P
T
E
R

GSM and TDMA Technology

Upon completion of this chapter, the student should be able to:

- Discuss the basic services offered by GSM cellular and the frequency bands of operation.
- Discuss the network components of a GSM system and the basic functions of the mobile station, station system, and network switching system.
- Explain the concept of GSM network interfaces and protocols, and their relationship to the OSI mo
- Explain the GSM channel concept.
- Discuss the functions of the GSM logical channels.
- Explain the TDMA concept and how it is implemented in GSM.
- Explain the mapping of logical channels on to the GSM physical channels.
- Discuss the various GSM identities.
- Explain the GSM operations of call setup, location updating, and handover.
- Discuss the GSM operations that occur over the Um interface.

This chapter provides a detailed description of the GSM wireless cellular telephone system and the division multiple access (TDMA) technology used to implement the air interface portion of the sy GSM cellular is by far the most popular wireless system in the world with over one billion subsc Because of this popularity, this chapter presents an in-depth explanation of the architecture of this sy and the access technology used to implement it. Because of the amount of detail included in this ch the chapter has been organized into three parts: an overview of GSM, GSM network operations, and TDMA systems.

Part I coverage starts with a short prologue to the evolution of GSM and the rationale behind its duction. The GSM frequency bands are introduced and the channel numbering system is explained. the network components that compose a GSM system are introduced and their functions are describ detail. How these subsystem components are interconnected and the messages that are sent between are looked at from several different viewpoints. The GSM standards specify various system interfaces are introduced to the reader along with the protocols used by the subsystems to deliver the messages commands needed for overall system operation. The OSI model is used extensively to frame the theo GSM operation.

Next, the GSM channel concept is introduced with descriptions of the various logical channels and function. How the system uses time division multiplexing to provide a means by which system comm messages, and traffic can be transmitted over the air interface during selected timeslots is examin

detail. Several examples of possible TDMA frame timing schemes are presented to give the reader a feel for the complexity of the system and the number of operations needed to make the system functional.

Part II of the chapter reviews GSM system identifiers before a detailed coverage of GSM traffic cases is started. The three basic operations needed to support a subscriber's mobility within a wireless cellular system—call setup, location updating, and call handover—are now treated from the viewpoint of the interactions between subsystem components through command and message transmissions over the interfaces specified in the GSM standards. The last portion of this section takes the reader a step closer to the networking aspect of GSM system operation by examining typical system management functions in the context of the OSI model.

In Part III, the last section of this chapter introduces NA-TDMA, a cellular technology very similar to GSM but not compatible with it. Because of the amount of detail already provided about GSM, this topic is dealt with in a fairly superficial manner by simply indicating the system similarities and differences. This chapter does not cover the operations needed for high-speed packet data transmission over a GSM or NA-TDMA network. Discussion of that topic is delayed until Chapter 7.

PART I GSM SYSTEM OVERVIEW

5.1 INTRODUCTION TO GSM AND TDMA

As discussed in prior chapters, the GSM system evolved due to a desire by the European countries to develop a pan-European system that would allow roaming on an international basis. At the time, digital technology and microelectronics had advanced sufficiently to allow for the development of an entirely digital second-generation cellular system. Other TDMA digital cellular standards such as North American IS-136 are very similar to GSM. The GSM standards, as published by the ETSI, includes specifications for the air interface portion of the system as well as the fixed network infrastructure used to support the services offered over the wireless network. The GSM standards may be downloaded from www.etsi.org.

In 1982, the frequency bands of 890–915 MHz and 935–960 MHz were allocated for a pan-European second-generation digital cellular system (GSM 900) that would replace the incompatible first-generation systems that were already in existence in different countries. The allocation of the frequency bands was only the first step in this process. An international task force was also assembled during 1982 and by 1987 GSM was formally adopted by the European Commission. The ETSI took over development in 1989 and published the standards for the first phase of GSM in 1990. The development process continued, resulting in the deployment of a functional system in 1992. A new frequency band in the 1800-MHz range was added worldwide for what was originally named digital cellular system (DCS 1800). This upbanded version of GSM 900 was renamed GSM 1800 in 1997. GSM service in the 1900-MHz range (GSM 1900) using the PCS bands in the United States has been deployed recently. Also, the implementation of additional GSM services offered under Phase 2 and Phase 2+ of GSM has been an ongoing process and continues today under the direction of the ETSI. Today, the GSM system is by far the most popular cellular wireless system in the world.

GSM Services

The first-generation analog cellular systems were designed for basic voice service. Data services for fax or circuit-switched data transmission using a voiceband modem were classified as "overlay" services that run on top of the voice service. The second-generation GSM cellular system was designed to be an integrated wireless voice-data service network that offered several other services beyond just voice telephone service. The types of services to be offered over the GSM network were classified into two categories: teleservices and bearer services (see Figure 5–1). In addition, there are supplementary services that can be added to the teleservices.

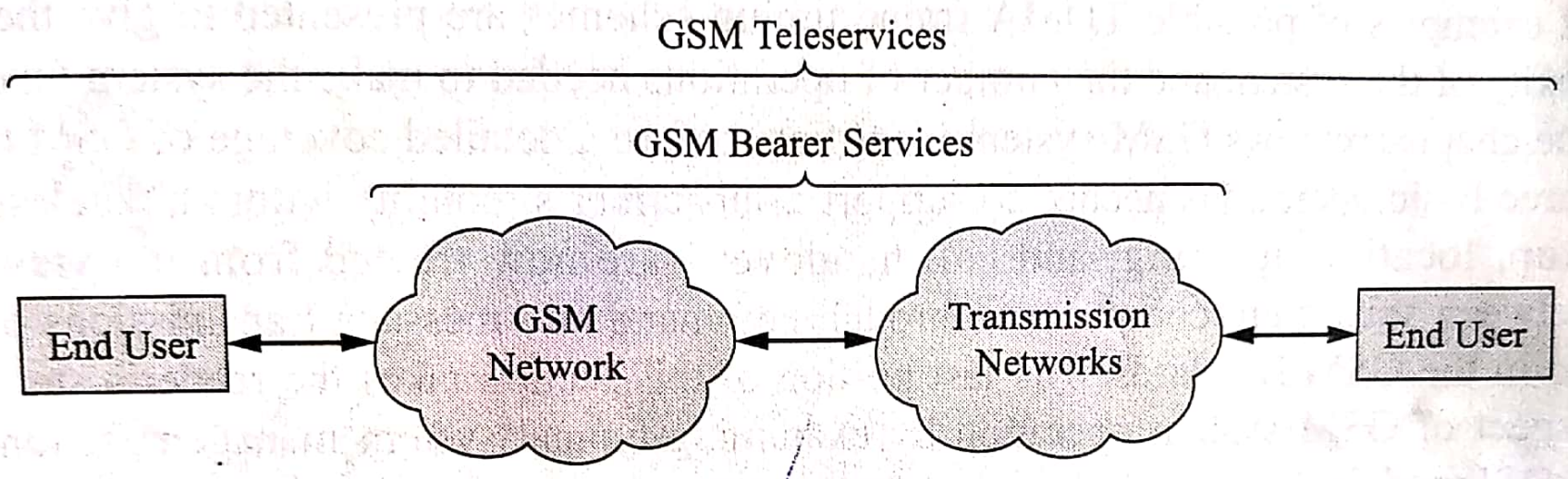


Figure 5–1 Relationship of teleservices and bearer services to the GSM system (Courtesy of ETSI).

Teleservices provide standard voice communications between two end users and additional communications between two end user applications according to some standard protocol. **Bearer services** provide the user with the ability to transmit data between user network interfaces. Supplementary services are services that enhance or support a teleservice provided by the network.

The planning of GSM system development and deployment called for the implementation of system services to be carried out in two phases. In the first phase, the GSM services offered were as shown in Table 5–1. In the second phase of GSM implementation, the service offerings would be expanded to include those shown in Table 5–2. Presently, the development of GSM system services has evolved into Phase 2+. Phase 2+ is primarily focused on the addition of high-speed packet data services to GSM. This initiative is embodied in general packet radio service (GPRS) and enhanced data rates for global evolution (EDGE). These topics will be discussed in more detail in Chapter 7.

Table 5–1 Phase 1 GSM services (Courtesy of ETSI).

Service Category	*Service*	*Additional Details*
GSM Teleservices	Telephony Emergency calls Short Message Service Videotext access Teletex, FAX, etc.	Full rate at 13 kbps voice "112" is GSM-wide emergency number Point-to-point (between two users) and cell broadcast types
GSM Bearer Services	Asynchronous data Synchronous data Synchronous packet data Others	300–9600 bps (transparent/nontransparent) 2400–9600 bps transparent
Supplementary Services	Call forwarding Call barring	All calls, when the subscriber is not available Outgoing calls with specifications

GSM Radio Frequency Carriers

For GSM cellular systems the air interface consists of channels that have a frequency separation of 200 kHz. For the three most widely used frequency bands devoted to GSM system operation this channel spacing yields a different total number of carrier frequencies per band. The GSM 900 band has 124 carrier frequencies, the GSM 1800 band has 374 carrier frequencies, and the GSM 1900 band has 299 carrier frequencies. Since each carrier can be shared by up to eight users, the total number of channels for each system is:

$$124 \times 8 = 992 \text{ channels for GSM 900}$$

Table 5–2 Phase 2 GSM services (Courtesy of ETSI).

Service Category	*Service*	*Additional Details*
GSM Teleservices	Half-rate speech coder Enhanced full rate	Optional implementation
Supplementary Services	Calling line identification Connected line identification Call waiting Call hold Multiparty communications Closed user group Advice of charge Operator determined call barring	Presentation or restriction of displaying the caller's ID Presentation or restriction of displaying the called ID Incoming call during current conversation Put current call on hold to answer another Up to five ongoing calls can be included in one conversation Restriction of certain features from individual subscribers by operator

$374 \times 8 = 2992$ channels for GSM 1800

$299 \times 8 = 2392$ channels for GSM 1900/PCS 1900

The frequency bands allocated to the five present GSM system implementations are shown in Table 5–3. The channels have absolute radio frequency channel numbers (ARFCNs) associated with them and are numbered as 1–124, 259–293, 306–340, 512–885, and 512–810 for Primary GSM 900 (P-GSM 900), GSM 450, GSM 480, GSM 1800, and GSM 1900/PCS 1900, respectively. Also note that Extended GSM 900 (E-GSM 900) and Railways GSM 900 (R-GSM 900) have added channels 975–1023 and 955–1023,

Table 5–3 GSM frequency bands and channel numbers (Courtesy of 3GPP).

