's function is to set up, supervise, and disconnect packet-switched calls. It also supports cell change, radio resource configuration, and channel assignment. The BTS is merely relay equipment without protocol functions and it performs the modulation, demodulation, and channel measurements. The PCU may be located anywhere between the SGSN and the BTS [3].

5.7.2.4 Border Gateway (BG)

The BG is not specified by GPRS specifications and PLMN operators have to define its functionality in their roaming agreements. It may contain firewall functions to ensure secure connections over the inter-PLMN backbone network. The BG may be integrated into the GGSN.

The GPRS network contains some network elements that are not shown in Figure 5.16. Two important examples of these are the *charging gateway* (CG), which collects charging information from SGSN and GGSN and sends it to the billing system, and the *domain name server* (DNS), which maps logical domain names to IP address numbers the same way as in any IP network (see Section 6.6.10).

5.7.2.5 GPRS Network Interfaces

Several interfaces are defined in GPRS standards, the most important of which are as follows:

- Gb, between BSS and SGSN;
- Gn, between SGSN and GGSN;
- Gi, between GGSN and external network;
- Gs, between SGSN and VLR;
- Gr, between SGSN and HLR.

Interface specifications define protocols needed for packet-switched operation. Typically IP packets are transmitted from the MS to the external PDN and additional IP tunneling is used in the GPRS core network.

5.7.2.6 MS

GPRS requires completely new terminals, which can be regular mobile telephones, PC cards, or specific modules built in to a machine. These terminals are divided into three classes:

1. *Class A terminals* can handle both circuit-switched and packet-switched services simultaneously and independently.
2. *Class B terminals* can handle either circuit- or packet-switched service at one time. It can automatically switch between these two modes. For example, in the case of an incoming circuit-switched call, it may suspend packet transfer and resume it afterward.
3. *Class C terminals* must be manually set into one of the modes. In the circuit-switched mode, it is cannot be accessed for packet-switched traffic and vice versa. A special case of class C mobile is a packet-only terminal integrated into laptop.

5.7.3 Operation of GPRS

GPRS provides genuine packet-switched radio access and packet service users share the radio channels allocated for GPRS. Information about whether the

network provides GPRS service and which channels (frequencies and time slots) are allocated for packet users is broadcast on the cell broadcast channel.

HLR/GR stores information about the services and present location of its MSs (SGSN). SGSN, which corresponds to MSC/VLR, stores more accurate location of MSs and data related to their current service, such as the current IP address. It also performs security functions, such as authentication.

When a GPRS user wants to access a packet-switched service, for example, the Internet, he or she performs GPRS attach. Then IP address is allocated for the MS and the user sees the Web page of his or her ISP's browser. The URL (see Section 6.6.11) of this default page is stored in his or her subscriber information in HLR/GR and transferred to SGSN at the time of GPRS attach. The GGSN in Figure 5.16 acts as a border router between GPRS and the Internet; the GPRS network looks the same as any other IP network from outside the Internet. The GGSN stores the routing table for all active IP addresses to be able to route packets to the correct SGSN. The SGSN then routes packets further to the cell where the destination MS is currently located.

Physical radio channel, one time slot in each TDMA frame, transmits data blocks that occupy one time slot in four subsequent TDMA frames. Multiple users share each physical channel and each downlink packet contains identification of the destination MS. In the uplink direction, some data blocks are reserved for uplink channel requests from MSs. When an MS wants to transmit packet data it requests an uplink packet channel. According to these requests, SGSN assigns uplink capacity to MSs. Each downlink data block contains MS identification that is allowed to transmit the next block in the uplink direction.

We see that a mobile station can be connected to GPRS service continuously, but it reserves capacity only if it needs to transmit or receive. Charging can be based on a low fixed monthly fee and the fee based on the amount of transmitted and received data. This is makes GPRS superior to earlier circuit-switched alternatives, such as HSCSD.

5.8 Problems and Review Questions

Problem 5.1

What are the main advantages of cellular systems compared with the old generation radio telephone systems that did not utilize a cellular network structure?

Problem 5.2

An analog radio telephone network has a frequency band of 100 (bidirectional) FDMA channels. The network covers a 50 × 50–km urban area. Give the maximum number of simultaneous calls in the network if (a) only one base station is in use; (b) the network is upgraded to a cellular network with a cell size of 10 × 10 km and the frequency reuse ratio is 1:9 (each channel is used again in every ninth cell); (c) cell size is reduced to 1 × 1 km; and (d) cell size is reduced further to 0.35 × 0.35 km (that is, equal to the minimum size of cells in early GSM). For simplicity, assume here that the cells are rectangular and all channels are used as traffic channels. [*Hint:* Divide all channels of the network between a cell cluster (group) of nine cells. Then repeat this cluster to cover the geographical area of the network.]

Problem 5.3

What are the two main types of channels used in each cell of a cellular mobile system?

Problem 5.4

What is handover? Explain the handover principle, that is, how it is carried out in a cellular network.

Problem 5.5

How does the cellular network route an incoming call to a subscriber located anywhere in the network or even in a different country? What are the roles of the HLR and VLR in the routing of an incoming call?

Problem 5.6

Explain the main phases that occur in the radio interface of a cell when an outgoing call is requested. Explain also what happens when an MS in a cellular network receives an incoming call.

Problem 5.7

Explain the applications of cordless telephones. How do cordless systems basically differ from cellular systems?

Problem 5.8

Explain the structure of a GSM network. What are the main network elements and what are their roles in the operation of GSM?

Problem 5.9

Explain the multiple-access method of GSM.

Problem 5.10

Explain how location update is performed in GSM. What triggers it and what happens after that?

Problem 5.11

Explain how a call is routed from a GSM MS to another MS of the same home network. Assume that (a) both are located in home network and (b) both have roamed to another country.

Problem 5.12

Explain how handover is performed in the GSM network.

Problem 5.13

Explain the security functions implemented in the GSM network.

Problem 5.14

What are the main new network elements that are needed in GPRS network? What are their roles in GPRS operation?

Problem 5.15

What are the basic operating differences between GPRS and circuit-switched GSM?

References

[1] Redl, M. S., M. K. Weber, and M. W. Oliphant, *An Introduction to GSM,* Norwood, MA: Artech House, 1995.

[2] Mouly, M., and M. B. Pautet, *The GSM System for Mobile Communications,* Paris, France: Michel Mouly and Marie-Bernadette Pautet, 1992.

[3] Heine, G.A., and Inacon GmbH, *GPRS from A–Z,* Norwood, MA: Artech House, 2000.