Prentice Hall Communications Engineering and Emerging Technologies Series

Theodore S. Rappaport, *Series Editor*

DOSTERT *Powerline Communications*

GARG *Wireless Network Evolution: 2G to 3G*

GARG *IS-95 CDMA and cdma2000: Cellular/PCS Systems Implementation*

GARG & WILKES *Principles and Applications of GSM*

HAĆ *Multimedia Applications Support for Wireless ATM Networks*

KIM *Handbook of CDMA System Design, Engineering, and Optimization*

LIBERTI & RAPPAPORT *Smart Antennas for Wireless Communications: IS-95 and Third Generation CDMA Applications*

PAHLAVAN & KRISHNAMURTHY *Principles of Wireless Networks: A Unified Approach*

RAPPAPORT *Wireless Communications: Principles and Practice, Second Edition*

RAZAVI *RF Microelectronics*

STARR, CIOFFI & SILVERMAN *Understanding Digital Subscriber Line Technology*

PRINCIPLES OF WIRELESS NETWORKS

A Unified Approach

Kaveh Pahlavan
Worcester Polytechnic Institute
University of Oulu

Prashant Krishnamurthy
University of Pittsburgh

PH PTR
Prentice Hall PTR
Upper Saddle River, New Jersey 07458
www.phptr.com

Library of Congress Cataloging-in-Publication Data

Pahlavan, Kaveh, 1951-
Principles of wireless networks: a unified approach / Kaveh Pahlavan, Prashant Krishnamurthy
p. cm.— (Prentice Hall communications engineering and emerging technologies series)
Includes bibliographical references and index.
ISBN 0-13-093003-2
1. Wireless communication systems. I. Krishnamurthy, Prashant. II. Title. III. Series.
TK5103.2 .P3397 2002
621.382—dc21

2002002268

To those whose love kept us writing, those whose work inspired our learning, and those with whom we learned.

Acquisitions editor: *Bernard Goodwin*
Marketing manager: *Dan DePasquale*
Manufacturing buyer: *Alexis Heydt-Long*
Editorial/production supervision: *Jessica Balch (Pine Tree Composition)*
Production coordinator: *Anne R. Garcia*
Cover design director: *Jerry Votta*
Cover design: *Anthony Gemmellaro*
Art director: *Gail Cocker-Bogusz*
Art studio: *LP Graphics*

Prentice-Hall, Inc.
Upper Saddle River, New Jersey 07458

Prentice Hall books are widely used by corporations and government agencies for training, marketing, and resale.

The publisher offers a discount on this book when ordered in bulk quantities. For more information, contact: Corporate Sales Department, Phone: 800-382-3419; Fax: 201-236-7141; E-mail: corpsales@prenhall.com; or write: Prentice Hall PTR, Corp. Sales Dept., One Lake Street, Upper Saddle River, NJ 07458

Printed in the United States of America
10 9 8 7 6 5 4 3 2

Reprinted with corrections November, 2002.

ISBN 0-13-093003-2

Pearson Education Ltd., *London*
Pearson Education Australia Pty, Limited, *Sydney*
Pearson Education Singapore, Pte. Ltd.
Pearson Education North Asia Ltd., *Hong Kong*
Pearson Education Canada, Ltd., *Toronto*
Pearson Educación de Mexico, S.A. de C.V.
Pearson Education—Japan, *Tokyo*
Pearson Education Malaysia, Pte. Ltd.

CONTENTS

Preface xi

CHAPTER 1 Overview of Wireless Networks 1

1.1 Introduction 2
1.2 Different Generations of Wireless Networks 12
1.3 Structure of the Book 21
Appendix 1A Backbone Networks for Wireless Access 26
Appendix 1B Summary of Important Standards Organizations 33
Questions 34

PART ONE PRINCIPLES OF AIR-INTERFACE DESIGN 37

CHAPTER 2 Characteristics of the Wireless Medium 39

2.1 Introduction 40
2.2 Radio Propagation Mechanisms 44
2.3 Path-Loss Modeling and Signal Coverage 46
2.4 Effects of Multipath and Doppler 58
2.5 Channel Measurement and Modeling Techniques 68
2.6 Simulation of the Radio Channel 71
Appendix 2A What is dB? 76
Appendix 2B Wired Media 77
Appendix 2C Path Loss Models 79
Appendix 2D Wideband Channel Models 79
Questions 80
Problems 81

CHAPTER 9 MOBILE DATA NETWORKS

During the evolution of 2G systems, mobile data or data-oriented wireless WANs emerged as independent connectionless networks serving mobile computers over a large geographical area. As we got closer to the 3G systems, mobile data services became integrated with the cellular voice services. Chapter 9 is devoted to various aspects of this fragmented technology. We first provide an overview of the major mobile data networks and classify them into logical groups. Then we provide details of CDPD and GPRS networks to demonstrate the operation of two popular methods for implementation of the mobile data services. The last sections in the chapter describe SMS and wireless data applications.

CHAPTER 7

GSM AND TDMA TECHNOLOGY

7.1 Introduction

7.2 What is GSM?

7.2.1 GSM Services
7.2.2 Reference Architecture

7.3 Mechanisms to Support a Mobile Environment

7.3.1 Registration
7.3.2 Call Establishment
7.3.3 Handover
7.3.4 Security

7.4 Communications in the Infrastructure

7.4.1 Layer I: Physical Layer
7.4.2 Layer II: Data Link Layer
7.4.3 Layer III: Networking Layer

Questions

Problems

7.1 INTRODUCTION

In this book we first provided the path of evolution of the wireless information networking industry and identified forces that have shaped this evolution. All the major standards that have emerged in this evolution were introduced, and they were logically categorized into different groups at different stages of evolution. In the second part of the book, we introduced principles of operation of these networks by dividing technical aspects into logical categories and explaining each aspect with examples from existing systems. In the rest of the book, we discuss the example systems to provide the reader with a deeper understanding of the details of how a variety of networks operate. This description is also divided into two groups, systems for WANs and those for LANs. Among WANs we first discuss voice-oriented networks that employ TDMA and CDMA for channel access. Our detailed example of TDMA systems is GSM, and for CDMA systems we discuss IS-95 and IMT-2000. Then we examine data-oriented WANs—those integrated with the voice-oriented networks by using the same air-interface and those that have their own air-interface. The example for the first group is GPRS, and the example for the second group is CDPD.

The rest of this chapter is devoted to TDMA systems with GSM as the example system. As we described in Chapter 1, a number of TDMA systems emerged in the 1980s during the evolution of the 2G systems. These systems included the Pan-European GSM, the North American IS-136, and the Japanese JDC digital cellular standards, and CT-2, DECT, PHS, and PACS standards for the then so-called PCS services. In the 1990s, with the advancements in battery technology for handheld terminals and the overwhelming popularity of cellular telephones, the differentiation between digital cellular and PCS systems disappeared. The increasing demand for capacity diverted the attention of the service providers to the availability of spectrum rather than technology. With the emergence of the new PCS bands at around 2 GHz, most service providers expanded their cellular services by upgrading the frequency of operation of their digital cellular systems from around 1 GHz to around 2 GHz, without using the so-called PCS standards. Today, GSM is by far the most popular TDMA standard in the world; it is used both in the cellular and PCS bands. The structure of the system is also very clear and useful for educational purposes. Therefore, we use GSM as our example for TDMA systems.

Wireless networks are complex multidisciplinary systems, and a description of their standards is often very long and tedious. Our objective in explaining standards is to provide the reader with an adequate understanding of the overall objectives of a system, a view of the architecture of the hardware and software elements of the network, and details of protocols and algorithms to understand how information transfer works. In this chapter we first define the objectives and architecture of the GSM. Then we discuss mechanisms that are designed to support mobility to the GSM terminals, and at last we describe protocols used for communication among the elements of the infrastructure. For further details and other presentations of the GSM standard, we refer the readers to [SIE95], [MEH97], [TIS98], [GOO97]. To minimize the difficulties in understanding the details of all standards, we have made a conscious effort to follow a similar pattern in describing other standards in the rest of the book. Following a similar format will help the reader grasp a better overall picture and be more comfortable in reading the details. However, this effort will not completely eliminate our difficulties because each standard uses its own reference model and a number of acronyms that are different from one standard to another. To further help the reader, we have also provided a number of examples that describe certain features of a standard in depth. This way we have preserved the flow of the depth of the text, while some important features are treated in more details.

