GSM

11.3 Global System for Mobile (GSM)

Global System for Mobile (GSM) is a second generation cellular system standard that was developed to solve the fragmentation problems of the first cellular systems in Europe. GSM was the world's first cellular system to specify digital modulation and network level architectures and services, and is the world's most popular 2G technology. Before GSM, European countries used different cellular standards throughout the continent, and it was not possible for a customer to use a single subscriber unit throughout Europe. GSM was originally developed to serve as the pan-European cellular service and promised a wide range of network services through the use of ISDN. GSM's success has exceeded the expectations of virtually everyone, and it is now the world's most popular standard for new cellular radio and personal communications equipment throughout the world. As of 2001, there were over 350 million GSM subscriers worldwide.

The task of specifying a common mobile communication system for Europe in the 900 MHz band was taken up in the mid-1980s by the GSM (Groupe spécial mobile) committee which was a working group of the CEPT. In 1992, GSM changed its name to the *Global System for Mobile Communications* for marketing reasons [Mou92]. The setting of standards for GSM is under the aegis of the European Technical Standards Institute (ETSI).

GSM was first introduced into the European market in 1991. By the end of 1993, several non-European countries in South America, Asia, and Australia had adopted GSM and the technically equivalent offshoot, DCS 1800, which supports Personal Communication Services (PCS) in the 1.8 GHz to 2.0 GHz radio bands recently created by governments throughout the world.

ISDN → Integrated Services digital N/w.
– Common channel signalling.

11.3.1 GSM Services and Features

GSM services follow ISDN guidelines and are classified as either *teleservices* or *data services*. Teleservices include standard mobile telephony and mobile-originated or base-originated traffic. Data services include computer-to-computer communication and packet-switched traffic. User services may be divided into three major categories:

- **Telephone services**, including emergency calling and facsimile. GSM also supports Videotex and Teletex, though they are not integral parts of the GSM standard.
- **Bearer services** or **data services** which are limited to layers 1, 2, and 3 of the open system interconnection (OSI) reference model (see Chapter 10). Supported services include packet switched protocols and data rates from 300 bps to 9.6 kbps. Data may be transmitted using either a transparent mode (where GSM provides standard channel coding for the user data) or nontransparent mode (where GSM offers special coding efficiencies based on the particular data interface).
- **Supplementary ISDN services**, are digital in nature, and include call diversion, closed user groups, and caller identification, and are not available in analog mobile networks. Supplementary services also include the *short messaging service* (SMS) which allows GSM subscribers and base stations to transmit alphanumeric pages of limited length (160 7 bit ASCII characters) while simultaneously carrying normal voice traffic. SMS also provides *cell broadcast*, which allows GSM base stations to repetitively transmit ASCII messages with as many as fifteen 93-character strings in concatenated fashion. SMS may be used for safety and advisory applications, such as the broadcast of highway or weather information to all GSM subscribers within reception range.

From the user's point of view, one of the most remarkable features of GSM is the *Subscriber Identity Module* (SIM), which is a memory device that stores information such as the subscriber's identification number, the networks and countries where the subscriber is entitled to service, privacy keys, and other user-specific information. A subscriber uses the SIM with a four-digit personal ID number to activate service from any GSM phone. SIMs are available as smart cards (credit card sized cards that may be inserted into any GSM phone) or plug-in modules, which are less convenient than the SIM cards but are nonetheless removable and portable. Without a SIM installed, all GSM mobiles are identical and nonoperational. It is the SIM that gives GSM subscriber units their identity. Subscribers may plug their SIM into any suitable terminal—such as a hotel phone, public phone, or any portable or mobile phone—and are then able to have all incoming GSM calls routed to that terminal and have all outgoing calls billed to their home phone, no matter where they are in the world.

A second remarkable feature of GSM is the on-the-air privacy which is provided by the system. Unlike analog FM cellular phone systems which can be readily monitored, it is virtually impossible to eavesdrop on a GSM radio transmission. The privacy is made possible by encrypting the digital bit stream sent by a GSM transmitter, according to a specific secret cryptographic

key that is known only to the cellular carrier. This key changes with time for each user. Every carrier and GSM equipment manufacturer must sign the Memorandum of Understanding (MoU) before developing GSM equipment or deploying a GSM system. The MoU is an international agreement which allows the sharing of cryptographic algorithms and other proprietary information between countries and carriers.