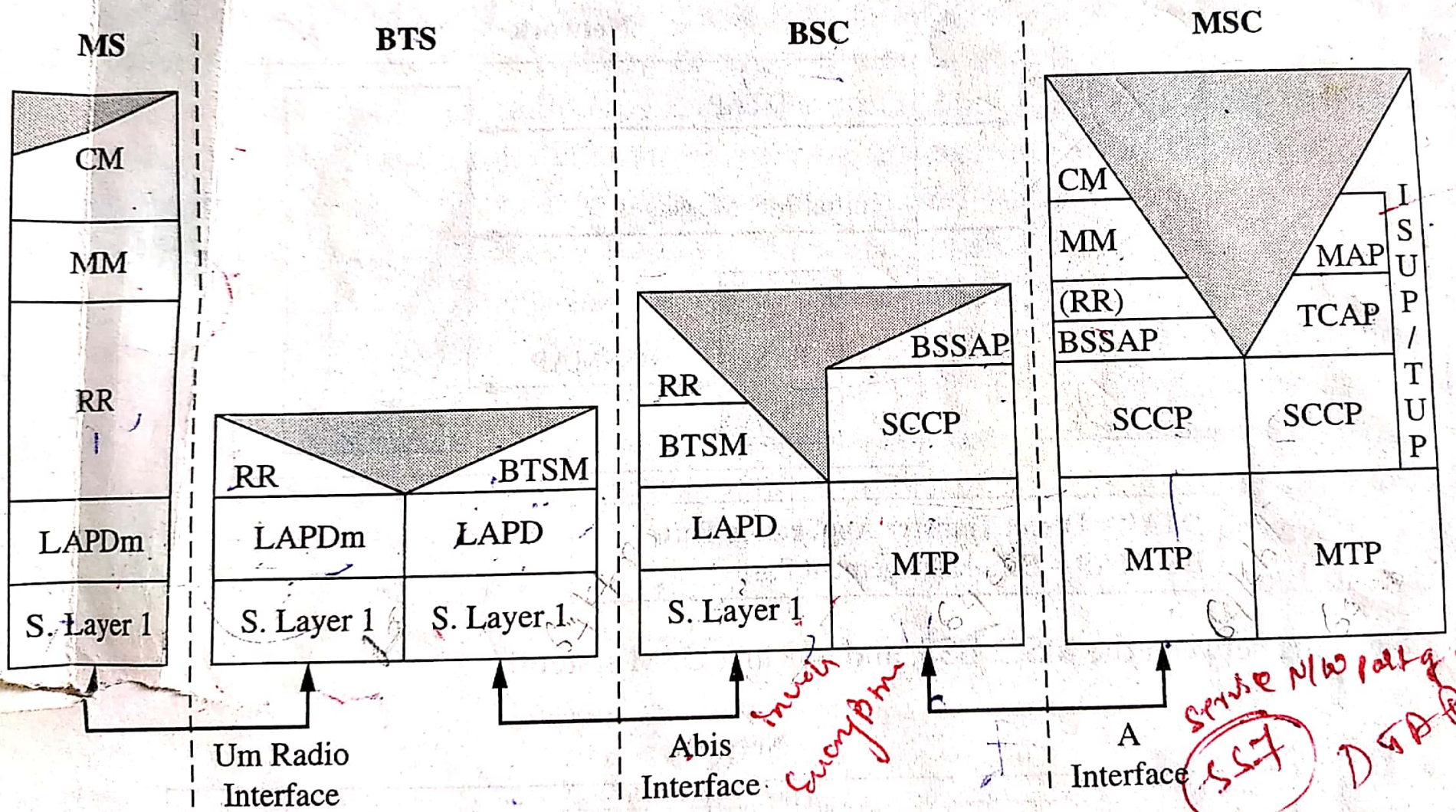
GSM Band	*Uplink Frequency*	*Downlink Frequency*
P-GSM 900 ARFCN=1...124	890 - 915 MHz (ARFCN-1) × 0.2 MHz + 890.2 MHz	935 - 960 MHz Uplink frequency + 45 MHz
E-GSM 900 ARFCN=975...1023	880 - 890 MHz (ARFCN = 0 = 890 MHz) (ARFCN-975) × 0.2 MHz + 890 MHz	925 - 935 MHz Uplink frequency + 45 MHz
R-GSM 900 ARFCN=955...1023	876 - 890 MHz (ARFCN-1023) × 0.2 MHz + 890 MHz	921 - 935 MHz Uplink frequency + 45 MHz
GSM 1800 ARFCN=512...885	1710 - 1785 MHz (ARFCN-512) × 0.2 MHz + 1710.2 MHz	1805 - 1880 MHz Uplink frequency + 95 MHz
GSM 1900 ARFCN=512...810	1850 - 1910 MHz (ARFCN-512) × 0.2 MHz + 1850.2 MHz	1930 - 1990 MHz Uplink frequency + 90 MHz
GSM 450 ARFCN=259...293	450.4 - 457.6 MHz (ARFCN-259) × 0.2 MHz + 450.6 MHz	460.4 - 467.6 MHz Uplink frequency + 10 MHz
GSM 480 ARFCN=306...340	478.8 - 486 MHz (ARFCN-306) × 0.2 MHz + 478.8 MHz	488.8 - 496 MHz Uplink frequency + 10 MHz

receiving

GSM Protocols and Signaling Model

Figure 5–6 shows a signaling model for the GSM system. As shown by the figure, the MS communicates with the MSC to provide system connection, mobility, and radio resource management by sending messages back and forth over the air interface from the MS to the BTS, between the BTS and the BSC, and between the BSC and the MSC. The figure indicates the various protocols that are used between the different GSM interfaces and at the different OSI layer levels. Additionally, the MSC communicates with the various networks that it is connected to (PSTN, PLMN, etc.) by using the various protocols shown in the figure. These operations will be briefly summarized in the next several sections and then explained in more detail in Section 5.6 of this chapter.

Um Interface The Layer 1, Um, air interface specifications will be detailed more extensively in Section 5.6 of this chapter and in Chapter 8. The Layer 2 protocol used on the Um interface is LAPDm, a modified



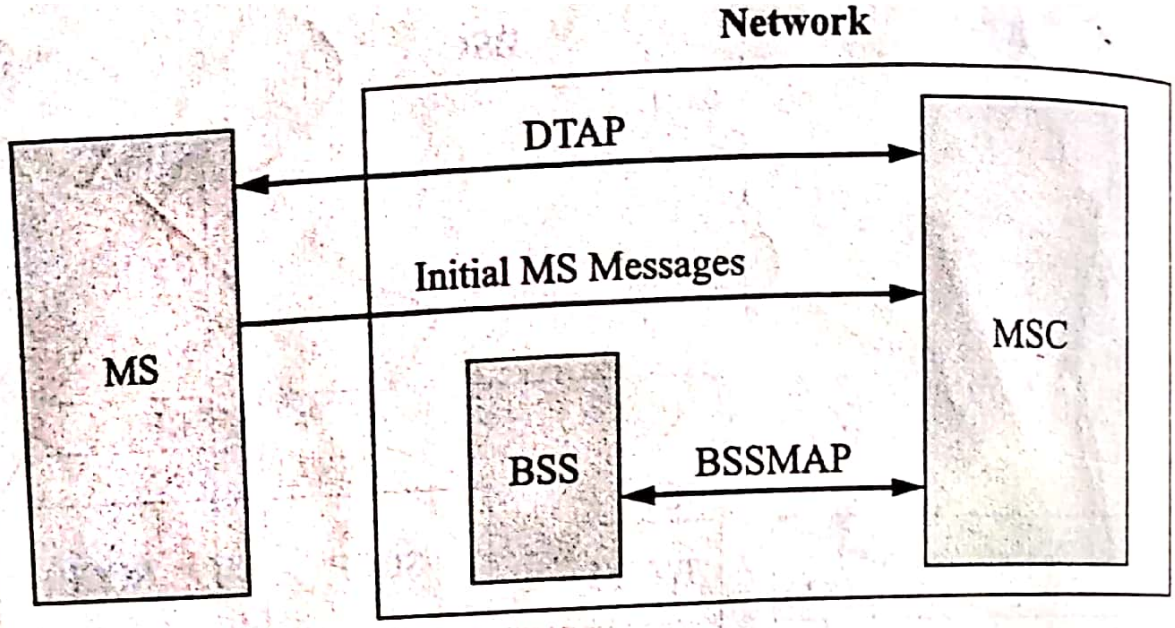
5–6 GSM signaling model

version of the ISDN protocol LAPD. The major differences between LAPD and LAPDm protocol are the following: for LAPDm no error detection is employed since it has been built into Layer 1 signaling and LAPDm messages are segmented into shorter messages than LAPD to be compatible with the TDMA frame length used in GSM.

Abis Interface The Abis interface exists between the BSC and the BTS. The Layer 2 protocol used on the Abis interface is LAPD. At the Layer 3 level, most messages just past through the BTS transparently. However, there are some radio resource management messages that are closely linked to the system radio hardware that must be handled by the BTS. The BTS management (BTSM) entities manage these messages. An example of this type of radio resource message involves encryption. The ciphering message sends the cipher key, K_c, to the BTS and then the BTS sends the ciphering mode command to the MS. Abis Layer 1 signaling details will also be discussed further in Chapter 8.