7.2 WHAT IS GSM?

The Global System for Mobile (GSM) is an ETSI standard for 2G pan-European digital cellular with international roaming. In 1982, frequency bands of 890–915 MHz and 935–960 MHz were allocated for the Pan-European Public Land Mobile Network (PLMN), and the GSM was formed. The main charter of the group was to develop a 2G standard to resolve the roaming problem in the six existing different 1G analog cellular systems in Europe. After evaluating several options, the committee decided to go for a unified new digital standard as it would facilitate roaming and at the same time provide for large-volume production. In 1986, the task force was formed, and in 1987 a memorandum of understanding was signed. In 1989, ETSI included GSM in its domain, and the name of the group was changed to Special Mobile Group (SMG). The resulting standard was named the Global System for Mobile (GSM) communications. In 1991, the specification of the standard was completed, and in 1992, the first deployment started. By the year 1993, 32 operators in 22 countries adopted the GSM standard, and by 2001, close to 150 countries [GSMweb] had adopted GSM for cellular operation.

Although the original goals of the GSM could be met only by defining a new air-interface, the group went beyond just the air-interface and defined a system that complied with emerging ISDN-like services and other emerging fixed network features. To this end, the committee also defined a number of other interfaces between the hardware and software elements of the network, making GSM a complete digital cellular standard that is very suitable for pedagogical purposes. One of the interesting ironies of this evolution is that GSM, and later on all other 2G digital cellular systems, brought ISDN-like mobile digital services to all users while the original wired ISDN lost its popularity and never found a massive acceptance with users. This reflects the real multidisciplinary nature of the telecommunication industry in which the behavior of the market is not always as predictable as more focused industries such as component design.

7.2.1 GSM Services

The first step in understanding a multipurpose system is to identify the services that are provided by that network because the entire network is designed to support these services. Analog cellular systems were developed for a single application—voice—and in a manner similar to analog access to the PSTN, other data services such as fax and voice-band modems were defined as overlay services on top of the

analog voice service. GSM is an integrated voice-data service that provides a number of services beyond cellular telephone. Table 7.1 [RED95] shows the GSM Phase 1 services and Table 7.2 [RED95] shows the GSM Phase 2 services. These services are divided into three categories: teleservices, bearer services, and supplementary services.

Teleservices provide communication between two end user applications according to a standard protocol. As shown in Table 7.1, Phase 1 GSM bearer services were telephony, emergency speech calls, Group 3 facsimile, teletex, short messages (unicast and multicast), and videotex. The upper-most layer of the protocol stack of the standard should be specified so that it could communicate with protocols used in these applications.

Bearer services provide capabilities to transmit information among user-network-interfaces or APs. Traditional bearer services include a variety of asynchronous and synchronous data access to PSTN/ISDN and packet switched public data networks as shown in Table 7.1. To implement bearer services, the lower layers and frame format of the standard should specify how these transmissions would be implemented over the air-interface.

Supplementary services are not stand-alone services but they are services that supplement a bearer- or teleservice. Supplementary services in Phase 1 GSM were call forwarding and call barring. They were applied to both bearer and teleservices. Other supplementary services include call waiting and calling number identification. These services are usually implemented at the wired infrastructure of the cellular network. Table 7.2 provides a wider range of services for GSM Phase 2 which demonstrate how services can evolve with different phases in time.

7.2.2 Reference Architecture

Description of a wireless network standard is a complex process that involves detailed specification of the terminal, fixed hardware backbone, and software databases that are needed to support the operation. To describe such a complex system, a reference model or overall architecture is needed to provide an overall understanding of the network elements and operation and divide the system into subsys-

Table 7.1 GSM Phase 1 Services

Service Category	Service	Comment
Teleservices	Telephony	Full rate at 13 kbps voice
	Emergency calls	"112" is GSM-wide emergency number
	Short messaging service	Point to point (between two users) and cell broadcast types
	Videotext access	
	Teletex, FAX, etc.	
Bearer Services	Asynchronous data	300–9,600 bps (transparent/nontransparent)
	Synchronous data	2400–9,600 bps transparent
	Synchronous packet data	
	Others	
Supplementary Services	Call forwarding	All calls, when subscriber is not available
	Call barring	Outgoing calls with specifications

Table 7.2 GSM Phase 2 Additional Services

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

tems. Our presentation of the GSM system is organized in three major segments shown in Figure 7.1. These segments are mobile station (MS), base station subsystem (BSS), and network and switching subsystem (NSS). Figure 7.2 provides a more physical representation of the architectural elements of GSM and the relation among these elements. This division of the architectural elements was adopted from [HAU94], and we follow that for the description of the system elements in the following section.

7.2.2.1 Mobile Station

The MS communicates the information with the user and modifies it to the transmission protocols of the air-interface to communicate with the BSS. The user information is communicated with the MS through a microphone and speaker for

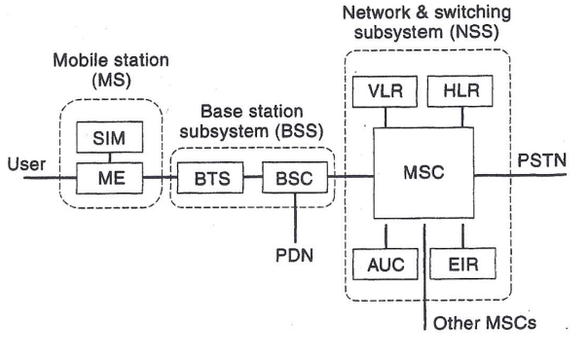

Figure 7.1 Reference architecture of GSM.

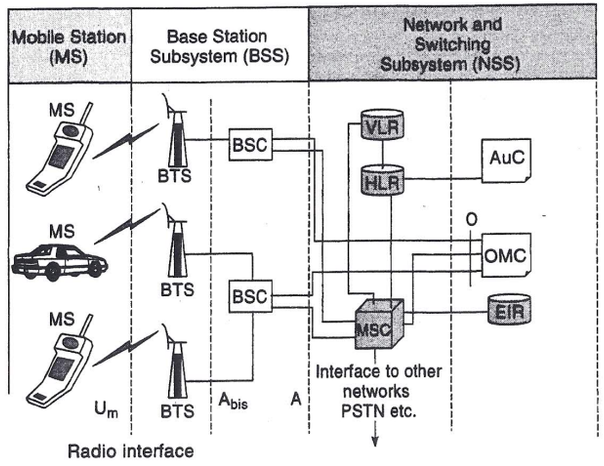

Figure 7.2 A different view of the reference architecture for GSM.

the speech, keypad, and display for short messaging, and the cable connection for other data terminals. The MS has two elements. The first element is *mobile equipment* (ME), which is a piece of hardware that the customer purchases from the equipment manufacturer or their dealers. This hardware piece contains all the components needed for the implementation of the protocols to interface with the user and the air-interface to the BSS. The components include speaker, microphone, keypad, and the radio modem. Therefore, the ME is an expensive piece of hardware. To encourage more users to subscribe to the wireless services, a number of service providers in the early days of the cellular industry, and even today, subsidize the price of the MEs.

The second element of the MS in the GSM is the *subscriber identity module* (SIM) that is a smart card issued at the subscription time identifying the specifications of a user such as address and type of service. The calls in the GSM are directed to the SIM rather than the terminal. Short messages are also stored in the SIM card. Using SIM cards was not a possibility with the analog cellular systems, and the existing North American digital cellular standards have not implemented this option. Although implementing a SIM is a fairly simple concept, it has a significant impact on the way that a user transacts with the service provider. A SIM card carries every user's personal information which enables a number of useful applications.

Example 7.1: Roaming and SIMs

People visiting different GSM-enabled countries who are not keen on making calls at their home number can always carry their own terminal and purchase a SIM card in every country that they visit. This way they avoid roaming charges and the expense of having a different contact number.

Example 7.2: Sharing a Single Terminal and SIMs

Several users can share a terminal with different SIM cards. At the Telecommunication Laboratory, University of Oulu, Finland, they have a number of GSM MEs that they loan to visitors for use with their own SIMs. Therefore, visitors from the United States and Canada can obtain a cellular service for their personal use without investing in a terminal that may not be useful at home.

Because SIM cards carry the private information for a user, a security mechanism is implemented in the GSM that asks for a four-digit PIN number to make the information on the card available to the user.

7.2.2.2 Base Station Subsystem

The BSS communicates with the user through the wireless air-interface and with the wired infrastructure through the wired protocols. In other words, it translates between the air-interface and fixed wired infrastructure protocols. The needs for the wireless and wired media are different because the wireless medium is unreliable, bandwidth limited, and needs to support mobility. As a result, protocols used in the wireless and wired mediums are different. The BSS provides for the translation among these protocols.

Example 7.3: Speech Conversion

The user's speech signal is converted into 13 kbps-digitized voice with a speech coder and communicated over the air-interface to provide a bandwidth efficient air-interface. The backbone wired network uses a 64 kbps PCM digitized voice in the PSTN hierarchy. Conversion from analog to 13 kbps voice takes place at the MS, and the change from 13 to 64 kbps coding takes place at the BSS.

Example 7.4: Signaling in GSM

The signaling format to establish a connection in wired networks is a multitone frequency scheme used in POTS. GSM, on the other hand, establishes the call through the exchange of a number of packets. The translation of this communication into a dialing signal is made in the BSS.