11.3.2 GSM System Architecture

The GSM system architecture consists of three major interconnected subsystems that interact between themselves and with the users through certain network interfaces. The subsystems are the *Base Station Subsystem* (BSS), *Network and Switching Subsystem* (NSS), and the *Operation Support Subsystem* (OSS). The *Mobile Station* (MS) is also a subsystem, but is usually considered to be part of the BSS for architecture purposes. Equipment and services are designed within GSM to support one or more of these specific subsystems.

The BSS, also known as the *radio subsystem*, provides and manages radio transmission paths between the mobile stations and the Mobile Switching Center (MSC). The BSS also manages the radio interface between the mobile stations and all other subsystems of GSM. Each BSS consists of many Base Station Controllers (BSCs) which connect the MS to the NSS via the MSCs. The NSS manages the switching functions of the system and allows the MSCs to communicate with other networks such as the PSTN and ISDN. The OSS supports the operation and maintenance of GSM and allows system engineers to monitor, diagnose, and troubleshoot all aspects of the GSM system. This subsystem interacts with the other GSM subsystems, and is provided solely for the staff of the GSM operating company which provides service facilities for the network.

Figure 11.5 shows the block diagram of the GSM system architecture. The Mobile Stations (MSs) communicate with the Base Station Subsystem (BSS) over the radio air interface. The BSS consists of many BSCs which connect to a single MSC, and each BSC typically controls up to several hundred *Base Transceiver Stations* (BTSs). Some of the BTSs may be co-located at the BSC, and others may be remotely distributed and physically connected to the BSC by microwave link or dedicated leased lines. Mobile handoffs (called *handovers*, or HO, in the GSM specification) between two BTSs under the control of the same BSC are handled by the BSC, and not the MSC. This greatly reduces the switching burden of the MSC.

As shown in Figure 11.6, the interface which connects a BTS to a BSC is called the *Abis interface*. The Abis interface carries traffic and maintenance data, and is specified by GSM to be standardized for all manufacturers. In practice, however, the Abis for each GSM base station manufacturer has subtle differences, thereby forcing service providers to use the same manufacturer for the BTS and BSC equipment.

The BSCs are physically connected via dedicated/leased lines or microwave link to the MSC. The interface between a BSC and a MSC is called the *A interface*, which is standardized within GSM. The A interface uses an SS7 protocol called the *Signaling Correction Control Part*

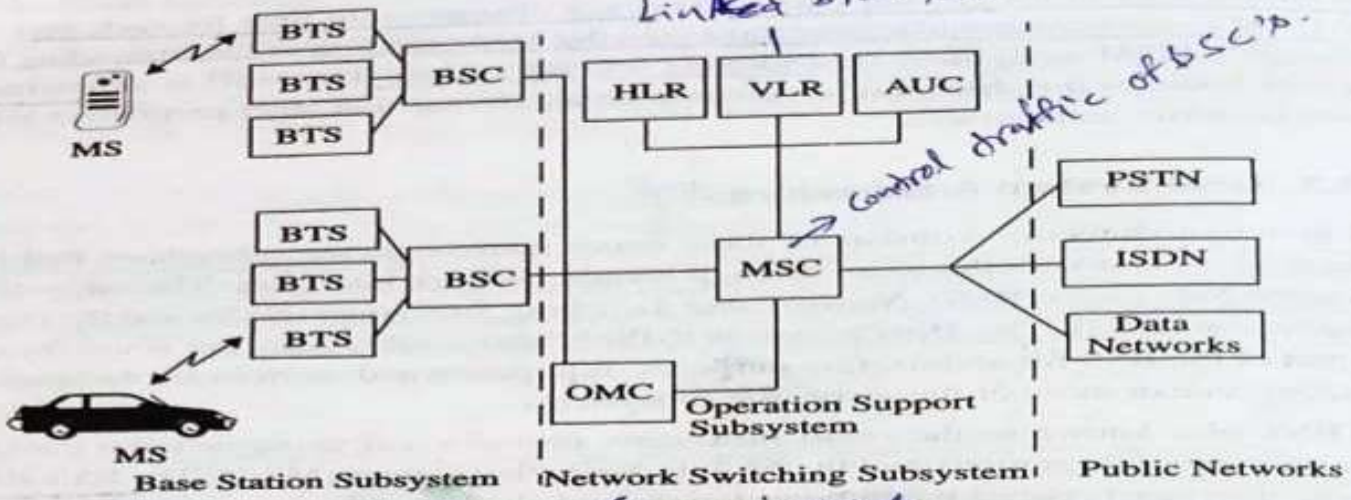


Figure 11.5 GSM system architecture.