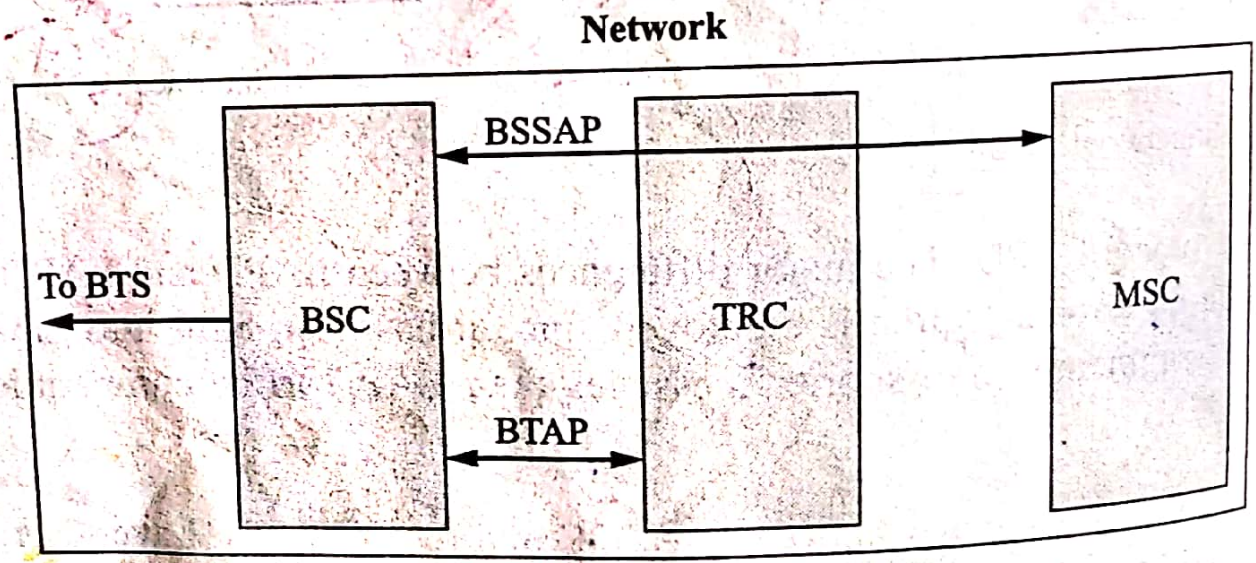
A Interface The A interface exists between the BSC and the MSC. Signaling over the A interface is done according to base station signaling application part (BSSAP) using the network service part of SS7. In the MSC, in the direction of the MS, Layer 3 is subdivided into three parts: radio resource management (RR), mobility management (MM), and connection management (CM). More will be said about these sublayers in Section 5.6 of this chapter. As mentioned, the protocol used to transfer the CM and MM messages is BBSAP. The BBSAP protocol has two subparts: direct transfer application part (DTAP) and base station system management application part (BSSAMP). DTAP is used to send CM and MM messages between the MSC and the MS transparently through the BSS. BSSAMP is used to send messages between the MSC and the BSC. This operation is detailed in Figure 5–7.

Ater Interface The Ater interface only exists in GSM systems that have separate units for the transcoder controller and BSC (this is typical of some vendors' GSM equipment). Signaling between the BSC and the TRC is performed by the use of BSC/TRC application part (BTAP) protocol (BTAP is a vendor- [Ericsson] specific protocol) over the Ater interface. Figure 5–8 shows this type of operation. The figure indicates how BSSAP signaling is sent transparently through the TRC node. Ater Layer 1 signaling details will also be discussed further in Chapter 8.



DTAP = Direct Transfer Application Part
BSSMAP = BSS Management Part

e 5–7 Signaling between the MSC, BSS, and MS in a GSM system.



BTAP = BSC/TRC Application Part
BSSAP = BSS Application Part

igure 5–8 Signaling over the GSM Ater interface.

MSC Interfaces The GSM signaling model (Figure 5–6) shows two protocol stacks within the MSC node. The protocol stack on the left-hand side is associated with the A interface and has been discussed earlier. The right-hand protocol stack corresponds to the MSC network interfaces to the VLR, HLR, GMSC, and the PSTN or other PLMNs. Within the network interface stack are the following protocols: MTP, SCCP, TCAP, MAP, and ISUP/TUP. Message transfer part (MTP) is used to transport messages and for routing and addressing. MTP corresponds to OSI Layers 1, 2, and parts of 3. Signaling connection control part (SCCP) adds functions to SS7 signaling to provide for more extensive addressing and routing. Together, MTP and SCCP form the network service part (NSP) and correspond to Layers 1–3 in the OSI model. Transfer capabilities application part (TCAP) and mobile application part (MAP) are Layer 7 protocols. TCAP provides services based on connectionless network services. MAP is a protocol specifically designed for mobile communications. It is used for the signaling between databases (HLR, VLR, EIR, AUC, etc.) and is further designated as MAP-*n* where *n* is given as shown by Figure 5–5. ISDN-user part (ISDN-UP) and temporary user part (TUP) are used from Layer 3 up to Layer 7 and are used between the MSC and the ISDN/PSTN for call setup and supervision. More detail about these protocols and operations will be given later in this chapter.

5.3 GSM CHANNEL CONCEPT

As discussed in previous chapters, cellular telephone networks use various control and traffic channels to carry out the operations necessary to allow for the setup of a subscriber radio link for the transmission of

either a voice conversation or data and the subsequent system support for the subscriber's mobility. The GSM cellular system is based on the use of **time division multiple access** (TDMA) to provide additional user capacity over a limited amount of radio frequency spectrum. This is accomplished by dividing the air interface connection period into timeslots that can be used by different subscribers for voice or data traffic and also for the transmission of the required system signaling and control information. In essence, this process provides additional channels to the system over the same physical radio link.

As shown by Figure 5–9, the GSM system divides the radio link connection time into eight equal and repeating timeslots known as **frames** for both uplink and downlink transmissions. The timeslots can be considered logical channels. That is, from a system point of view, each timeslot may carry either subscriber traffic or signaling and control information required for the management of the radio link and other system resources. The system can use several different types of repeating frame structures known as **multiframes** depending upon the type of information being transmitted. The next several sections will provide more detail about the timeslots and the frame structure and the operations and the various functions performed by the signaling and control channels.

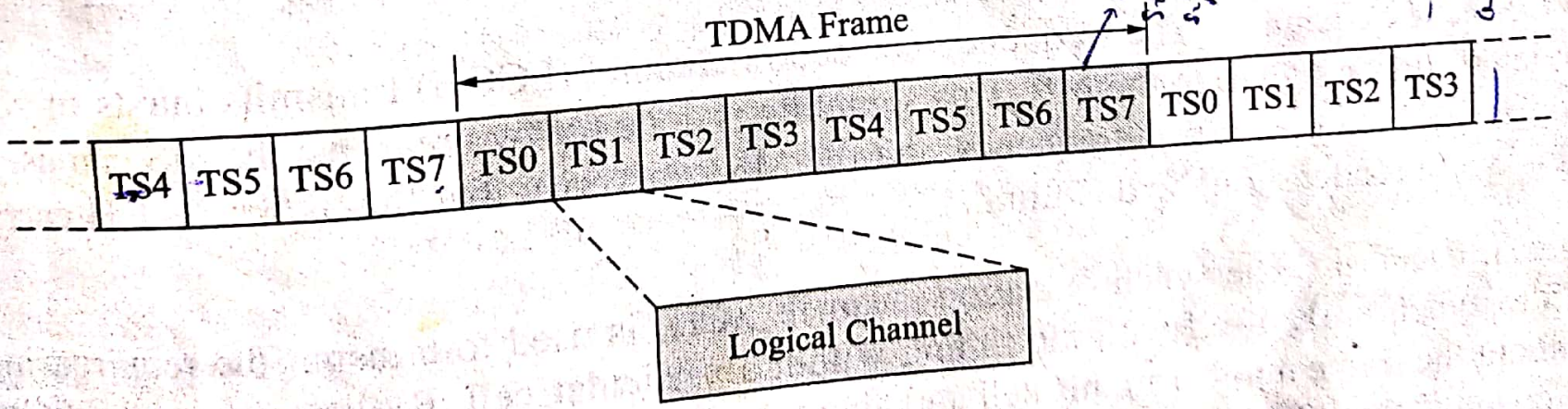


Figure 5–9 GSM TDMA frame.

Logical Channels

As previously mentioned, the **logical channels** may carry either subscriber traffic or signaling and control information to facilitate subscriber mobility. Presently, there are three types of traffic channels (TCHs). The full-rate traffic channel (TCH/F or Bm) carries one conversation by using one timeslot. The transmitted voice signal is encoded at a 13-kbps rate, but it is sent with additional overhead bits. This information plus additional channel overhead bits yields a final channel data rate of 22.8 kbps. The full-rate traffic channel may also carry data at rates of 14.4, 9.6, 4.8, and 2.4 kbps. The half-rate traffic channel (TCH/H or Lm) carries voice encoded at 6.5 kbps or data at rates of 4.8 or 2.4 kbps. With additional overhead bits, the total data rate for TCH/H becomes 11.4 kbps. Therefore, two conversations or a conversation and a data transfer or two data transfers may be transmitted over one channel at the same time. Enhanced full-rate (EFR) traffic encodes voice at a 12.2-kbps rate and like TCH/F adds overhead bits to yield a 22.8 kbps channel data rate. The EFR channel may also transmit data at the TCH/F rates. More will be said about these channels later.

The signaling and control channels consist of three channel sub-categories: broadcast channels, common control channels, and dedicated control channels. The function of these channels will be explained in more detail next. Later, the timing scheme used to transmit the signaling and control channels within the TDMA frame structure will be examined.

Broadcast Channels

The GSM cellular system uses broadcast channels (BCHs) to provide information to the mobile station about various system parameters and also information about the location area identity (LAI). The three types of BCHs are broadcast control channel, frequency correction channel, and synchronization channel. Using the information transmitted over these three BCHs, the MS can tune to a particular base transceiver system

(BTS) and synchronize its timing with the frame structure and timing in that cell. Each time the MS attaches to a new BTS it must listen to these three BCHs.

At present, the timing of different GSM cells is not synchronized. However, there are several emerging technologies that may be adopted in the near future that may alter this fact. The use of single-antenna interference cancellation (SAIC) algorithms to increase GSM system capacity is being investigated by the GSM industry. This noise cancellation technique is enhanced for synchronous networks. Therefore, eventually GSM cells may all be aligned to some master clock like the Global Positioning System (GPS).

Broadcast Control Channel The broadcast control channel (BCCH) contains information that is needed by the MS concerning the cell that it is attached to in order for the MS to be able to start making or receiving calls, or to start roaming. The type of information broadcast on the BCCH includes the LAI, the maximum output power allowed in the cell, and the BCCH carrier frequencies for the neighboring cells. This last information is used by the MS to allow it to monitor the neighboring cells in anticipation of a possible handover operation that might be needed as the MS moves about. The BCCH is only transmitted on the downlink from BTS to MS.

Frequency Correction Channel The frequency correction channel (FCCH) transmits bursts of zeros (this is an unmodulated carrier signal) to the MS. This signaling is done for two reasons: the MS can use this signal to synchronize itself to the correct frequency and the MS can verify that this is the BCCH carrier. Again, the FCCH is only broadcast on the downlink.

Synchronization Channel The synchronization channel (SCH) is used to transmit the required information for the MS to synchronize itself with the timing within a particular cell. By listening to the SCH, the MS can learn about the frame number in this cell and about the BSIC of the BTS it is attached to. The BSIC can only be decoded if the BTS belongs to the GSM network. Again, SCH is only transmitted in the downlink direction.

direction.

Common Control Channels

The common control channels (CCCHs) provide paging messages to the MS and a means by which the mobile can request a signaling channel that it can use to contact the network. The three CCCHs are the paging channel, random access channel, and the access grant channel.