As with speech coding and dialing, explained in these examples, data transmission protocols over the air-interface are different from that of the wired infrastructure. All these translations are performed at the BSS. As we will see in the description of GPRS in Chapter 9, to implement packet data services on the same air-interface as GSM, the BSS also separates packet switching data from the PSTN traffic and directs it to the packet switched data networks. There are two architectural elements in the BSS.

The *BTS* is the counterpart of the MS for physical communication over the air-interface. The BTS components include a transmitter, a receiver, and signaling equipment to operate over the air-interface, and it is physically located in the center of the cells where the BSS antenna is installed. One BSS may have from one up to several hundred BTSs under its control [RED95].

The second architectural element of the BSS is the *BSC,* that is a small switch inside the BSS in charge of frequency administration and handover among the BTSs inside a BSS. The hardware of the BSC in single BTS site is located at the antenna and in the multi-BTS systems in a switching center where other hardware elements of NSS are located.

7.2.2.3 Network and Switching Subsystem

The NSS is responsible for network operation. It provides for communications with other wired and wireless networks, as well as support for registration and maintenance of the connection with the MSs. The NSS could be interpreted as a wireless specific switch that communicates with other switches in the PSTN and at the same time supports functionalities that are needed for a cellular mobile environment. The NSS in the GSM interconnects to the PSTN through ISDN protocols. Indeed, in the development of GSM a conscious effort has been made to use ISDN compatible protocols. The NSS is the most elaborate element of the GSM network, and it has one hardware, MSC, and four software elements: visitor location register (VLR), home location register (HLR), equipment identification register (EIR), and authentication center (AUC).

A *MSC* is the hardware part of the wireless switch that can communicate with PSTN switches using the signaling system-7 (SS-7) protocol, as well as other MSCs in the coverage area of a service provider. Sometime the MSC that communicates with the PSTN is referred to as Gateway MSC (GMSC) [RED95]. The MSC also provides to the network the specific information on the status of the mobile terminals.

HLR is database software that handles the management of the mobile subscriber account. It stores the subscriber's address, service type, current location, forwarding address, authentication/ciphering keys, and billing information. In addition to the ISDN telephone number for the terminal, the SIM card is identified with an international mobile subscriber identity (IMSI) number that is totally different from the ISDN telephone number. The IMSI is used totally for internal networking applications.

Example 7.5: Numbering Schemes in GSM

The telephone number of a subscriber in Finland could be 358-40-770-5246. The first three digits are the country code; the next two are the digits for the specific MSC, and the rest are the telephone number. The IMSI of the same user can be 244-91 followed by a 10-digit number that is totally different from the ISDN telephone number. The first three digits of the IMSI identify the country, Finland, and the next two digits, the billing company (SONERA, formerly Finnish Telecom).

VLR is a temporary database software similar to the HLR identifying the subscribers visiting inside the coverage area of an MSC. The VLR assigns a temporary mobile subscriber identity (TMSI) that is used to avoid using IMSI on the air. Maintenance of two databases at home and at the visiting site allows a mechanism to support call routing and dialing in a roaming situation where the MS is visiting the coverage area of a different MSC. As discussed in Chapter 6 and as we will see in the later chapters, the mechanism of holding two databases to support mobility is used almost in all mobile networks.

The *AUC* holds different algorithms that are used for authentication and encryption of the subscribers. Different classes of SIM cards have their own algorithms, and the AUC collects all of these algorithms to allow the NSS to operate with different terminals from different geographic areas.

The *EIR* is another database managing the identification of the mobile equipment against faults and theft. This database keeps the *international mobile equipment identity* (IMEI) that reveals the manufacturer, country of production, and terminal type. Such information can be used to report stolen phones or check if the phone is operating according to the specification of its type. The implementation of the EIR is left optional to the service provider.

7.3 MECHANISMS TO SUPPORT A MOBILE ENVIRONMENT

Now that we have described all the hardware and software elements of the GSM network, we can describe how different functionalities of the network is implemented with these elements. Four mechanisms are embedded in all voice-oriented wireless networks that allow a mobile to establish and maintain a connection with the network. These mechanisms are registration, call establishment, handover (or hand-off), and security. Registration takes place as soon as one turns the mobile unit on, call establishment occurs when the user initiates or receives a call, handover helps the MS to change its connection point to the network, and security protects the user from fraud and eavesdropping. General description of these mechanisms are in Chapter 6; in this section we describe the details of their implementation over the GSM architecture that was described in the last section. To illustrate the complexity of wireless networks, when we discuss registration and call establishment in GSM we compare these mechanisms with their counterpart in POTS.

7.3.1 Registration

When we subscribe to a POTS service, the telephone company brings a pair of wires to our home that is connected to a port of a switch in a PSTN end office. Then our telephone number is registered in a database in the network, and our registration is fixed. Therefore, connection and registration process for a wired access to the network is a one-shot operation, and after that connection is active and registration is valid as long as subscription to service is valid. With wireless access to a cellular network, each time that we turn the MS on we need to establish a new connection and possibly establish a new registration with the network. We may actually connect to the network at different locations through a BS that may not be

owned by our service provider. Therefore, a wireless network needs a registration process that is far more complex than the registration in wired networks.

Technically speaking, as we turn on an MS it passively synchronizes to the frequency, bit, and frame timings of the closest BS to get ready for information exchange with the BS.

After this preliminary setup, the MS reads the system and cell identity to determine its location in the network. If the current location is not the same as before, the MS initiates a *registration* procedure. During a registration procedure, network provides the MS with a channel for preliminary signaling. The MS provides its identity in exchange for the identity of the network, and finally the network authenticates the MS. The simplest connection takes place if the MS is turned on in the previous area, and the most complex registration process occurs when the mobile is turned on in a new MSC area which needs changes in the entries of the VLR and HLR. The following example illustrated the complexity of the registration process of the GSM when a mobile is turned on in a new MSC.

Example 7.6: The Registration Procedure

Figure 7.3 shows the 12-step registration process in the GSM that takes place when an MS is turned on in a new MSC area. In the first four steps, a radio channel is established between the MS and BSS to process the registration. In the next four steps, the NSS authenticates the MS. In the next three steps, a TMSI is assigned, and adjustments are made to the entries in the VLR and HLR. In the final step, the temporary radio channel for communication is released, and transmission starts over a traffic channel.

Steps	MS	BTS	BSC	MSC	VLR	HLR
1. Channel request	→	→				
2. Activation response		←				
3. Activation ACK		→				
4. Channel assigned	←	←				
5. Location update request	→	→	→			
6. Authentication request	←	←	←			
7. Authentication response	→	→	→			
8. Authentication check				↔		
9. Assigning TMSI	←	←	←			
10. ACK for TMSI	→	→	→			
11. Entry to VLR and HLR				↔	↔	
12. Channel release	←	←				

Figure 7.3 Registration procedure.

7.3.2 Call Establishment

Call establishment in POTS starts with a dialing process that transfers the number to the nearest PSTN switch where a routing algorithm finds the best connection through intermediate switches to the destination. After establishment of the link, the last switch (end office) at the destination sends a signal back to the source to announce whether the destination is available or busy that is signaled to the user at the source. When the destination POTS terminal is off-hook, another signal is sent to the source end-office to stop the waiting tone and establish the traffic line. In the mobile environment we have two separate call establishment procedures for mobile-to-fixed and fixed-to-mobile calls. Mobile-to-mobile calls are a combination of the two. The following two examples provide the detailed procedure in the GSM network for both types of call establishment.

Example 7.7: Mobile Originated Call

The five-step procedure in POTS for call setup changes to a 15-step mobile originated call establishment procedure in the GSM. As shown in Figure 7.4, the first five steps are similar to the registration process in GSM, except that these are done to prepare for call establishment. The next two steps start ciphering (encryption) to provide a protection against eavesdropping. The rest of the steps are similar to those in wired networks except that we have an additional traffic channel assignment procedure.

Steps	MS	BTS	BSC	MSC
1. Channel request	→	→	→	
2. Channel assigned	←	←	←	
3. Call establishment request	→	→	→	→
4. Authentication request	←	←	←	←
5. Authentication response	→	→	→	→
6. Ciphering command	←	←	←	←
7. Ciphering ready	→	→	→	→
8. Send destination address	→	→	→	→
9. Routing response	←	←	←	←
10. Assign traffic channel	→	→	→	
11. Traffic channel established	←	←	←	
12. Available/busy signal	←	←		
13. Call accepted	←	←	←	←
14. Connection established	→	→	→	→
15. Information exchange	←			→

Figure 7.4 Mobile originated call.