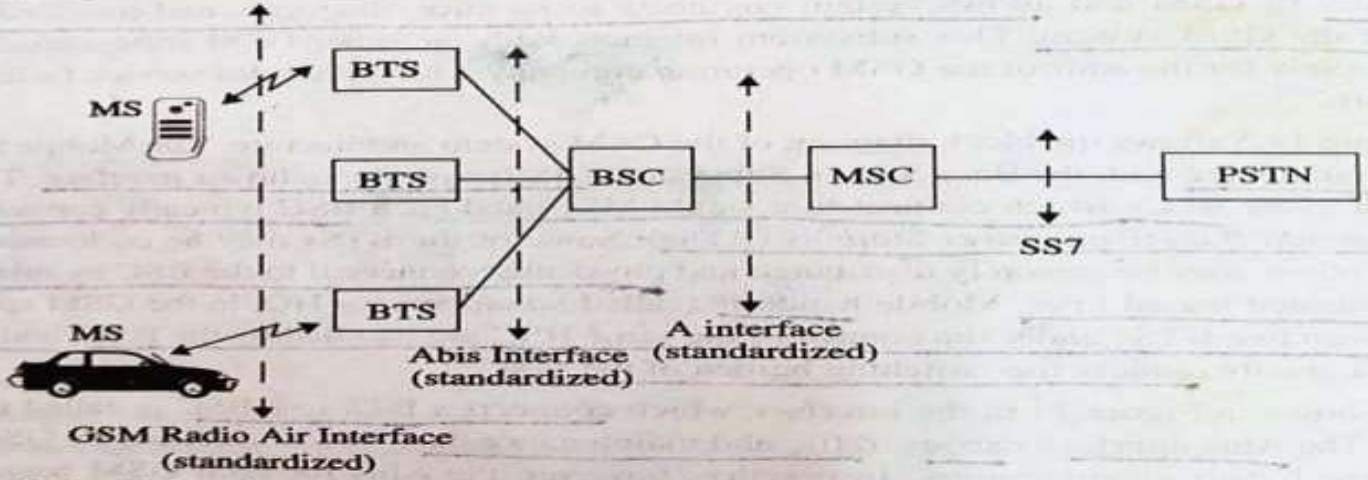


Figure 11.6 The various interfaces used in GSM.

(SCCP) which supports communication between the MSC and the BSS, as well as network messages between the individual subscribers and the MSC. The A interface allows a service provider to use base stations and switching equipment made by different manufacturers.

The NSS handles the switching of GSM calls between external networks and the BSCs in the radio subsystem and is also responsible for managing and providing external access to several customer databases. The MSC is the central unit in the NSS and controls the traffic among all of the BSCs. In the NSS, there are three different databases called the *Home Location Register* (HLR), *Visitor Location Register* (VLR), and the *Authentication Center* (AUC). The HLR is a database which contains subscriber information and location information for each user who resides in the same city as the MSC. Each subscriber in a particular GSM market is assigned a unique *International Mobile Subscriber Identity* (IMSI), and this number is used to identify each home user. The VLR is a database which temporarily stores the IMSI and customer information for each roaming subscriber who is visiting the coverage area of a particular MSC. The VLR is linked between several adjoining MSCs in a particular market or geographic region and contains subscription information of every visiting user in the area. Once a roaming mobile is logged in the VLR, the MSC sends the necessary information to the visiting subscriber's HLR so that calls to the roaming mobile can be appropriately routed over the PSTN by the roaming user's HLR. The Authentication Center is a strongly protected database which handles the authentication and encryption keys for every single subscriber in the HLR and VLR. The Authentication Center contains a register called the *Equipment Identity Register* (EIR) which identifies stolen or fraudulently altered phones that transmit identity data that does not match with information contained in either the HLR or VLR.