Paging Channel The paging channel (PCH) is used by the system to send paging messages to the mobiles attached to the cell. The MS listens to the PCH at certain time intervals to learn if the network wants to make contact with it. The mobile will be paged whenever the network has an incoming call ready for the mobile or some type of message (e.g., short message or multimedia message) to deliver to the mobile. The information transmitted on the PCH will consist of a paging message and the mobile's identity number (e.g., ISMI or TMSI). The PCH is transmitted in the downlink direction only.

Random Access Channel The random access channel (RACH) is used by the mobile to respond to a paging message. If the mobile receives a page on the PCH, it will reply on the RACH with a request for a signaling channel. The RACH can also be used by the mobile if it wants to set up a mobile-originated call. The RACH is only transmitted in the uplink direction. For this last operation, the RACH also plays an important role in the determination of the required timing advance needed by the MS and the subsequent assignment of this parameter to the mobile by the network.

The format of the signal sent on the RACH provides enough information to the wireless network (i.e., the BSC) to allow it to calculate the distance of the mobile from the BTS. This measured time delay is then translated into a timing advance (TA) that is sent to the MS. The use of a TA allows any mobile within the cell to transmit information that will arrive at the BTS in correct synchronization with the start of the TDMA frame. In the GSM system, the structure of the RACH signal allows for a maximum cell radius of 35 km except when extended range cells are defined by the system.

Speech Processing

Before examining the structure of a timeslot, it will be instructive to take a brief look at how speech is processed in a GSM system. Figure 5–10 depicts this process. In the mobile, speech is digitized and broken up into 20-ms segments. It is then coded to reduce the bit rate and to control errors. This process produces 8000 samples of 13 bits per sample per second or 160 samples of 13 bits per sample per 20 ms. The speech coder yields 260 bits per 20 ms or 13 kbps whereas channel coding yields 456 bits per 20 ms or a 22.8-kbps data rate. Interleaving, ciphering, and burst formatting yields 156.25 bits per timeslot. This yields an overall data transfer rate of 270.8 kbps over a GSM channel.

The receiver works in the following manner: signal bursts are received and used to create a channel model. The channel model is created in the equalizer where an estimated bit sequence is calculated for a received signal. After all of the bursts containing information about a 20-ms segment of speech have been received and deciphered, they are reassembled into the 456-bit message. This sequence is then decoded to detect and correct any errors that occurred during transmission. More details about the signal bursts will be forthcoming shortly and more information about the interleaving and ciphering operations will be presented in Chapter 8.

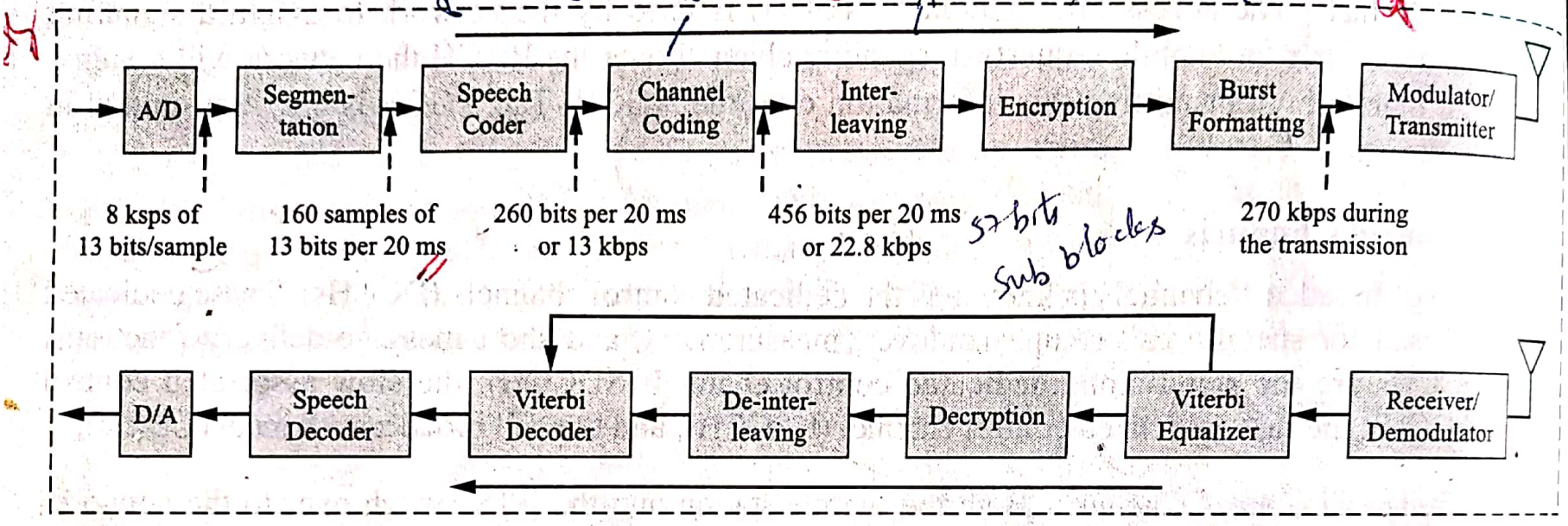


Figure 5–10 GSM speech processing.

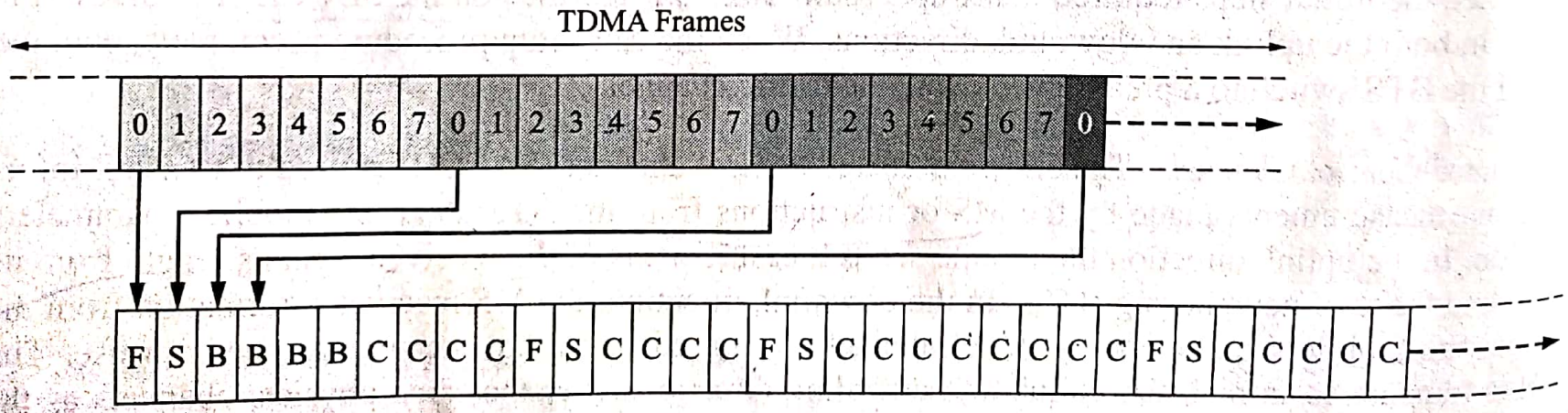


Figure 5–11 Relationship between timeslots and TDMA multiframes.

Timeslots and TDMA Frames

In a GSM system, both traffic and signaling and control information are transmitted over the same physical frequency channel. To accomplish this, time division multiplexing is used. The physical channels of the system used for the transmission of traffic are distinguished by virtue of their particular timeslot within a TDMA frame and the system signaling and control information is organized in terms of both the specific timeslot within the TDMA frame and the particular frame within a larger organization of TDMA frames (multiframes). The relationship between timeslots and TDMA multiframes is depicted in Figure 5–11. The next several sections will examine the concepts of timeslots and TDMA frames in more detail.

TDMA Frames

In the GSM system, eight timeslots constitute a TDMA frame. The system assigns numbers to the frames sequentially from 0 to 2,715,648 and then the process repeats itself. Our description of GSM timing will start with the largest system time period. This grouping of successive TDMA frames is known as a hyperframe. The hyperframe (as shown in Figure 5–12) consists of 2,048 superframes (2,715,648 frames) and takes 3 hours 28 minutes 53 seconds and 760 milliseconds to complete. Each superframe consists of 1,326 TDMA frames that take approximately 6.12 seconds to complete. These superframes may take on one of two possible formats. An explanation of why this is the case will be forthcoming shortly. One form of a superframe consists of 51 (26 frame) multiframes (i.e., each multiframe consists of 26 TDMA frames that take 120 ms to complete). The other superframe format consists of 26 (51 frame) multiframes (i.e., each multiframe consists of 51 TDMA frames that take about 235 ms to complete). Finally, as previously mentioned, within a TDMA frame there are eight timeslots that take approximately 4.615 ms to complete.