Example 7.8: Mobile Terminated Call

The most complicated call establishment is for the situation where a fixed telephone dials a mobile visiting another MSC. As shown in Figure 7.5, after dialing, the PSTN directs the call to the MSC identified by the destination address. The MSC requests routing information from the HLR. Because, in this case, the mobile is roaming in the area of a different MSC, the address of the new MSC is given to MSC, and it contacts the new MSC. At the destination MSC, the VLR initiates a paging procedure in all BSSs under the control of the MSC holding the registration. After a reply from the MS, the VLR sends the necessary parameters to the MSC to establish the link to the MS.

7.3.3 Handoff

Handoff in the United States is referred to as handover in Europe and hence in GSM. The procedures for handoff broadly follow the procedures described in Chapter 6 that dealt with mobility management in general. There are two types of handover—internal and external. Internal handover is between BTSs that belong to the same BSS, and external handovers are between two different BSSs belonging to the same MSC. Sometimes there are handoffs between BSSs that are controlled by two different MSCs. In such a case, the old MSC continues to handle call management. Roaming between two MSCs in two different countries is prohibited, and the call simply drops.

Handoff is initiated because of a variety of reasons. Signal strength deterioration is the most common cause for handoff at the edge of a cell. Other reasons include traffic balancing where the handoff is network oriented to ease traffic congestion by moving calls in a highly congested cell to a lightly loaded cell. The handoff could be synchronous where the two cells involved are synchronized or it may be asynchronous. Because the MS does not have to resynchronize itself in the

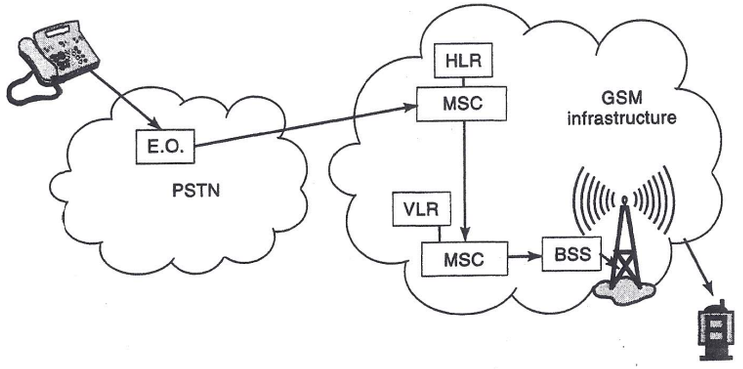

Figure 7.5 Mobile terminated call in a visiting network.

former scenario, the handoff delay is much smaller (100 ms against 200 ms in the asynchronous case).

Figure 7.6 shows the handoff procedure between two BSSs that are controlled by one MSC. The BTS provides the MS with a list of available channels in neighboring cells via the BCCH. The MS monitors the RSS from the BCCHs of these neighboring cells and reports these values to the MSC using the SACCH. This is called *mobile-assisted* handoff as discussed in Chapter 6. The BTS also monitors the RSS from the MS to make a handoff decision. Proprietary algorithms are used to decide when a handoff should be initiated. If a decision to make a handoff is made, the MSC negotiates a new channel with the new BSS and indicates to the MS that a handoff should be made using a handoff command. Upon completion of the handoff, the MS indicates this with a handoff complete message to the MSC.

7.3.4 Security

As discussed in Chapter 6, security in cellular systems is implemented to prevent fraud via authentication, avoid revealing the subscriber number over the air, and encrypt conversations where possible. All these are achieved using proprietary (secret) algorithms in GSM. The SIM cards discussed in Example 7.1 have a microprocessor chip that can perform the computations required for security purposes. A secret key K_i is stored on the SIM card, and it is unique to the card. This key is used in two algorithms—A3 and A8—that are used for authentication and confidentiality, respectively. For authentication purposes, the secret key K_i is used in a challenge response protocol using the A3 algorithm between the BSS and the MS. The secret key K_i is used to generate a privacy key K_c that is used to encrypt messages (voice or data) as the case may be using the A8 algorithm. The control channel signals are encrypted using a third encryption algorithm called A5. The size of the secret key K_i is 128 bits, and the response to the challenge is 32 bits long. Consequently, it is not very secure.

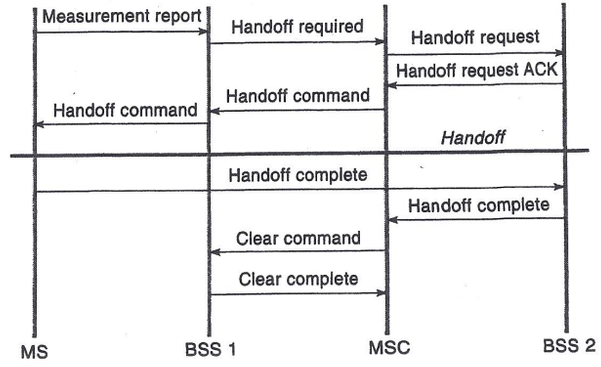

Figure 7.6 Handoff involving a single MSC and two BSSs.

Another aspect of security in GSM is that the secret key information is not shared between systems. Instead a triple consisting of the random number used in the challenge, the response to the challenge, and the data encryption key K_c is exchanged between the VLR and the HLR. The VLR verifies if the response generated by the MS is the same. The algorithms A8 and A3 are secret and not shared between different systems.

7.4 COMMUNICATIONS IN THE INFRASTRUCTURE

In the previous sections of this chapter, we introduced the GSM services and architectural elements, as well as an overview of the mechanisms that allows this architecture to support mobile operation. In this section we provide the description of how these elements and mechanisms are integrated with one another to implement the services. Elements of a network communicate with each other through a protocol stack that is specified by the standard committee. The GSM standard specifies the interfaces among all the elements of the architecture that was discussed earlier. Figure 7.7 shows the protocol architecture for communication between the main hardware elements and the associated interfaces.

The air-interface U_m, which specifies communication between the MS and BTS, is the most detailed and wireless related interface. The A-bis interface between the BTS and BSC and the A interface between BSC and MSC draw signifi-

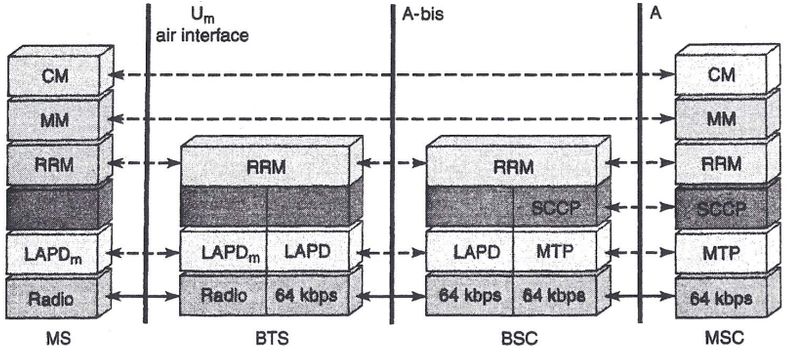

Figure 7.7 The GSM protocol architecture.

cantly on the existing ISDN protocols. The protocol stack is divided into three layers:

Layer 1: Physical Layer

Layer 2: Data Link Layer (DLL)

Layer 3: Networking or Messaging Layer

Messages between the BTS and BSC flow through the A-bis interface. The support on this interface is for voice traffic at 64 kbps and data/signaling traffic at 16 kbps. Both types of traffic are carried over LAPD (which is a data link protocol used in ISDN). The A-interface is used for message transfer between different BSCs to the MSC. The physical layer is a 2 Mbps CCITT connection and employs SS-7 protocols for communication. The Message Transport Protocol (MTP) and the Signaling Connection Control Part (SCCP) of SS-7 are used for error-free transport and logical connection, respectively. The applications that employ the SS-7 protocols deal with direct transfer of data and management (via the BSS application part—BSSAP) for radio resource handling and operation and maintenance information (via the BSS operation and maintenance application part—BSSOMAP) for the operation and maintenance communication messages.

In the following three sections, we cover more details of the three layers with specific examples to provide the readers with an understanding of how a GSM system operates to support different services.

7.4.1 Layer I: Physical Layer

The physical layer of the A and A-bis interfaces follow the ISDN standard with 64 kbps digital data per voice user. The new physical layer defined in the GSM specifications is for the U_m air-interface. This layer specifies how the information from different voice and data services are formatted into packets and sent through the radio channel. It specifies the radio modem details, structure of traffic and control packets in the air, and the packaging of a variety of services into the bits of a packet. This layer specifies modulation and coding techniques, power control methodology, and time synchronization approaches which enable establishment and maintenance of the channels.

7.4.1.1 Power and Power Control

As discussed in Chapter 6, power management is an important issue in wireless networks in general. Power management in cellular telephone networks helps the service provider to control the interference among the users and minimize the power consumption at the terminal. Therefore, power management has direct impact on QoS and the life of the batteries that are the extremely important to the users.