The OSS supports one or several *Operation Maintenance Centers* (OMC) which are used to monitor and maintain the performance of each MS, BS, BSC, and MSC within a GSM system. The OSS has three main functions, which are 1) to maintain all telecommunications hardware and network operations with a particular market, 2) manage all charging and billing procedures, and 3) manage all mobile equipment in the system. Within each GSM system, an OMC is dedicated to each of these tasks and has provisions for adjusting all base station parameters and billing procedures, as well as for providing system operators with the ability to determine the performance and integrity of each piece of subscriber equipment in the system.

11.3.3 GSM Radio Subsystem

GSM originally used two 25 MHz cellular bands set aside for all member countries, but now it is used globally in many bands. The 890–915 MHz band was for subscriber-to-base transmissions (reverse link), and the 935–960 MHz band was for base-to-subscriber transmissions (forward link). GSM uses FDD and a combination of TDMA and FHMA schemes to provide multiple access to mobile users. The available forward and reverse frequency bands are divided into 200 kHz wide channels called ARFCNs (Absolute Radio Frequency Channel Numbers). The ARFCN denotes a forward and reverse channel pair which is separated in frequency by 45 MHz and each channel is time shared between as many as eight subscribers using TDMA.

Each of the eight subscribers uses the same ARFCN and occupies a unique timeslot (TS) per frame. Radio transmissions on both the forward and reverse link are made at a channel data rate of 270.833 kbps (1625.0/6.0 kbps) using binary $BT = 0.3$ GMSK modulation. Thus, the signaling bit

duration is 3.692 μs, and the effective channel transmission rate per user is 33.854 kbps (270.833 kpbs/8 users). With GSM overhead (described subsequently), user data is actually sent at a maximum rate of 24.7 kbps. Each TS has an equivalent time allocation of 156.25 channel bits, but of this, 8.25 bits of guard time and six total start and stop bits are provided to prevent overlap with adjacent time slots. Each TS has a time duration of 576.92 μs as shown in Figure 11.7, and a single GSM TDMA frame spans 4.615 ms. The total number of available channels within a 25 MHz bandwidth is 125 (assuming no guard band). Since each radio channel consists of eight time slots, there are thus a total of 1000 traffic channels within GSM. In practical implementations, a guard band of 100 kHz is provided at the upper and lower end of the GSM spectrum, and only 124 channels are implemented. Table 11.3 summarizes the GSM air interface.

The combination of a TS number and an ARFCN constitutes a *physical channel* for both the forward and reverse link. Each physical channel in a GSM system can be mapped into different *logical channels* at different times. That is, each specific time slot or frame may be dedicated to either handling traffic data (user data such as speech, facsimile, or teletext data), signaling data (required by the internal workings of the GSM system), or control channel data (from the MSC, base station, or mobile user). The GSM specification defines a wide variety of logical channels which can be used to link the physical layer with the data link layer of the GSM network. These logical channels efficiently transmit user data while simultaneously providing control of the network on each ARFCN. GSM provides explicit assignments of time slots and frames for specific logical channels, as described below.