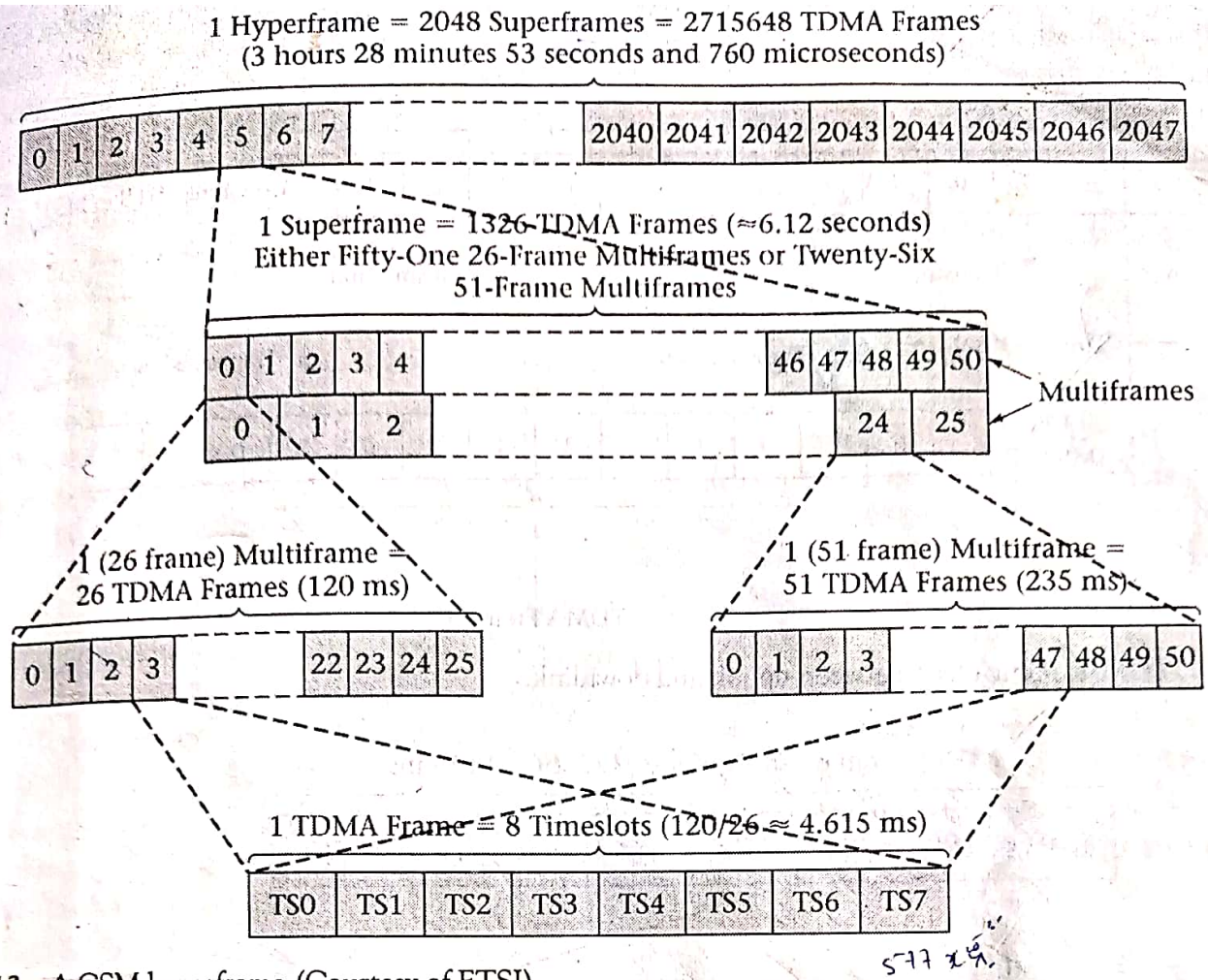


Figure 5–12 A GSM hyperframe (Courtesy of ETSI).

Timeslots

The organization of the transmitted digital bits within the air **timeslot** itself can take on several different formats depending upon the type of information being transmitted (i.e., voice traffic, data, or signaling and control messages). As shown in Figure 5–13, the air interface timeslot has a duration of 3/5200 seconds or approximately 577 µs (or 156.25 bit periods) whereas the typical transmitted burst is approximately 546 µs (or 148 bit periods). A bit time is 48/13 µs or approximately 3.69 µs. The overall bit rate over the air interface is approximately 270.8 kbps.

The start of a TDMA frame on the uplink is delayed by three timeslot periods from the downlink frame as shown in Figure 5–14. The purpose of this delay is so that the same timeslot may be used on both the downlink and uplink radio paths without the need for the MS to receive and transmit at the same time. This extends mobile battery life and makes it easier for the mobile's hardware to implement the RF operations needed for proper system functioning.

Timeslot Bursts The transmission of a normal (traffic and control channels) burst and the other types of burst signals are shown in Figure 5–15. In the case of a normal **burst,** two groups of 57 encrypted bits are transmitted on either side of a training sequence of bits. This **training sequence** consists of alternating 0s

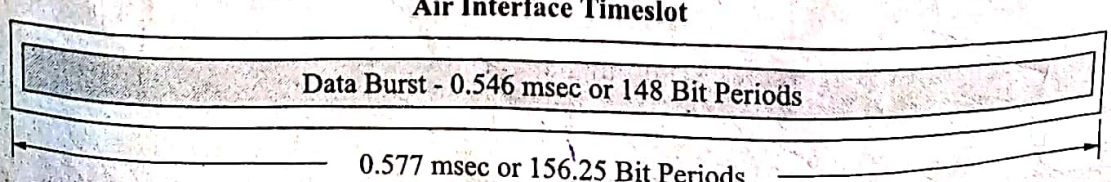


Figure 5–13 The GSM air interface timeslot.

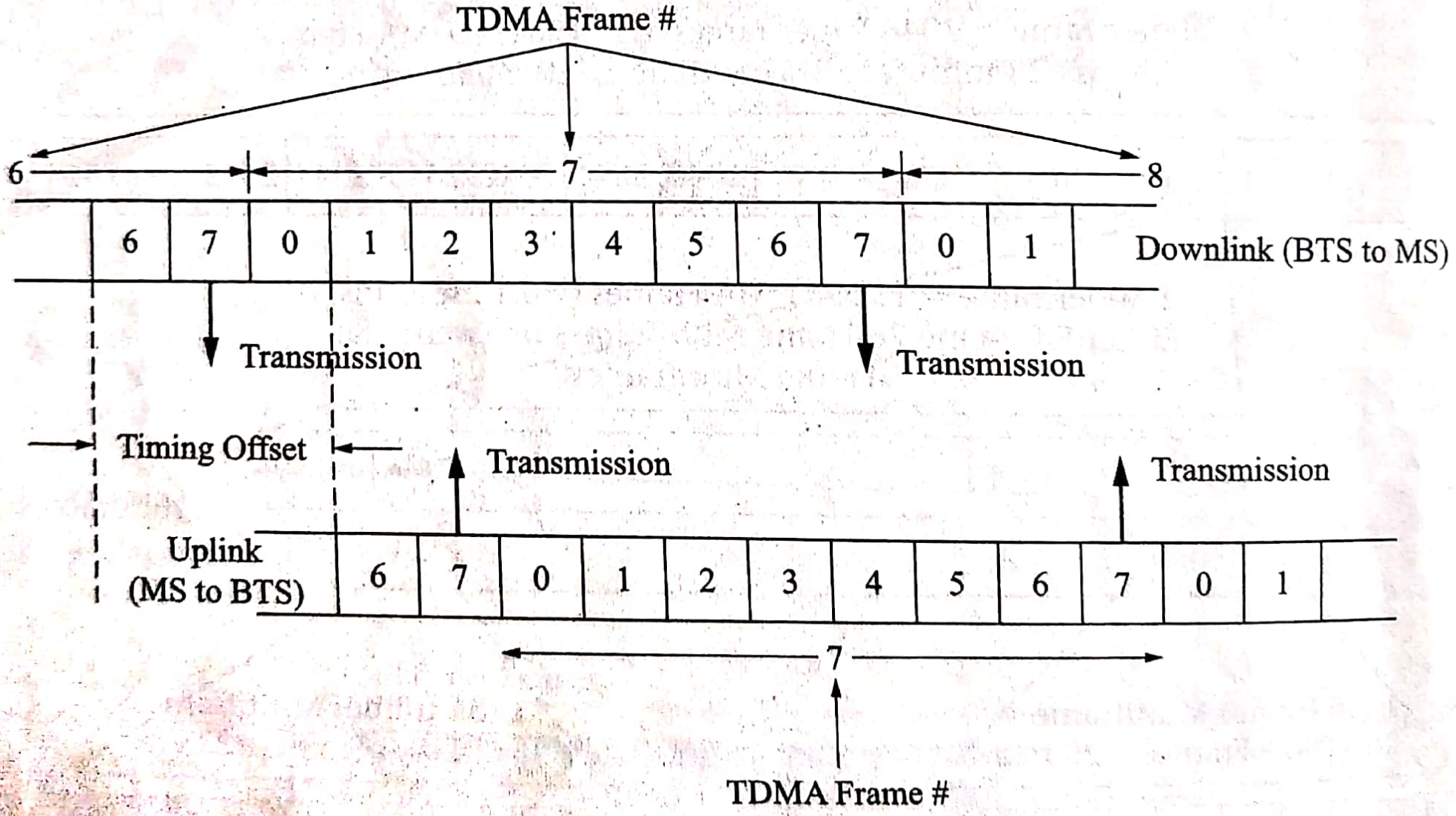


Figure 5–14 TDMA timing offset between uplink and downlink.

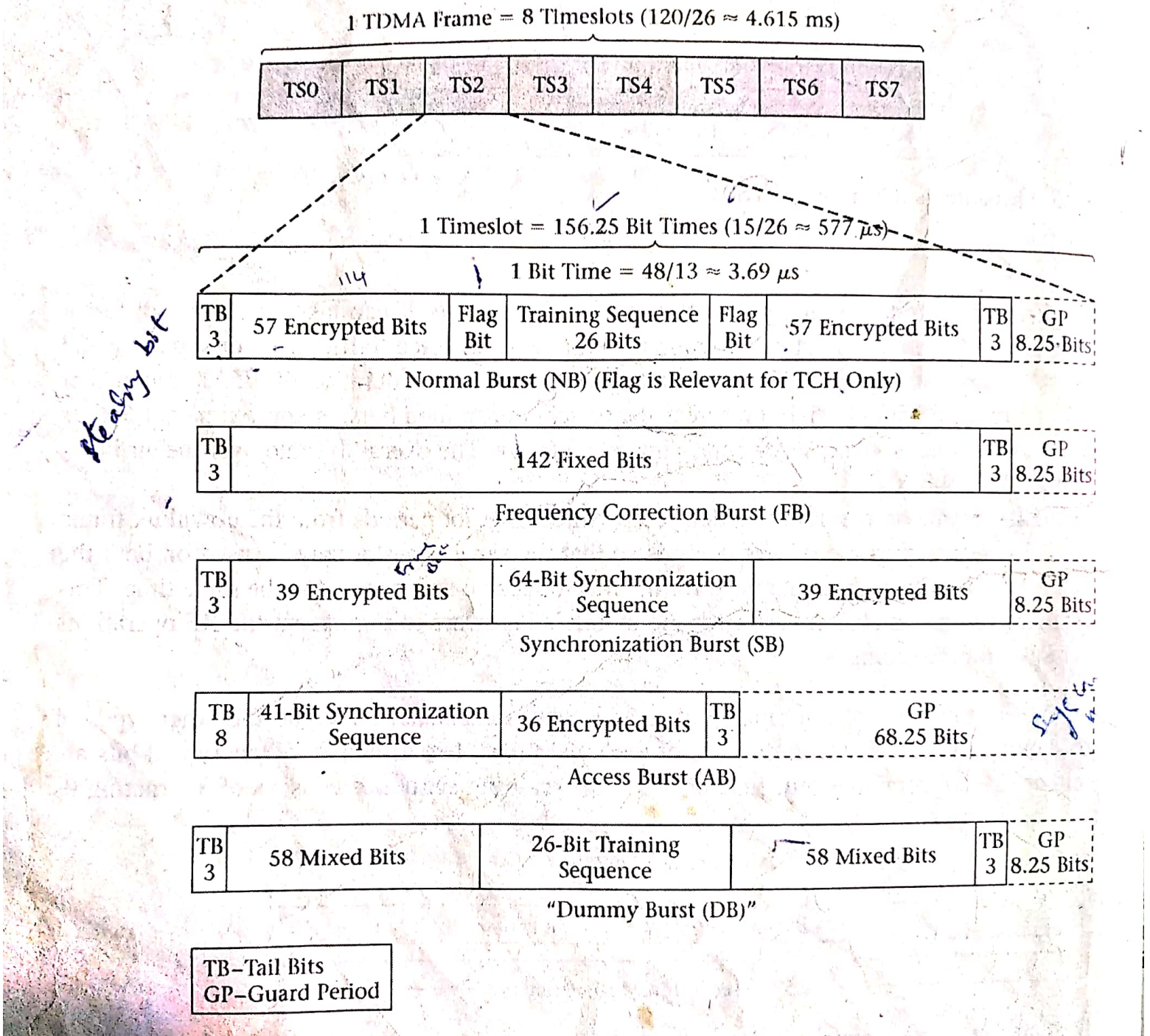


Figure 5–15 GSM traffic and control signal bursts (Courtesy of ETSI).