There are three major classes of mobile stations: vehicle mounted, portable, and handheld terminals. Mobile mounted uses the car battery, portables use larger rechargeable batteries, and handheld uses smaller rechargeable batteries. The antenna for the mobile is mounted outside the car, which is away from the user's body, whereas the antenna in the handheld terminals is next to the ear and brain of

the user which raises health concerns for high-radiated powers. GSM cells have radii ranging from 300 m to 35 km. The size of the cells also plays a role in the required transmitted power for the BTS and the MS. To allow manufacturers and service providers to accommodate the diversified requirements for different MS and BSS subsystems, a number of radiated power classes are identified by the GSM standard. There are five power classes for the mobile terminal from 29 dBm (0.8 W) up to 44 dBm (20 W) with a 4 dB separation between consecutive mobile classes. There are eight classes for the BTS power ranging from 34 dBm (2.5 W) up to 55 dBm (320 W) in 3-dB steps.

Transmitted radio frequency power in the MS is always controlled to its minimum required value to minimize the cochannel interference among different cells and maximize the life of the battery. The MS is allowed to reduce its peak output power down to 20 mW in 2 dB steps. The BSS calculates the power level for individual MSs by monitoring the interference and received signal strength and sends this information through control signaling packets to the MS.

7.4.1.2 Physical Packet Bursts

GSM uses 890–915 MHz for the uplink (reverse) and 935–960 MHz for the downlink (forward) channels. As shown in Figure 7.8, the 25 MHz band for each direction is divided into 124 channels, each occupying 200 kHz with 100 kHz guard band at two edges of the spectrum. Each carrier supports eight time slots for the TDMA operation. The data rate of each carrier is 270.833 kbps that is provided with a GMSK modem with a normalized bandwidth expansion factor of 0.3. With this data rate, the duration of each bit is 3.69 μsec. The user transmission packet burst is fixed at 577 μsec, which accommodates information bits and a time gap between the packets for duration equivalent to 156.25 times the bit duration of 3.69 μsec.

GSM supports four types of bursts for traffic and control signaling. Figure 7.9 shows all four bursts types. The *normal burst (NB),* shown in Figure 7.9a, consists of three tail bits (TBs) at the beginning and at the end of the packet, equivalent to 8.25 bits of gap period (GP), two sets of 58 bits encrypted bits (a total of 116 bits), and a 26-bits training sequence. The TBs are 3 zero bits providing a gap time for the digital radio circuitry to cover the uncertainty period to ramp on and off for the radiated power and to initiate the convolutional decoding of the data. The 26-bit

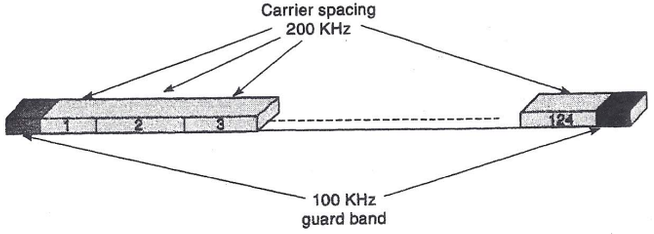

Figure 7.8 Frequency bands in GSM.

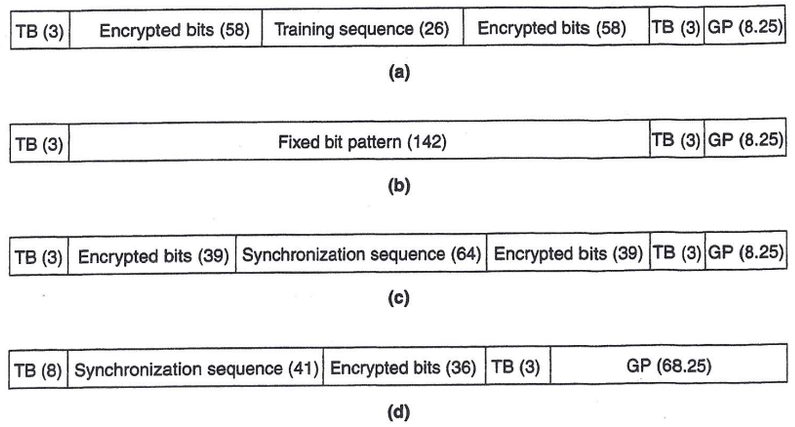

Figure 7.9 The four burst types in GSM: (a) normal burst, (b) frequency correction burst, (c) synchronization burst, and (d) random access burst.

training sequence is used to train the adaptive equalizer at the receiver. Because the channel behavior is constantly changing during the transmission of the packet, the most effective place for the training of the equalizer is in the middle of the burst. The 116 encrypted data bits include 114 bits of data and two flag bits at the end of each part of the data which indicates whether data is user traffic or signaling and control. The user traffic data arrives in frames of length 456 bits as shown in Figure 7.10. They are interleaved into the transmitted normal bursts in blocks of 57 bits plus one flag bit. The purpose of interleaving is to improve the performance for the users by distributing the effects of fade hits among several users. The 456 bits are produced every 20 ms. Therefore, the equivalent of 20 ms of arriving information is mapped into 456 bits. The standard specifies the method that maps the 20 ms of the traffic into the 456 bits.

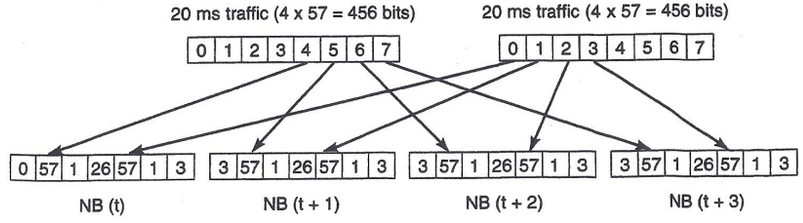

Figure 7.10 Interleaving traffic frames onto TDMA GSM frame in the air.

Example 7.9: Packets of Voice Traffic

Figure 7.11 shows how the 456-bit packets are formed from the speech signal. Each 20 ms of the coded speech at 13 kbps forms a 260-bit packet. The first 50 most significant bits receives a 3-bit CRC code protection first, and then they are added to the second group of 132 bits with lower importance and a 4-bit tail that is all zeros. The resulting 132 + 53 + 4 = 189 bits are then encoded with a ½ convolutional encoder that doubles number of bits to 378. The convolutional code provides for error correction capabilities. The 378 coded bits are added to the 78 least important speech-coded bits to form a 456 bits packet every 20 ms. The 456 bits packets are used to form normal transmission bursts shown in Figure 7.9. In this encoding scheme, we have three classes of speech coded bits. The first class of 50 bits receives both CRC error detection and the rate ½ convolutional error correcting coding protection. The second 132 bits receive only the convolutional encoding protection, and the last 78 bits receives no protection. Therefore, the speech coder can protect the more important bits representing larger values of voltages by assigning them into different categories.

Example 7.10: Packets of Data Traffic

Figure 7.12 shows the formation of the 456 bit packets for 9,600 bps data. The 192 bits of information are accompanied by 48 bits of signaling information and 4 tail bits to form a 244 bits packet that is then expanded to 456 bits using a ½ rate punctured convolutional encoder. Punctured coding can eliminate the need for doubling the number of transmitted bits by eliminating (puncturing) a certain number of bits [PRO01]. The resulting 456 bits are turned to NBs similar to the speech packets. The interesting point is that the 13 kbps speech coded signal and 9,600 bps data modem both occupy the same transmission resources on the air-interface. More channel coding bits are allocated to the data modem packets that are expected to provide better error rate performance.

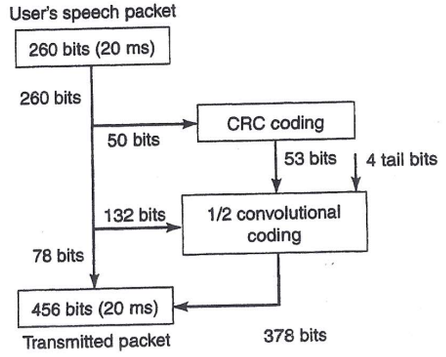

Figure 7.11 Coded speech packets in GSM.

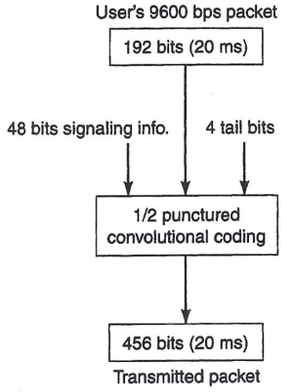

Figure 7.12 Coded data packets in GSM.

Example 7.11: Packets of Signaling Channel

In addition to the traffic channels, we need a number of signaling or control channels that are used to determine how the traffic packets should be routed in the network. Signaling channels using the NB as the channel over-the-air-interface (shown in Figure 7.13) use 184 signaling bits to convey the signaling message. These bits are first block coded with 40 additional parity check bits and 4 tail bits to form a 228-bits block. The 228-bits block is then coded with a ½ rate convolutional encoder to form a 456 bits packet occupying a 20 ms slot that is turned to a burst for transmission as shown in Figure 7.10.