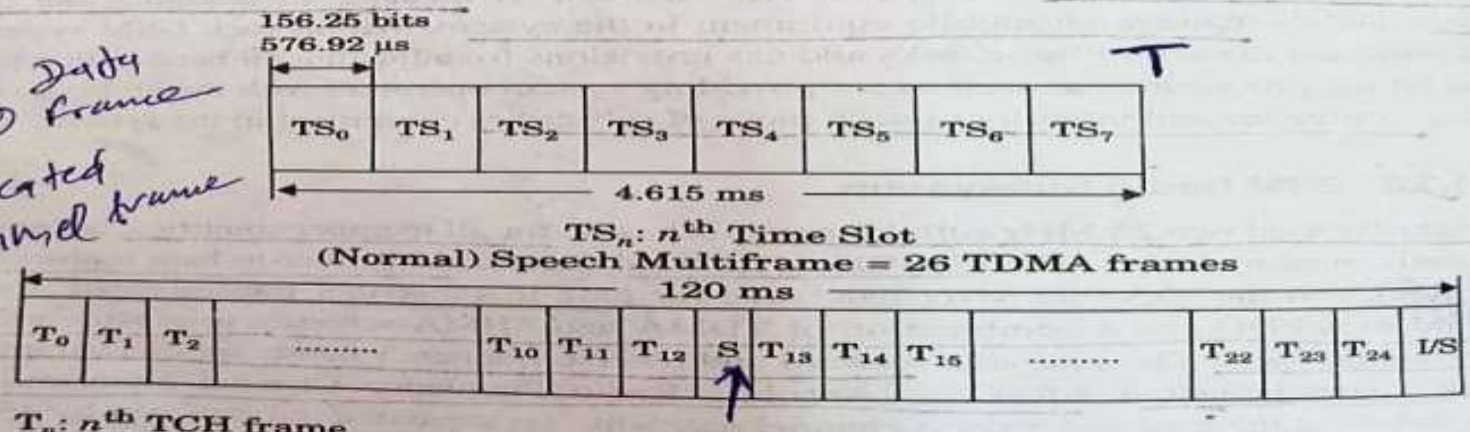


Figure 11.7 The speech dedicated control channel frame and multiframe structure.

Table 11.3 GSM Air Interface Specifications Summary

Parameter	Specifications
Reverse Channel Frequency	890–915 MHz
Forward Channel Frequency	935–960 MHz
ARFCN Number	0 to 124 and 975 to 1023
Tx/Rx Frequency Spacing	45 MHz
Tx/Rx Time Slot Spacing	3 Time slots
Modulation Data Rate	270.833333 kbps
Frame Period	4.615 ms
Users per Frame (Full Rate)	8
Time Slot Period	576.9 μs
Bit Period	3.692 μs
Modulation	0.3 GMSK
ARFCN Channel Spacing	200 kHz
Interleaving (max. delay)	40 ms
Voice Coder Bit Rate	13.4 kbps

11.3.4 GSM Channel Types

There are two types of GSM logical channels, called *traffic channels* (TCHs) and *control channels* (CCHs) [Hod90]. Traffic channels carry digitally encoded user speech or user data and have identical functions and formats on both the forward and reverse link. Control channels carry signaling and synchronizing commands between the base station and the mobile station. Certain types of control channels are defined for just the forward or reverse link. There are six different types of TCHs provided for in GSM, and an even larger number of CCHs, both of which are now described.

11.3.4.1 GSM Traffic Channels (TCHs)

GSM traffic channels may be either full-rate or half-rate and may carry either digitized speech or user data. When transmitted as full-rate, user data is contained within one TS per frame. When transmitted as half-rate, user data is mapped onto the same time slot, but is sent in alternate frames. That is, two half-rate channel users would share the same time slot, but would alternately transmit during every other frame.

In the GSM standard, TCH data may not be sent in TS 0 within a TDMA frame on certain ARFCNs which serve as the broadcast station for each cell (since this time slot is reserved for control channel bursts in most every frame, as described subsequently). Furthermore, frames of TCH data are broken up every thirteenth frame by either slow associated control channel data (SACCH) or idle frames. Figure 11.7 illustrates how the TCH data is transmitted in consecutive frames. Each group of twenty-six consecutive TDMA frames is called a *multiframe* (or *speech multiframe*, to distinguish it from the control channel multiframe described below). For every twenty-six frames, the thirteenth and twenty-sixth frames consist of Slow Associated Control Channel (SACCH) data, or the idle frame, respectively. The twenty-sixth frame contains idle bits for the case when full-rate TCHs are used, and contains SACCH data when half-rate TCHs are used.

Full-Rate TCH

The following full rate speech and data channels are supported:

- **Full-Rate Speech Channel (TCH/FS)** — The full-rate speech channel carries user speech which is digitized at a raw data rate of 13 kbps. With GSM channel coding added to the digitized speech, the full-rate speech channel carries 22.8 kbps.
- **Full-Rate Data Channel for 9600 bps (TCH/F9.6)** — The full-rate traffic data channel carries raw user data which is sent at 9600 bps. With additional forward error correction coding applied by the GSM standard, the 9600 bps data is sent at 22.8 kbps.
- **Full-Rate Data Channel for 4800 bps (TCH/F4.8)** — The full-rate traffic data channel carries raw user data which is sent at 4800 bps. With additional forward error correction coding applied by the GSM standard, the 4800 bps is sent at 22.8 kbps.
- **Full-Rate Data Channel for 2400 bps (TCH/F2.4)** — The full-rate traffic data channel carries raw user data which is sent at 2400 bps. With additional forward error correction coding applied by the GSM standard, the 2400 bps is sent at 22.8 kbps.