and 1s and is used to train the adaptive equalizer incorporated into the GSM mobile receiver. Three (3) tail bits precede the first group of traffic bits and 3 tail bits trail the last group of traffic bits. These tail bits consist of three zeros (unmodulated carrier) that provide time for the digital radio circuitry to initialize itself. Two single flag bits separate the training bit sequence from the encrypted bit groups. The flag bits are used to indicate whether the encrypted bits contain traffic or control information. The normal burst has an 8.25-bit long guard period at the end of the burst where no transmission activity takes place. When used as a traffic channel, a total of 114 encrypted bits are delivered per timeslot. Details of the encryption process will be presented later.

The frequency correction burst is used by the mobile to obtain frequency synchronization. It consists of 142 fixed bits (binary 0s or an unmodulated carrier) proceeded by 3 tail bits and followed by 3 tail bits. It also has the same 8.25-bit long guard period after it. The repetition of the frequency correction burst by the BTS within the GSM frame structure becomes the frequency correction channel (FCCH).

The synchronization burst is used by the mobile to obtain timing synchronization. It consists of 3 tail bits, followed by 39 encrypted bits, a 64-bit synchronization sequence, 39 more encrypted bits, 3 tail bits, and the same 8.25-bit long guard period. The encrypted bits contain information about the frame number (FN) and the base station identity code (BSIC). The repetition of the synchronizing sequence burst by the BTS within the GSM frame structure becomes the synchronizing channel (SCH).

The access burst is used by the mobile to facilitate random access requests by the mobile and handover operations. It consists of 8 tail bits followed by a 41-bit synchronization sequence, then 36 encrypted bits, and 3 tail bits. In this case, the length of the guard bit time period is equal to 252 μs or 68.25 bits. The reason for the long guard time is so a mobile that has just become active or has just been handed off and does not know the system timing advance can be accommodated. The value chosen allows for a cell radius of 35 km. The access burst is used on both the random access channel (RACH) and on the fast associated control channel (FACCH) during handover.

The dummy burst is transmitted on the radio frequency designated as c_0 when no other type of burst signal is being transmitted. It consists of 3 tail bits, 58 mixed bits, a 26-bit training sequence, 58 more mixed bits, 3 tail bits, and the same 8.25-bit long guard period. The purpose of the dummy burst is to ensure that the base station is always transmitting on the frequency carrying the system information. This affords the mobile the ability to make power measurements on the strongest BTS in its location and thus determine which BTS to attach to when first turned on. Furthermore, the mobile can also make measurements of other BTSs and therefore provide information to the system if handover is needed.

Access Grant Channel The access grant channel (AGCH) is used by the network to assign a signaling channel to the MS. After the mobile requests a signaling channel over the RACH the network will assign a channel to the mobile by transmitting this information over the AGCH. The AGCH is only transmitted in the downlink direction.

Dedicated Control Channels

The last group of broadcast channels is known as the dedicated control channels (DCCHs). These dedicated channels are used for specific call setup, handover, measurement, and short message delivery functions. The four DCCHs are the stand-alone dedicated control channel (SDCCH), the slow associated control channel (SACCH), the fast associated control channel (FACCH), and the cell broadcast channel (CBCH).

Stand-alone Dedicated Control Channel Both the mobile station and the BTS switch over to the network-assigned stand-alone dedicated control channel (SDCCH) that is assigned over the access grant channel in response to the mobile's request that has been transmitted over the random access channel. The call setup procedure (i.e., the initial steps required to set up a radio link) is performed on the SDCCH. The SDCCH is transmitted in both the uplink and downlink directions. When the call setup procedure is complete, both the mobile and the BTS switch to a preassigned available traffic channel.

Slow Associated Control Channel The slow associated control channel (SACCH) is used to transmit information about measurements made by the MS or instructions from the BTS about the mobile's parameters of operation. In the uplink direction the mobile sends measurements of the received signal strength from its own BTS and those of neighboring BTSs. In the downlink direction, the MS receives information from the BTS about the mobile's output power level and the timing advance that the mobile needs to use. The SACCH is transmitted in both the uplink and downlink directions over the same physical channels as the SDCCH or the TCH.

Fast Associated Control Channel The fast associated control channel (FACCH) is used to facilitate the handover operation in a GSM system. If handover is required, the necessary handover signaling information is transmitted instead of a 20-ms segment of speech over the TCH. This operation is known as "stealing mode" since the time allotted for the voice conversation is stolen from the system for a short period. The subscriber is usually not aware of this loss of speech since the speech coder in the mobile simply repeats the last received voice block during this process.

Cell Broadcast Channel The cell broadcast channel (CBCH) is used to deliver short message service in the downlink direction. It uses the same physical channel as the SDCCH.

Reverse Logical Channels

The IS-95 CDMA reverse logical channels exist between the subscriber devices and the CDMA base station. As mentioned previously, the encoding of digital information on the reverse channels is performed differently than on the forward channels. The data to be transmitted is not initially spread by a Walsh codes; instead, the data is mapped into Walsh codes that are then transmitted. Since there are sixty-four, 64-bit Walsh codes, every 6 bits of data to be transmitted may be mapped to a particular Walsh code. This technique yields an over tenfold increase in bandwidth since 64 bits are now transmitted for every 6 bits of

data; however, the system error rate is reduced in the process. The mapping of groups of 6 data bits to a Walsh code is very straightforward since there exists a one-to-one relationship between the two.

Each reverse channel is spread by a long PN sequence code and scrambled by the short PN sequence code. The long PN sequence code is derived from the subscriber device's 32-bit electronic serial number (ESN) and therefore provides the means by which the user is uniquely identified within the CDMA system. There are basically two types of reverse CDMA channels: access channels and reverse traffic/control channels. These logical channels will be further described in the next sections.

Access Channels

The CDMA access channels are used by the mobile to answer pages and to transmit control information for the purpose of call setup and tear down. Figure 6–18 shows the access channel processing for a IS-95 CDMA system. As shown in the figure, an access message at 4.8 kbps undergoes the familiar convolutional encoding, symbol repetition, and block interleaving that raises the data rate to 28.8 kbps. At this point, the orthogonal modulation subsystem processes the signal by encoding every 6 bits into a 64-bit Walsh code. This process raises the signal rate to 307.2 kcps. The reader should note the use at this time of chips per second (cps) instead of bits per second. This is standard notation within the CDMA industry when referring to the signal spreading process. Next, the long PN code spreads the signal by a factor of 4 that yields a chip rate of 1.2288 mcps. The signal is further scrambled by the short PN sequence codes. The long PN code is used by the system to differentiate the thirty-two possible access channels.

I Channel Pilot PN
at 1.2288 mcps

Access Channels

The CDMA access channels are used by the mobile to answer pages and to transmit control information for the purpose of call setup and tear down. Figure 6–18 shows the access channel processing for a IS-95 CDMA system. As shown in the figure, an access message at 4.8 kbps undergoes the familiar convolutional encoding, symbol repetition, and block interleaving that raises the data rate to 28.8 kbps. At this point, the orthogonal modulation subsystem processes the signal by encoding every 6 bits into a 64-bit Walsh code. This process raises the signal rate to 307.2 kcps. The reader should note the use at this time of chips per second (cps) instead of bits per second. This is standard notation within the CDMA industry when referring to the signal spreading process. Next, the long PN code spreads the signal by a factor of 4 that yields a chip rate of 1.2288 mcps. The signal is further scrambled by the short PN sequence codes. The long PN code is used by the system to differentiate the thirty-two possible access channels.

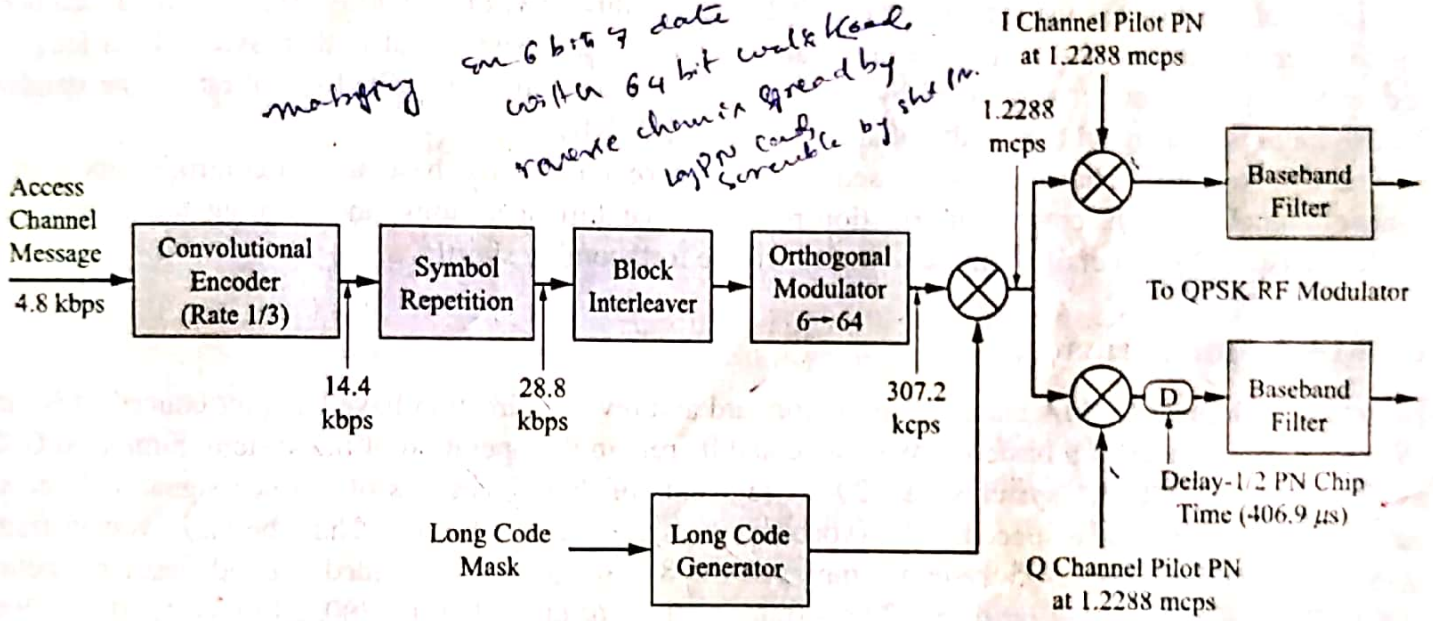


Figure 6–18 Generation of the CDMA reverse access channel.