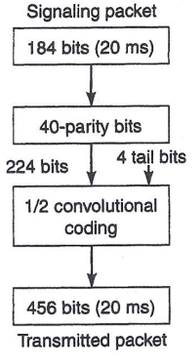

Figure 7.13 Coded signaling packets in GSM.

The other three types of bursts are more simple and designed for specific tasks. The simplest of all the remaining bursts is the *frequency-correction burst* (FB), shown in Figure 7.9(b). It has three TBs at the start and the end of the burst. The rest of the packet contains all zeros that allows simple transmission of the carrier frequency without any modulated information. An equivalent of 8.25-bits duration is used as the GP between this burst and others. The BS broadcasts FB, and MSs use it to synchronize with the master clock in the system. The *synchronization burst* (SB), shown in Figure 7.9(c), is very similar to the NB except that the training sequence is longer and the coded data are used for the specific task of identifying the network. The BTS broadcasts the SB, and the MSs use it for initial training of the equalizer, as well as initial learning of the network identity and to synchronize the time slots. The *random access burst* (RAB) is used by the MS to access the BS as it registers to the network. The overall structure is similar to NB except that a longer start-up and synchronization sequence is used to initiate the equalizer. Another major difference is the length of the much longer GP which allows rough calculation of the distance of the MS from the BTS. This calculation is possible from determining the arrival time of the RAB. A GP of 68.25 bits translates to 252 μsec. The signal transmitted from a MS should travel more than 75.5 km (at the speed of 300,000 km/sec) before arriving at the BTS to exceed this GP.

7.4.1.3 TDMA Frame Hierarchy

When a number of different slots carry the user traffic and a variety of control signals, a hierarchy is needed to identify the location of certain bursts among the large stream of bursts that are directed toward different terminals. Each terminal needs a number of counters to track the related packets at different levels of the hierarchy.

The GSM radio-interface standard provides a variety of traffic channels and control channels defined in a hierarchy built upon the basic eight-slot TDMA transmission format. The frame hierarchy, depicted in Figure 7.14, shows the TDMA hierarchy of the GSM network from a burst of 0.577 ms interval to a hyperframe of length of around 3.5 hours. The basic building block of the frame hierarchy is a 4.615-ms frame. Each frame comprises eight bursts or time slots. The time-slot interval is equivalent to the transmission time for about 156.25 bits, for which, as we saw in Figure 7.9, durations equivalent to 8.25 (68.25 for RAB) bit times are used as guard times during which no signal is transmitted. The next level in the hierarchy is a GSM multiframe, shown in Figure 7.14. Each 120-ms multiframe is composed of 26 frames, each containing eight time slots. In each multiframe, 24 frames carry user information, and two frames carry system control information related to individual users. The data rate per voice user is calculated by considering that for each 120 ms, 24 voice-bursts each carrying $2 \times 57 = 114$ bits of information are transmitted. Therefore, the data rate per user is $24 \times 114/0.120 = 22{,}800$ bits/s. The speech coder has a data rate of 13 kbps, and the addition of error-detection and error-correction coding brings the transmission rate up to 22.8 kbps.

Figure 7.14 shows that the eight-slot frames may be also organized into control multiframes rather than traffic multiframes. Control multiframes are used to establish several types of signaling and control channels used for system access, call setup, synchronization, and other system control functions. Either traffic or

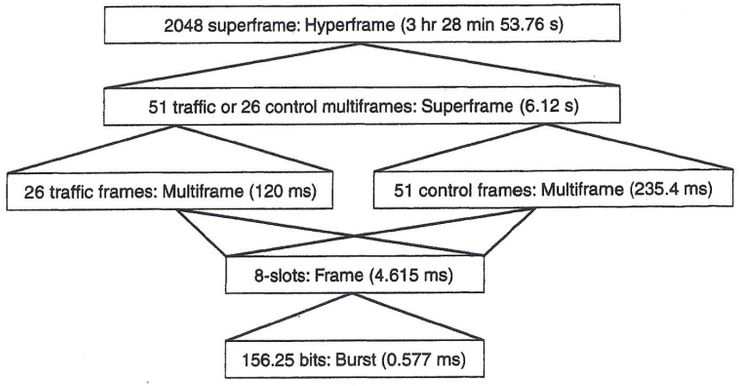

Figure 7.14 Frame hierarchy in GSM.

control-multiframes are grouped into superframes, which are in turn grouped into hyperframes. Counters at the terminals need to track the packet numbers at hyperframe, superframe, and mutiframe levels to communicate with the network.

Example 7.12: Counting Frames in GSM

The counter for multiframes in the mobile terminal needs to keep track of the traffic channel for the terminal. Another counter needs to track the traffic superframe to identify the location of the two control frames. A variety of control signaling information embedded in the control superframe is extracted from its appropriate location using the counter for those frames.

7.4.1.4 Logical Channels

In the last few sections, we described how traffic and control packets are inserted in a hierarchy and how terminals use counters to identify the location of specific packet bursts in the overall structure of the frames. Communication between the terminal and the BS is involved with both information traffic, as well as signaling and control. The entire communication system can be thought of as a distributed real-time computer that uses a number of instructions to transfer information packets from one location to another. We have several major tasks to make such a system work. We need initial signaling for registration and call establishment; we need to maintain the synchronization among the terminals; we need to manage mobility; and we need to transfer the data traffic. In a manner similar to computers, we need a set of instructions and ports to instruct different elements of the network to perform their specified duties. In telecommunication systems these ports are referred to as logical channels. Logical channels use a physical TDMA slot or a portion of a physical slot to specify an operation in the network.

To describe logical channels in the GSM network, we first divide these channels into two principal categories: *traffic channels* (TCHs) and *control channels* (CCHs). Traffic channels are two-way channels carrying the voice and data traffic between the MS and BTS. TCH logical channels are implemented over the NB physical bursts shown in Figure 7.9(a). There are two types of TCH channels:

- The *full-rate traffic channel* (TCH/F) uses a 13 kbps speech-coding scheme and 9,600 bps, 4,800 bps, and 2,400 bps data. Figures 7.11 and 7.12 show the procedures to create the frames for 13 kbps speech and 9,600 bps data, respectively. As we saw earlier, when we include signaling overhead each channel has a gross bit rate of 22.8 kbps for the network.
- The *half-rate traffic channel* (TCH/H): GSM also supports half-rate speech coding traffic channels. The TCH/H channel uses 16 slots per frame that has a gross bit rate of 11.4 kbps. The half-rate TCH supports 4.8 kbps and 2.4 kbps data.

There are three classes of control channels: *broadcast channels* (BCH), *common control channels* (CCCH), and *dedicated control channels* (DCCH). The BCH channels are broadcast from the BTS to MSs in the coverage area of the BTS. There are three broadcast channels:

- The *frequency control channel* (FCCH) used by the BTS broadcasts carrier synchronization signals. An MS in the coverage area of a BTS uses the broadcast FCCH to synchronize its carrier frequency and bit timing. The physical FCB shown in Figure 7.9(b) is used to implement the logical FCCH.
- The *synchronization channel* (SCH) used by the BTS to broadcast frame synchronization signals to all MSs. Using SCH, MSs will synchronize their counters to specify the location of arriving packets in the TDMA hierarchy. The physical SBs shown in Figure 7.9(c) are used to implement SCH.
- The *broadcast control channel* (BCCH) is used by BTS to broadcast synchronization parameters, available services, and cell ID. Once the carrier, bit, and frame synchronization between the BTS and MS are established, the BCCH informs the MS about the environment parameters associated with the BTS covering that area. The BCCH is physically implemented over the NBs. The BCCH is also a continuously keyed channel, and it is used for signal strength measurements for handoff.

The CCCH channels are also one-way channels used for call establishment. There are three CCCH logical channels:

- The *paging channel* (PCH) is used by the BTS to page the MS for an incoming call is a broadcast channel implemented on a NB.
- The *random access channel* (RCH) is used by the MS to access the BTS for call establishment. The RCH is used for implementation of a slotted-ALOHA protocol, which is used by mobile stations to contend for one of the available slots in the GSM traffic frames. The RCH is implemented on the short RABs shown in Figure 7.9(d).
- The *access grant channel* (AGCH) is used for implementation of the acknowledgement from the BTS to the MS after a successful attempt by MS using RCH. This channel is implemented on an NB and indicates the TCH for access to the GSM network.