Half-Rate TCH

The following half-rate speech and data channels are supported:

- **Half-Rate Speech Channel (TCH/HS)** — The half-rate speech channel has been designed to carry digitized speech which is sampled at a rate half that of the full-rate channel. GSM anticipates the availability of speech coders which can digitize speech at about 6.5 kbps. With GSM channel coding added to the digitized speech, the half-rate speech channel will carry 11.4 kbps.
- **Half-Rate Data Channel for 4800 bps (TCH/H4.8)** — The half-rate traffic data channel carries raw user data which is sent at 4800 bps. With additional forward error correction coding applied by the GSM standard, the 4800 bps data is sent at 11.4 kbps.
- **Half-Rate Data Channel for 2400 bps (TCH/H2.4)** — The half-rate traffic data channel carries raw user data which is sent at 2400 bps. With additional forward error correction coding applied by the GSM standard, the 2400 bps data is sent at 11.4 kbps.

11.3.4.2 GSM Control Channels (CCH)

There are three main control channels in the GSM system. These are the *broadcast channel* (BCH), the *common control channel* (CCCH), and the *dedicated control channel* (DCCH). Each control channel consists of several logical channels which are distributed in time to provide the necessary GSM control functions.

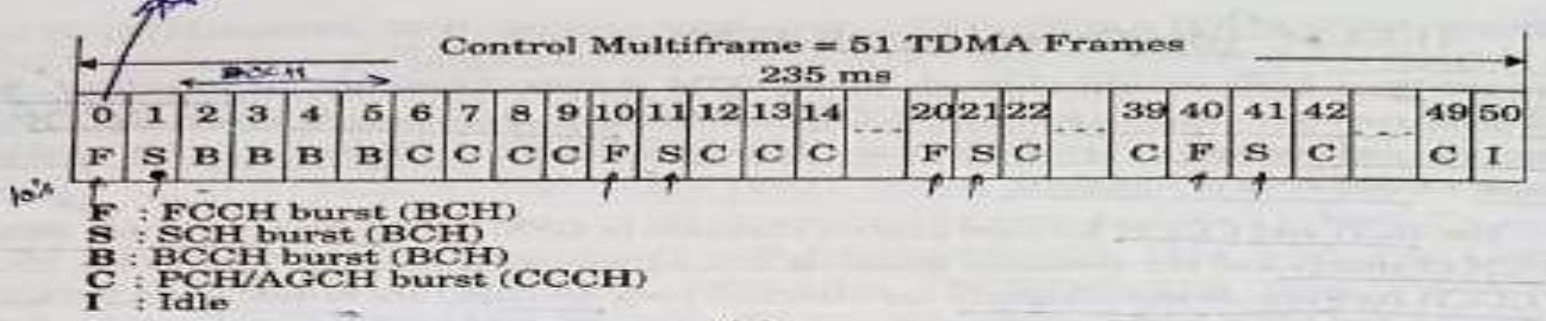
The BCH and CCCH forward control channels in GSM are implemented only on certain ARFCN channels and are allocated timeslots in a very specific manner. Specifically, the BCH and CCCH forward control channels are allocated only TS 0 and are broadcast only during certain frames within a repetitive fifty-one frame sequence (called the *control channel multiframe*) on those ARFCNs which are designated as broadcast channels. TS1 through TS7 carry regular TCH traffic, so that ARFCNs which are designated as control channels are still able to carry full-rate users on seven of the eight time slots.

The GSM specification defines thirty-four ARFCNs as standard broadcast channels. For each broadcast channel, frame 51 does not contain any BCH/CCCH forward channel data and is considered to be an idle frame. However, the reverse channel CCCH is able to receive subscriber transmissions during TS 0 of any frame (even the idle frame). On the other hand, DCCH data may be sent during any time slot and any frame, and entire frames are specifically dedicated to certain DCCH transmissions. GSM control channels are now described in detail.