At this point, the CDMA signal is applied to an RF quadrature modulator subsystem or IC. However, for the reverse channels, the form of modulation used to produce the final UHF passband signal is slightly different than for the forward channels. In this case, offset QPSK (OQPSK) is used instead of straight QPSK as in the case of the forward channels. Note the delay block of one-half of a PN chip (406.9 ns) used in the Q path to implement the OQPSK modulation. This form of modulation allows for a more power efficient and linear implementation by the subscriber device's RF electronics. As noted previously, any type of power savings technique that can lengthen battery life is usually employed when designing a mobile subscriber device.

Traffic/Power Control Channels

The IS-95 CDMA reverse traffic/power control channels support both voice and data at the two rate sets (RS1 and RS2) previously introduced. Figure 6–19 depicts the generation of a reverse traffic channel. In

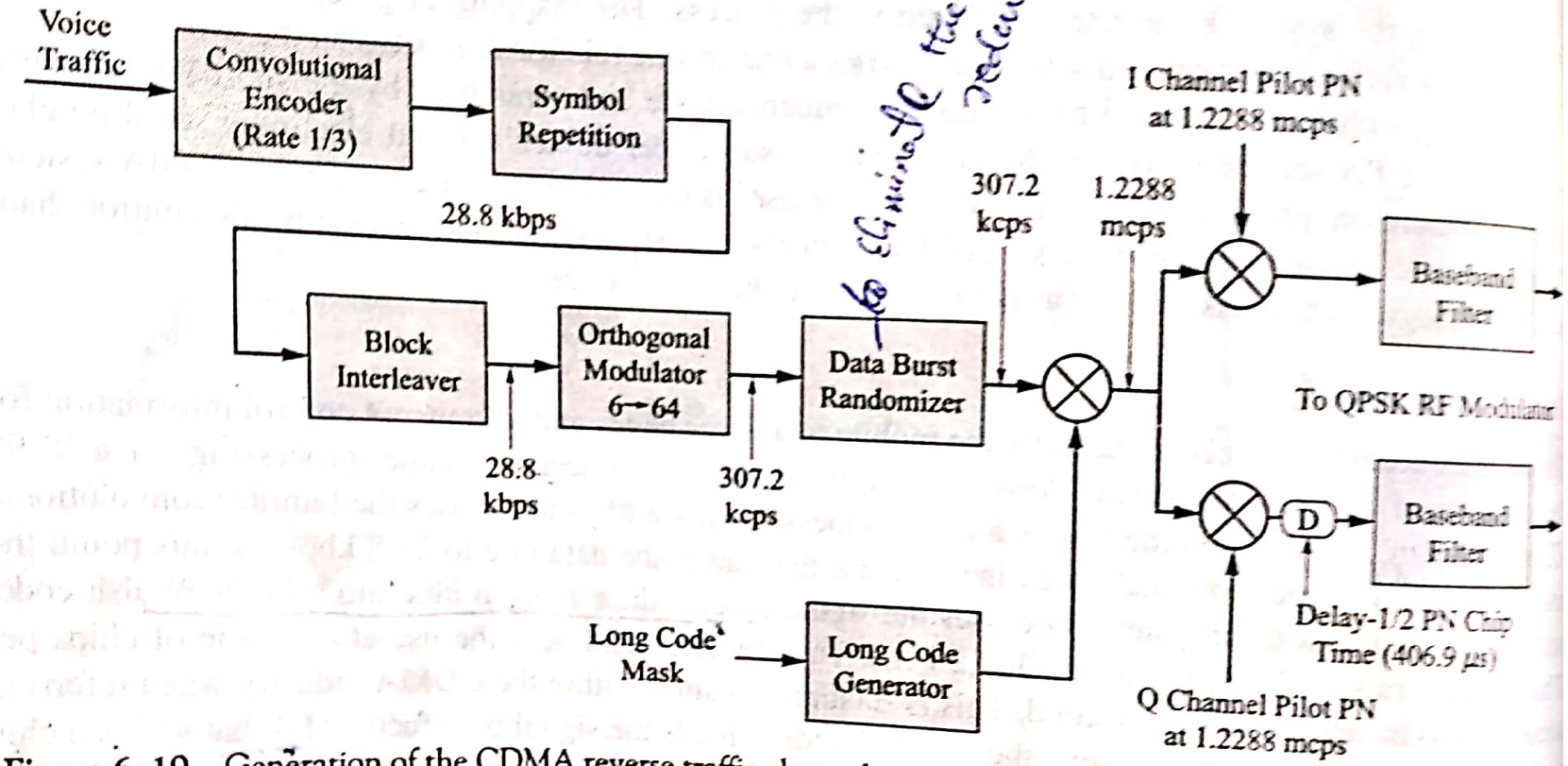


Figure 6–19 Generation of the CDMA reverse traffic channel.

either rate set case, the data rate at the input to the orthogonal modulator subsystem will be 28.8 kbps. A the output of this process the signal rate is 307.2 kcps. At this point the signal is processed by a data burs randomizer that in essence is used to eliminate redundant data. The signal is then spread by a long PN sequence code and further scrambled by the short PN sequence code. The final signal rate is the standard 1.2288 mcps with a signal bandwidth of approximately 1.25 MHz.

The reverse traffic channel is also used to send information to the base station controller about pilot channel signal strength, control information regarding handoff operations, and ongoing frame error rate (FER) statistics. More detail about these topics will be forthcoming shortly.

channel signal strength, control information regarding handoff operations, and ongoing frame error rate (FER) statistics. More detail about these topics will be forthcoming shortly.

CDMA Frame Format

Now that the logical CDMA channels in the forward and reverse direction have been introduced, it is time to examine the format of a basic CDMA frame and its role in the operation of the system. Similar to GSM system operation, CDMA systems take 20-ms segments of digital samples of a voice signal and encode them through the use of a speech coder (vocoder) into variable rate frames. Thus the basic system frame size is 20 ms. The first IS-95 systems employed the 8-kbps Qualcomm-coded excited linear prediction (QCELP) speech coder that produced 20-ms frame outputs of either 9600, 4800, 2400, or 1200 bps (Rate Set 1), with the addition of overhead (error detection) bits. The actual net bit rates are 8.6, 4.0, 2.0, or 0.8 kbps. A second encoder, the 13-kbps QCELP13 encoder, was introduced in 1995 and produced outputs of 14.4, 7.2, 3.6, and 1.8 kbps (Rate Set 2), with a net maximum bit rate of 13.35 kbps. In each case, the speech encoder makes use of pauses and gaps in the user's speech to reduce its output from a nominal 9.6 or 14.4 kbps to lower bit rates and 1.2 or 1.8 kbps during periods of silence.

The basic 20-ms speech encoder frame size is used in various configurations by several of the logical channels to facilitate CDMA system operation, increase system capacity, and improve mobile battery life. The next several sections will detail these operations.

Forward Channel Frame Formats

Of the four forward logical channels, only the pilot channel does not employ a frame format. It consists of a continuous transmission of the system RF signal (refer back to Figure 6–14). The forward traffic channel frames are 20 ms in duration and contain a varying number of information bits, frame error control check

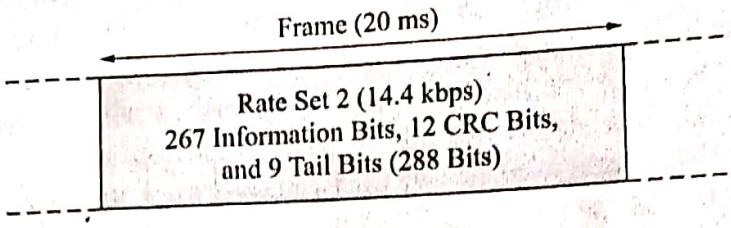


Figure 6–20 Rate Set 2 traffic channel structure.

bits, and tail bits depending upon the rate set and the data rate. Figure 6–20 depicts a forward traffic frame for Rate Set 2 at 14.4 kbps. The forward traffic channel frames are further logically subdivided into sixteen 1.25-ms power control groups. Power control bits transmitted over the forward traffic channels are randomly inserted into the data stream of each 1.25-ms power control group yielding a power control signal rate of 800 bps. More detail about the power control operation will be forthcoming later in this chapter.

The CDMA forward synchronization (sync) channel provides the mobile or subscriber device with system configuration and timing information. A sync channel message can be long and therefore the message is typically broken up into sync channel frames of 32 bits each. The sync channel frame consists of a start of message (SOM) bit and 31 data bits. The start of a sync message is indicated by a SOM bit set to 1 in the first frame and 0 in subsequent frames of the same message. At a data rate of 1200 bps, a sync channel frame is $26.66\bar{6}$ ms in duration (the same repetition period employed by the short PN codes). Three sync channel frames of 96 bits form a sync channel superframe of 80-ms duration (equal to four basic 20-ms frames). The sync message itself consists of a field that indicates the message length in bits, the message data bits, error checking code bits, and additional padding bits (zeros) as needed.

The forward paging channels are used by the CDMA base station to transmit system overhead information and mobile station-specific messages. In IS-95A, the paging channel data rate can be either 4800 or 9600 bps. The paging channel is formatted into 80-ms paging slots of eight half frames of 10-ms duration. Each half frame starts with a synchronized capsule indicator (SCI) bit that is functionally similar to the SOM bit. A synchronized paging channel message capsule begins immediately after an SCI bit set to 1. To accommodate varying-length paging messages and to prevent inefficient operation of the paging channel, additional message capsules may be appended to the end of the first message capsule if space is available within the half frame or subsequent half frames. A paging message must be contained in at most two successive slots.