The DCCH are two-way channels supporting signaling and control for individual users. There are three DCCH logical channels:

- The *stand-alone dedicated control channel* (SDCCH) is a two-way channel assigned to each terminal to transfer network control information for call establishment and mobility management. The physical channel for SDCCH occupies four slots in every 51 control-multiframes with an approximated gross data rate of 2 kbps per terminal.
- The *slow associated control channel* (SACCH) is a two-way channel assigned to each TCH and SDCCH channels. The SACCH is used to exchange the necessary parameters between the BTS and the MS to maintain the link. The gross data rate of the SACCH channel is half of that of the SDCCH.
- The *fast associated control channel* (FACCH) is a two-way channel used to support fast transitions in the channel when SACCH is not adequate. The FACCH is physically multiplexed with the TCH or SDCCH to provide additional support to the SACCH.

A more detailed description of the logical channels and GSM operation is available in [GOO97], [RED95]. At this stage we provide an example of using logical channels to implement an operation in a GSM network.

Example 7.13: Logical Channels Used for Call Establishment

Figure 7.15, which is similar to Figure 7.4, represents the 15 steps for mobile initiated call establishment procedure. In Figure 7.15 the logical channel used for each step is also identified. Call establishment is made through the common control RACH and AGCH. Calling number and security is through the dedicated SDCCH, signaling for connection status through dedicated FACCH and traffic exchange through TCH.

7.4.2 Layer II: Data Link Layer

Any connection-based network can be considered to be two networks: one used for traffic and the other for signaling and control. The signaling and control may be through the same physical channels or through separate physical channels. In traffic channels for GSM, as we saw in Figures 7.11 and 7.12, the information bits are encoded with strong error detection and correction codes to form packets of length 456 that are then sent with four normal bursts. Signaling and control data are conveyed through Layer II and Layer III messages. The overall purpose of DLL

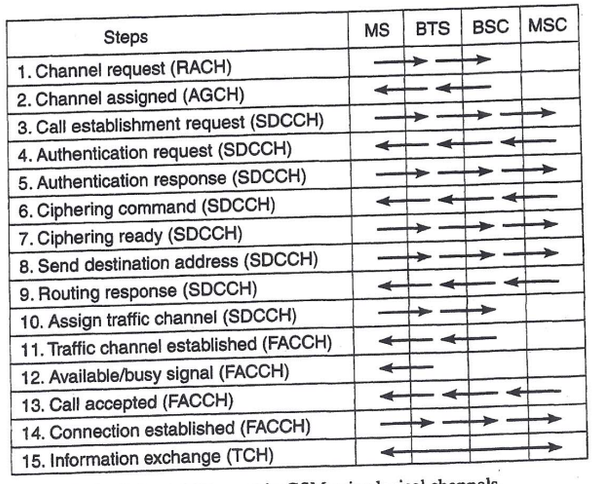

Figure 7.15 Call establishment in GSM using logical channels.

(Layer II) is to check the flow of packets for Layer III and allow multiple service access points (SAP) with one physical layer. In GSM the DLL checks the address and sequence number for Layer III and manages acknowledgments for transmission of the packets. In addition, the DLL allows two SAPs for signaling and short messages (SMS). Unlike other GSM data services that are carried through traffic channels, the SMS traffic channel in the GSM is not communicated through traffic channels. In GSM, the SMS is transmitted through a fake signaling packet that carries user information over signaling channels. The DLL in GSM provides this mechanism for multiplexing the SMS data into signaling streams.

As we saw in Figure 7.13, signaling packets delivered to the physical layer are each 184 bits, this number conforming with the length of the DLL packets in the LAPD protocol used in the ISDN networks. In fact, as shown in Figure 7.7, the LAPD protocol is used for the A and A-bis interfaces connecting the BTS to BSS and BSS to MSC, respectively. The DLL for the U_m air-interface is LAPDm where m refers to the modified version of LAPD adapted to the mobile environment. The length of the LAPDm packets, shown in Figure 7.16, is the same as LAPD, but the format is slightly adjusted to fit the mobile environment. The synchronization bits

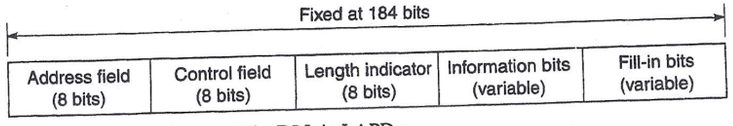

Figure 7.16 Frame format of the DLL in LAPDm.

and CRC codes in LAPD are eliminated in the LAPDm because GSM has the time synchronization and strong coding at the physical layer. The address field is optional, and it identifies the SAP, protocol revision type, and nature of the message. The control field is optional, and it holds the type of the frame (command or response) and the transmitted and received sequence numbers. The length indicator identifies the length of the information field. The information field carries the Layer III payload. Fill-in bits are all "1" bits to extend the length to the desired 184 bits. In peer-to-peer Layer II communications, such as DLL acknowledgments, there is no Layer III payload and fill-in bits cover this field.

The pure or peer-to-peer Layer II messages are set asynchronous balanced mode, disconnect, unnumbered acknowledgment, receiver ready, receiver not ready, and reject. These messages do not have Layer III information bits and are referred to as Layer II messages. The information bits in Layer II packets specify Layer III operations implemented on the logical signaling channels. These information bits are different for different operations.

Example 7.14: Information Field in Layer II Packets

The PCH, AGCH, and BCCH are each 176 bits. The DLL packets for these signaling channels only have an eight bit length of the field that makes a total length of 184 bits encoded into 456 bits transmitted over four physical NBs. The SDCCH and FACCH are each 160 bits with three 8-bits used for address, control, and length of the information fields. The SACCH has 144 bits that needs 16 fill-in bits in addition to the other three fields each carrying 8 bits.

7.4.3 Layer III: Networking Layer

As we discussed in Section 7.3, there are a number of mechanisms needed to establish, maintain, and terminate a mobile communication session. The networking or signaling layer implements the protocols needed to support these mechanisms. The networking layer in GSM is also responsible for control functions for supplementary and SMS services. The traffic channels, as we saw earlier, are mapped into the TCH and carried by normal bursts in different formats associated with different speech or data services. The signaling information uses other bursts and more complicated DLL packaging. A signaling procedure or mechanism or protocol, such as the registration process shown in Figure 7.3, is composed of a sequence of communication events or *messages* between hardware elements of the systems that are implemented on the logical channels encapsulated in the DLL frames illustrated in the last example of the last section. Layer III defines the details of implementation of messages on the logical channels encapsulated in DLL frames. Among all messages communicated between two elements of the network only a few, such as DLL acknowledgment, do not carry Layer III information.

Example 7.15: Format of Layer II and Layer III Messages

Figure 7.17 shows the typical format of Layer II and Layer III messages in a procedure between two elements of the network. They start with simple pure Layer II messages without Layer III information bits to initiate a procedure. Then a number

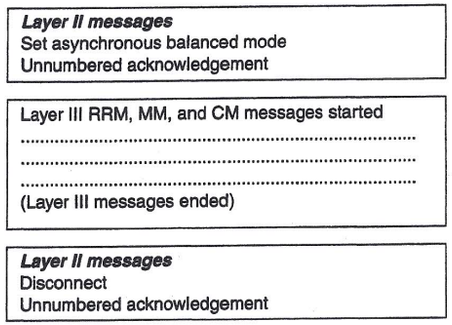

Figure 7.17 Typical format of the messages in a procedure used for implementation of a network operation mechanism.

of Layer II messages with Layer III information follow to complete the necessary operation for the procedure. At the end, a couple of pure Layer II messages disconnect the session between the two elements.

Information bits of the Layer II packets, shown in Figure 7.17, specify the operation of a Layer III message. As shown in Figure 7.18, these bits are further divided into several fields. The transaction identifier (TI) field is used to identify a procedure or protocol that consists of a sequence of messages. This field allows multiple procedures to operate in parallel. The protocol discriminator (PD) identifies the category of the operation (management, supplementary services, call control, and test procedure). The message type (MT) identifies the type of message for a given PD. Information elements (IE) is an optional field for the time that an instruction carries some information that is specified by an IE identifier (IEI).

The number of Layer III messages is much larger than the number of pure Layer II messages. To further simplify the description of the Layer III messages, GSM standard divides the messages into three subcategories or sublayers: Radio Resource Management (RRM), Mobility Management (MM), and Connection Management (CM) messages.

The RRM sublayer of Layer III manages the frequency of operation and the quality of the radio link. This sublayer does not have an equivalent in wired networks because there is no frequency assignment issue in the wired networks. The main responsibilities of the RRM are to assign the radio channel and hop to new channels in

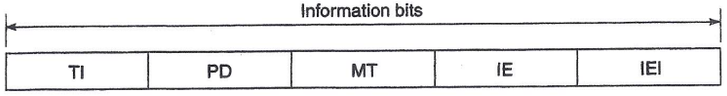

Figure 7.18 The typical Layer III message format.

implementation of the slow frequency hopping option, to manage handover procedure and measurement reports from MS for handover decision, to implement power control procedure, and to adapt to timing advance for synchronization.