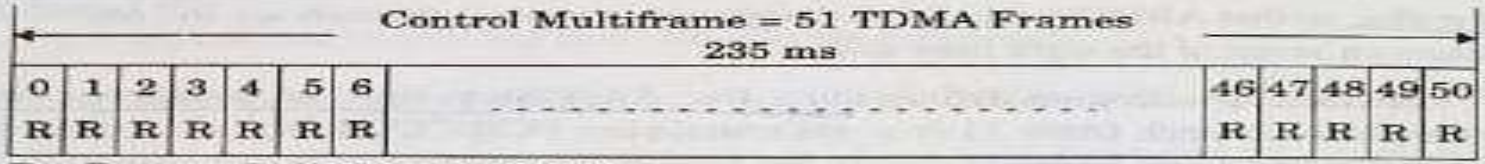
- **Broadcast Channels (BCHs)**— The broadcast channel operates on the forward link of a specific ARFCN within each cell, and transmits data only in the first time slot (TS 0) of certain GSM frames. Unlike TCHs which are duplex, BCHs only use the forward link. Just as the forward control channel (FCC) in AMPS is used as a beacon for all nearby mobiles to camp on to, the BCH serves as a TDMA beacon channel for any nearby mobile to identify and lock on to. The BCH provides synchronization for all mobiles within the cell and is occasionally monitored by mobiles in neighboring cells so that received power and MAHO decisions may be made by out-of-cell users. Although BCH data is transmitted in TS 0, the other seven timeslots in a GSM frame for that same ARFCN are available for TCH data, DCCH data, or are filled with dummy bursts. Furthermore, all eight timeslots on all other ARFCNs within the cell are available for TCH or DCCH data.

  The BCH is defined by three separate channels which are given access to TS 0 during various frames of the 51 frame sequence. Figure 11.8 illustrates how the BCH is allocated frames. The three types of BCH are now described.

  a) *Broadcast Control Channel (BCCH)* — The BCCH is a forward control channel that is used to broadcast information such as cell and network identity, and operating characteristics of the cell (current control channel structure, channel availability, and congestion). The BCCH also broadcasts a list of channels that are currently in use within the cell. Frame 2 through frame 5 in a control multiframe (4 out of every 51 frames) contain



(a)



(b)

Figure 11.8 (a) The Control Channel Multiframe (forward link for TS0); (b) The Control Channel Multiframe (reverse link for TS0).

BCCH data. It should be noted from Figure 11.8 that TS 0 contains BCCH data during specific frames, and contains other BCH channels (FCCH and SCH), common control channels (CCCHs), or an idle frame (sent every 51st frame) during other specific frames.

b) *Frequency Correction Channel (FCCH)* — The FCCH is a special data burst which occupies TS 0 for the very first GSM frame (frame 0) and is repeated every ten frames within a control channel multiframe. The FCCH allows each subscriber unit to synchronize its internal frequency standard (local oscillator) to the exact frequency of the base station.

c) *Synchronization Channel (SCH)* — SCH is broadcast in TS 0 of the frame immediately following the FCCH frame and is used to identify the serving base station while allowing each mobile to frame synchronize with the base station. The *frame number* (FN), which ranges from 0 to 2,715,647, is sent with the *base station identity code* (BSIC) during the SCH burst. The BSIC is uniquely assigned to each BST in a GSM system. Since a mobile may be as far as 30 km away from a serving base station, it is often necessary to adjust the timing of a particular mobile user such that the received signal at the base station is synchronized with the base station clock. The BS issues coarse *timing advancement* commands to the mobile stations over the SCH, as well. The SCH is transmitted once every ten frames within the control channel multiframe, as shown in Figure 11.8.