Furthermore, the paging channel structure is formatted into paging slot cycles to provide for increased mobile station battery life. A CDMA mobile may operate in either a slotted or unslotted mode. In the unslotted mode the mobile reads all the page slots while in the *mobile station idle state*. In the slotted mode, the mobile wakes up periodically to check for paging messages directed to it in specific preassigned slots (again, in the *mobile station idle state*). Therefore, slotted mode operation permits the mobile station to power down energy-consumptive RF electronic circuitry until its specific paging slot arrives. The mobile station will wake up for one or two paging slots (if required) of the paging slot cycle. The length of the paging cycle can vary from a minimum of sixteen slots (1.28 s) to a maximum of 2048 slots (163.84 s) (see Figure 6–21 for a diagram of the paging channel structure) as established by the system. Typically, minimal length cycles are employed; otherwise, significant delays in call termination could result. The CDMA system uses the mobile station's ESN to determine the correct slot to use for paging of the mobile. Further power savings are realized while in slotted mode by the transmission of a _DONE message by the base station after the end of the paging message scheduled for the particular mobile. In the case of a short message that uses only several half frames of a slot, the mobile can power down before the end of the slot to save even more battery power.

Reverse Channel Frame Formats

station

The mobile station with ... length of the paging cycle can vary from a minimum of sixteen slots (1.28 s) to a maximum of 2048 slots (163.84 s) (see Figure 6–21 for a diagram of the paging channel structure) as established by the system. Typically, minimal length cycles are employed; otherwise, significant delays in call termination could result. The CDMA system uses the mobile station's ESN to determine the correct slot to use for paging of the mobile. Further power savings are realized while in slotted mode by the transmission of a _DONE message by the base station after the end of the paging message scheduled for the particular mobile. In the case of a short message that uses only several half frames of a slot, the mobile can power down before the end of the slot to save even more battery power.

Reverse Channel Frame Formats

The reverse traffic channel, like the forward traffic channel, is also divided into 20-ms traffic channel frames. The reverse traffic channel frame is also further logically subdivided into sixteen 1.25-ms power

control groups. As was the case for the forward traffic channel, variable rate [illegible] reverse traffic channel. The coded bits from the convolutional encoder used in the reverse traffic channel are repeated before interleaving when the speech characteristics are such that the encoded data rate is less than the maximum. When the mobile transmit data rate is maximum, all sixteen power control groups are transmitted. If the transmitted data rate is one half of the maximum rate, then only eight power control groups are transmitted. Similarly, for a transmitted data rate of one-quarter or one-eighth, only four or two power control groups are transmitted per frame, respectively. As mentioned, this process, termed *burst transmission*, is made possible by the fact that reduced data rates have built-in redundancy that has been generated by the code repetition process. A data burst randomizer ensures that every repeated code symbol is only transmitted one time and that the transmitter is turned off at other times. This process reduces interference to other mobile stations operating on the same reverse CDMA channel by lowering the average transmitting power of the mobile and hence the overall background noise floor. The data burst randomizer generates a random masking pattern for the gating pattern that is tied to the mobile station's ESN. Figure 6–22 shows this process in more detail.

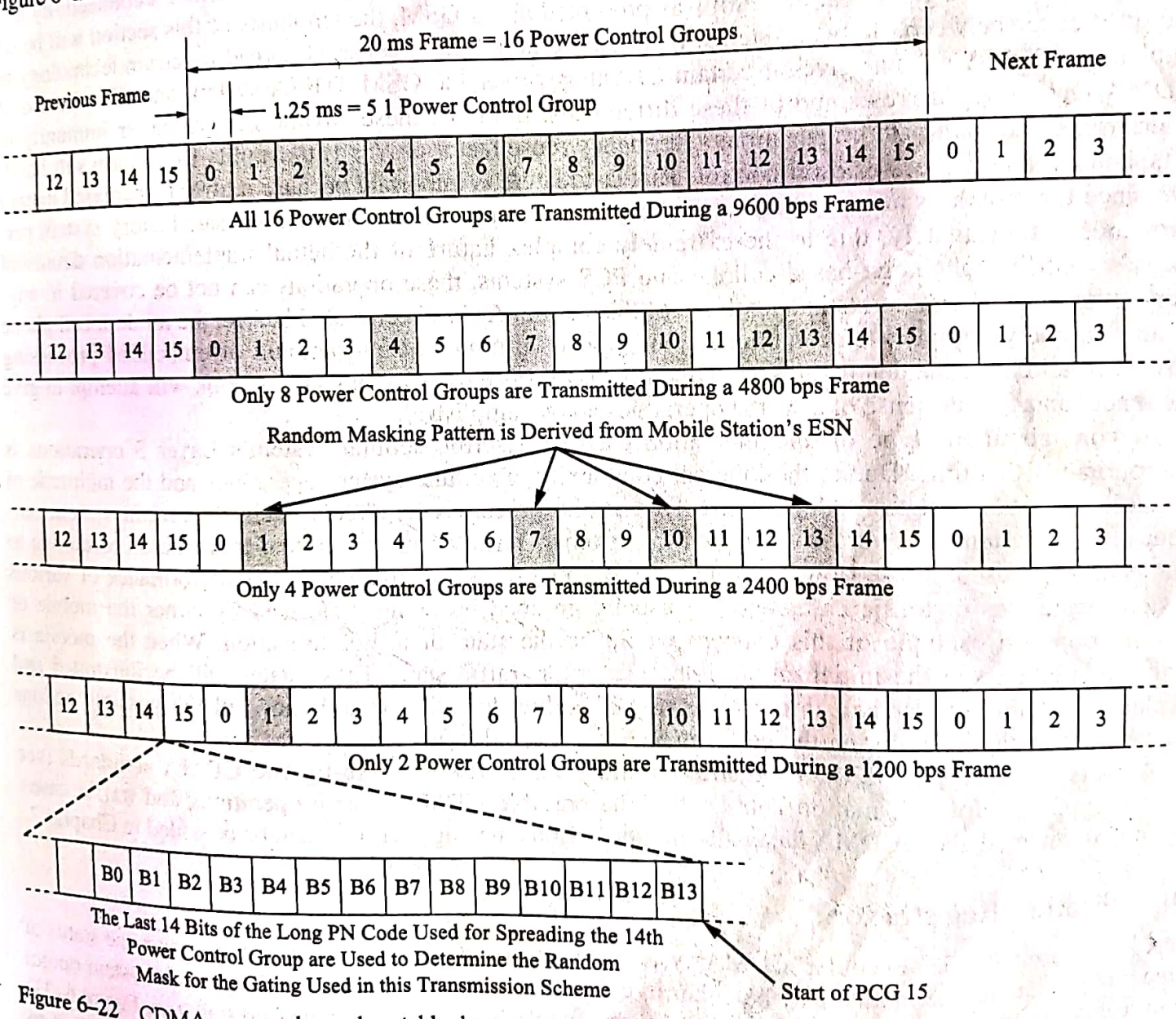


Figure 6–22 CDMA reverse channel variable data rate transmission.

The reverse access channel is used by the mobile station to communicate with the base station. The access channel is used for short message exchanges, such as responses to commands from the base station, for system registrations, and for call origination requests. The access channel data rate is 4.8 kbps using a

20-ms frame that contains 96 information bits. Each access channel message is typically composed of several access channel frames.

Since multiple mobile stations associated with the same paging channel may try to simultaneously access the same access channel, a random access protocol has been developed to avoid signal/data collisions. This topic will be discussed further in the next section about CDMA System Operations.

6.4 CDMA SYSTEM (LAYER 3) OPERATIONS

Initialization/Registration

As is the case with GSM cellular, CDMA system registration procedures are dependent upon the status of the mobile station. The mobile may be either in a detached condition (powered off or out of system range) or in an attached condition. When first turned on, the mobile goes through a power-up state (see Figure 6–23) during which it selects a CDMA system and then acquires the pilot and sync channels, which allows it to synchronize its timing to the CDMA system. When attached, the mobile may be in one of three states: the mobile station idle state, the system access state, or the mobile station control on the traffic channel state (see Figure 6–24).

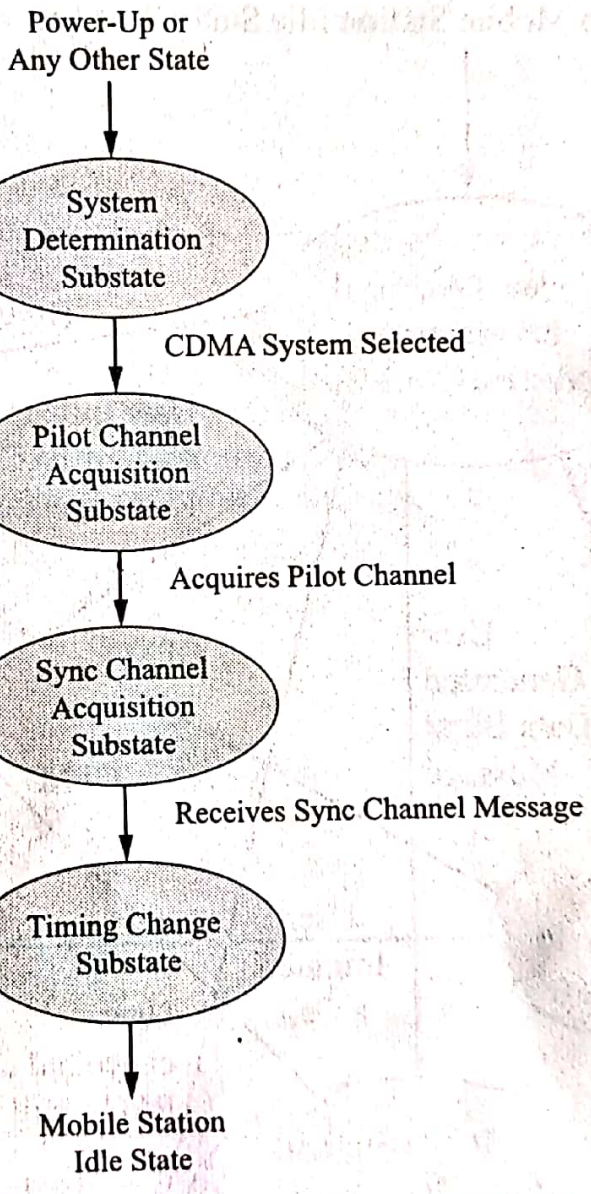


Figure 6–23 CDMA mobile station initialization state (Courtesy of 3GPP2).