The MM sublayer handles mobility issues that are not directly related to the radio. Major responsibilities of this sublayer are location update, authentication procedure, TMSI handling, and attachment and detachment procedures for the IMSI. The CM sublayer establishes, maintains, and releases the circuit-switched connection and helps in SMS. Specific procedures for the CM sublayer are mobile-originated and -terminated call establishment, change of transmission mode during the call, control of dialing using dual-tones, and call reestablishment after MM interruption

An explanation of the details of coding of each message and a complete list of the GSM messages are beyond the scope of this book. For the complete list of the messages used in Layer III of the GSM, the reader can refer to [GOO97], and for further detail of the operation to [RED95] or [GAR99]. We complete this section with an example of a procedure and division of the taskes among different sublayers.

Example 7.16: Call Establishment

Figure 7.19 shows the 15-step mobile initiated call establishment procedure that was discussed earlier in Figures 7.15 and 7.5. The first column identifies the message. The second column identifies the logical channel that is used to carry the message. The third column identifies the sublayer of the Layer III in which GSM standard describes the message. Note that Layer III does not handle the traffic message, and therefore we have no sublayer association for that part of the procedure.

Message name	Logical channel	Category
1. Channel request	RACH	RRM
2. Immediate assignment	AGCH	RRM
3. Call establishment request	SDCCH	CM
4. Authentication request	SDCCH	MM
5. Authentication response	SDCCH	MM
6. Ciphering command	SDCCH	RRM
7. Ciphering ready	SDCCH	RRM
8. Send destination address	SDCCH	CM
9. Routing response	SDCCH	CM
10. Assign traffic channel	SDCCH	RRM
11. Traffic channel established	FACCH	RRM
12. Available/busy signal	FACCH	CM
13. Call accepted	FACCH	CM
14. Connection established	FACCH	CM
15. Information exchange	TCH	

Figure 7.19 Layer III sublayer categories for mobile-assisted call establishment

QUESTIONS

7.1 What are the differences between a mobile digital telephone and POTS?
7.2 Name the three subsystems in the GSM architecture.
7.3 Name the three types of services provided by GSM.
7.4 What is the importance of the framing structure in GSM?
7.5 What are the data services provided by GSM?
7.6 What are the incentives for power control in a TDMA network? Name the elements of the GSM system that are involved in handling power control.
7.7 What are VLR and HLR, where they are physically located, and why we need them?
7.8 What is the difference between registration and call establishment?
7.9 What are the reasons to perform handoff?
7.10 What is the difference between network-decided and mobile-assisted handovers?
7.11 What is the difference between a logical and physical channel?
7.12 Name the five most important logical channels in GSM.
7.13 How does GSM convert 456 bits of the speech, data, or control signal into a normal burst of 156.25 bits?

PROBLEMS

7.1 a. Using the bit and time durations in Figure 7.11, show that the speech coding rate for GSM is 13 kbps and the effective transmission rate to support one 13 kbps coded voice channel is 22.8 kbps.

b. What is the required transmission bandwidth for eight slots of the GSM system?

c. Give the overall overhead rate of the system; that is, the difference between the required transmission rate for the traffic and the actual transmission rate of the GSM.

d. Determine the efficiency of the system that is the ratio of the overhead over raw transmission rate.

7.2 a. Consider the multiframe transmission in GSM depicted in Figure 7.14. Use the overall structure of the multiframe, frame, and slot to show that the transmission rate of the GSM is indeed 270.833 kbps.

b. In each GSM multiframe 24 frames are used for traffic and two for associated control signaling. Considering the detailed burst frame and multiframe infrastructure, show that the effective transmission rate for each GSM voice traffic is 22.8 kbps.

c. The slow association control channel uses 114 bits of one slot of each 26-slot traffic multiframe. What is the transmission rate for this channel in bits per second?

7.3 The stand-alone dedicated control channel (SDCCH) uses four time slots per each 51-control multiframe shown in Figure 7.14. Use the superframe timing to determine the effective data rate of this logical channel.

7.4 Considering Figure 7.12 give the net data rate (data plus signaling) and the effective transmission rate of a 9,600 bps GSM data service.

7.5 a. Considering the frequency allocation strategy of Fig 7.8 for the GSM systems, give the total number of traffic channels per 50 MHz of bandwidth used for two-way GSM communications.

b. Give the total number of GSM channel per MHz of bandwidth.

c. Give the number of channels per cell for frequency reuse factors of N = 4 and N = 3.

7.6 Repeat Problem 7.5 for the IS-136 assuming that this system replaces an AMPS system with 395 traffic channel and a frequency reuse factor of $N = 7$.

7.7 a. What is the allowable power ramping time for GSM receivers? (*Hint:* The time gaps of normal, frequency correction, and synchronization bursts, shown in Figure 7.9, are designed to allow power ramping.)

b. The time gap of the random access burst, shown in Fig. 7.9, is designed to assure this packet does not collide with the normal bursts. What is the maximum coverage, the distance between the BS and MS of a GSM base station? Assume that this gap is reserved for two-way travel and radio wave travel at 300,000 Km/sec.

c. The length of the synchronization sequence in synchronization burst is designed to allow time advance for two-way bit synchronization. Use this parameter to calculate the maximum coverage of GSM. Compare your results with that of part (b).

Acronyms and Abbreviations

π/4-DQPSK π/4 differential quadrature phase shift keying
1G First generation cellular
2G Second generation cellular
3G Third generation cellular
AAL ATM adaptation layer
ACF Association control function
ACH Access feedback channel
ACI Adjacent channel interference
ACTS Advanced communications technologies and services
ADPCM Adaptive differential pulse code modulation
AGCH Access grant channel
ALI Automatic location information
AM Amplitude modulation
AMPS Advanced mobile phone system
ANSI American National Standards Institute
AOA Angle of arrival
AP Access point
ARIB Association of Radio Industries and Businesses
ARN Authentication random number
ARP Address resolution protocol
ARQ Automatic repeat request
ASCH Association control channel
ASK Amplitude shift keying
ASN Authentication sequence number
ATM Asynchronous transfer mode
AuC Authentication center
AWGN Additive white Gaussian noise
BCCH Broadcast control channel
BCH Broadcast channel
BER Bit error rate
BG Border gateway
BLER Block error rate

BRAN Broadband radio access networks
BS Base station
BSA Basic service area
BSC Base station controller
BSIC Base station identity code
BSS Basic service set
BSS Base station subsystem
BSSGP BSS gateway protocol
BTMA Busy tone multiple access
BTS Base transceiver subsystem
CCA Clear channel assignment
CCH Control channel
CCI Co-channel interference
CCITT International Telegraph and Telephone Consultative Committee
CCK Complementary code keying
CDMA Code division multiple access
CDPD Cellular digital packet data
CELP Code excited linear prediction
CEPT Committee of European Post and Telecommunications
CFP Contention free period
CLI Calling line identification
CLNP Connectionless network protocol
CN Correspondent node
COA Care of address
COFDM Coded orthogonal frequency division multiplexing
CONS Connection oriented
COST Co-operative for scientific and technical research
CPC Centralized power control
CSMA/CA Carrier sense multiple access with collision avoidance
CSMA/CD Carrier sense multiple access with collision detection
CT Cordless telephony
CW Contention window
DAB Digital audio broadcast
DBPSK Differential binary phase shift keying
DCA Dynamic channel allocation
DCC DLC connection control
DCF Distributed coordination function
DDCA Distributed dynamic channel assignment
DDP Dominant direct path
DECT Digital enhanced cordless telephone
DES Data encryption standard
DFE Decision feedback equalizer
DFIR Diffused IR

DFS Dynamic frequency selection
DGPS Differential GPS
DIFS DCF inter-frame spacing
DL Discrete logarithm
DLC Data link control
DLL Data link layer
DLOS Direct line of sight
DPC Distributed power control
DQPSK Differential quadrature phase shift keying
DSL Digital subscriber line
DSMA Digital sense multiple access
DSS Digital signature standard
DSSS Direct sequence spread spectrum
DVCC Digital verification color code
EDGE Enhanced data rates for global evolution
EFR Enhanced full rate
EIR Equipment identity register
EOTD Enhanced observed time difference
ESS Extended service set
ETACS Enhanced total access communications system
ETSI European Telecommunications Standards Institute
EU European Union
FA Foreign agent
FACCH Fast associated control channel
FCA Fixed channel allocation
FCC Federal communications commission
FCH Frequency correction channel
FCS Frame correction sequence
FDD Frequency division duplexing
FDMA Frequency division multiple access
FER Frame error rate
F-ES Fixed end system
FFT Fast Fourier transform
FHSS Frequency hopping spread spectrum
FM Frequency modulation
FSK Frequency shift keying
FT Fixed terminal
FTP File transfer protocol
GBS Geolocation base station
GFSK Gaussian frequency shift keying
GGSN Gateway GPRS support node
GIS Geographic information system
GMSC Gateway MSC