- **Common Control Channels (CCCHs)** — On the broadcast (BCH) ARFCN, the common control channels occupy TS 0 of every GSM frame that is not otherwise used by the BCH or the Idle frame. CCCH consists of three different channels: the paging channel (PCH), which is a forward link channel, the random access channel (RACH) which is a reverse link channel, and the access grant channel (AGCH), which is a forward link channel. As seen in Figure 11.8, CCCHs are the most commonly used control channels and are used to page specific subscribers, assign signaling channels to specific users, and receive mobile requests for service. These channels are described below.
  a) *Paging Channel (PCH)* — The PCH provides paging signals from the base station to all mobiles in the cell, and notifies a specific mobile of an incoming call which originates from the PSTN. The PCH transmits the IMSI of the target subscriber, along with a request for acknowledgment from the mobile unit on the RACH. Alternatively, the PCH may be used to provide *cell broadcast* ASCII text messages to all subscribers, as part of the SMS feature of GSM.
  b) *Random Access Channel (RACH)* — The RACH is a reverse link channel used by a subscriber unit to acknowledge a page from the PCH, and is also used by mobiles to originate a call. The RACH uses a slotted ALOHA access scheme. All mobiles must request access or respond to a PCH alert within TS 0 of a GSM frame. At the BTS, every frame (even the idle frame) will accept RACH transmissions from mobiles during TS 0. In establishing service, the GSM base station must respond to the RACH transmission by allocating a channel and assigning a stand-alone dedicated control channel (SDCCH) for signaling during a call. This connection is confirmed by the base station over the AGCH.
  c) *Access Grant Channel (AGCH)* — The AGCH is used by the base station to provide forward link communication to the mobile, and carries data which instructs the mobile to operate in a particular physical channel (time slot and ARFCN) with a particular dedicated control channel. The AGCH is the final CCCH message sent by the base station before a subscriber is moved off the control channel. The AGCH is used by the base station to respond to a RACH sent by a mobile station in a previous CCCH frame.
- **Dedicated Control Channels (DCCHs)** — There are three types of dedicated control channels in GSM, and, like traffic channels (see Figure 11.7), they are bidirectional and have the same format and function on both the forward and reverse links. Like TCHs, DCCHs may exist in any time slot and on any ARFCN *except TS0* of the BCH ARFCN. The stand-alone dedicated control channels (SDCCHs) are used for providing signaling services required by the users. The Slow- and Fast-Associated Control Channels (SACCHs and FACCHs) are used for supervisory data transmissions between the mobile station and the base station during a call.
  a) *Stand-alone Dedicated Control Channels (SDCCHs)* — The SDCCH carries signaling data following the connection of the mobile with the base station, and just before a TCH assignment is issued by the base station. The SDCCH ensures that the mobile

station and the base station remain connected while the base station and MSC verify the subscriber unit and allocate resources for the mobile. The SDCCH can be thought of as an intermediate and temporary channel which accepts a newly completed call from the BCH and holds the traffic while waiting for the base station to allocate a TCH channel. The SDCCH is used to send authentication and alert messages (but not speech) as the mobile synchronizes itself with the frame structure and waits for a TCH. SDCCHs may be assigned their own physical channel or may occupy TS0 of the BCH if there is low demand for BCH or CCCH traffic.

b) *Slow Associated Control Channel (SACCH)* — The SACCH is always associated with a traffic channel or a SDCCH and maps onto the same physical channel. Thus, each ARFCN systematically carries SACCH data for all of its current users. As in the USDC standard, the SACCH carries general information between the MS and BTS. On the forward link, the SACCH is used to send slow but regularly changing control information to the mobile, such as transmit power level instructions and specific timing advance instructions for each user on the ARFCN. The reverse SACCH carries information about the received signal strength and quality of the TCH, as well as BCH measurement results from neighboring cells. The SACCH is transmitted during the thirteenth frame (and the twenty-sixth frame when half-rate traffic is used) of every speech/dedicated control channel multiframe (Figure 11.7), and within this frame, the eight timeslots are dedicated to providing SACCH data to each of the eight full-rate (or sixteen half-rate) users on the ARFCN.

c) *Fast Associated Control Channels (FACCHs)* — FACCH carries urgent messages, and contains essentially the same type of information as the SDCCH. A FACCH is assigned whenever a SDCCH has not been dedicated for a particular user and there is an urgent message (such as a handoff request). The FACCH gains access to a time slot by "stealing" frames from the traffic channel to which it is assigned. This is done by setting two special bits, called stealing bits, in a TCH forward channel burst. If the stealing bits are set, the time slot is known to contain FACCH data, not a TCH, for that frame.