


Martin Sauter

# Communication Systems

for the Mobile Information Society

Companion Website

 **WILEY**

# Contents

<b>Preface</b>	
<b>List of Figures</b>	<b>xi</b>
<b>List of Tables</b>	<b>xiii</b>
<b>List of Abbreviations</b>	<b>xix</b>
<b>1 Global System for Mobile Communications (GSM)</b>	<b>xxi</b>
1.1 Circuit-Switched Data Transmission	1
1.2 Standards	1
1.3 Transmission Speeds	3
1.4 The Signaling System Number 7	4
1.4.1 <i>The SS-7 Protocol Stack</i>	5
1.4.2 <i>SS-7 Protocols for GSM</i>	5
1.5 The GSM Subsystems	8
1.6 The Network Subsystem	9
1.6.1 <i>The Mobile Switching Center (MSC)</i>	9
1.6.2 <i>The Visitor Location Register (VLR)</i>	9
1.6.3 <i>The Home Location Register (HLR)</i>	12
1.6.4 <i>The Authentication Center</i>	13
1.6.5 <i>The Short Messaging Service Center (SMSC)</i>	17
1.7 The Base Station Subsystem (BSS)	19
1.7.1 <i>Frequency Bands</i>	20
1.7.2 <i>The Base Transceiver Station (BTS)</i>	21
1.7.3 <i>The GSM Air Interface</i>	22
1.7.4 <i>The Base Station Controller (BSC)</i>	24
1.7.5 <i>The TRAU for Voice Data Transmission</i>	30
Mobility Management and Call Control	35
1.8.1 <i>Location Area and Location Area Update</i>	44
1.8.2 <i>The Mobile Terminated Call</i>	45
	46



vi	51
	54
	59
1.9 The Mobile Station	62
1.10 The SIM Card	62
1.11 The Intelligent Network Subsystem and CAMEL	65
1.12 Questions	65
References	66
<b>2 General Packet Radio Service (GPRS)</b>	68
2.1 Circuit-Switched Data Transmission over GSM	68
2.2 Packet-Switched Data Transmission over GPRS	69
2.2.1 GPRS and the IP Protocol	69
2.2.2 GPRS vs. Fixed-Line Data Transmission	71
2.3 The GPRS Air Interface	72
2.3.1 GPRS vs. GSM Timeslot Usage on the Air Interface	73
2.3.2 Mixed GSM/GPRS Timeslot Usage in a Base Station	77
2.3.3 Coding Schemes	77
2.3.4 Enhanced Data Rates for GSM Evolution (EDGE) – EGPRS	79
2.3.5 Mobile Station Classes	81
2.3.6 Network Mode of Operation	84
2.3.7 GPRS Logical Channels on the Air Interface	84
2.4 The GPRS State Model	86
2.5 GPRS Network Elements	88
2.5.1 The Packet Control Unit (PCU)	89
2.5.2 The Serving GPRS Support Node (SGSN)	93
2.5.3 The Gateway GPRS Support Node (GGSN)	98
2.6 GPRS Radio Resource Management	98
2.7 GPRS Interfaces	98
2.8 GPRS Mobility Management and Session Management (GMM/SM)	101
2.8.1 Mobility Management Tasks	103
2.8.2 GPRS Session Management	106
2.9 Session Management from a User Point of View	111
2.10 WAP over GPRS	116
2.11 The Multimedia Messaging Service (MMS) over GPRS	116
2.12 Web Browsing via GPRS	119
2.12.1 Impact of Delay on the Web Browsing Experience	119
2.12.2 Web Browser Optimization for Mobile Web Browsing	120
2.13 Questions	121
References	121
<b>3 Universal Mobile Telecommunications System (UMTS)</b>	123
3.1 Overview, History, and Future	126
3.1.1 UMTS Release 99: A New Radio Access Network	127
3.1.2 UMTS Release 4: Enhancements for the Circuit-Switched Core Network	129
3.1.3 UMTS Release 5: Introduction of the IP Multimedia Subsystem (IMS)	129
3.1.4 UMTS Release 5: High Speed Downlink Packet Access (HSDPA)	129
3.1.5 UMTS Release 6: High Speed Uplink Packet Access (HSUPA)	129
3.1.6 UMTS Release 7 and Beyond: Even Higher Data Rates	129

3.2	Important New Concepts of UMTS	130
3.2.1	The Radio Access Bearer (RAB)	130
3.2.2	The Access Stratum and Non-Access Stratum	130
3.2.3	Common Transport Protocols for CS and PS	131
3.3	Code Division Multiple Access (CDMA)	132
3.3.1	Spreading Factor, Chip Rate, and Process Gain	136
3.3.2	The OVSF Code Tree	137
3.3.3	Scrambling in the Uplink and Downlink Directions	138
3.3.4	UMTS Frequency and Cell Planning	139
3.3.5	The Near-Far Effect and Cell Breathing	140
3.3.6	Advantages of the UMTS Radio Network Compared to GSM	142
3.4	UMTS Channel Structure on the Air Interface	144
3.4.1	User Plane and Control Plane	144
3.4.2	Common and Dedicated Channels	144
3.4.3	Logical, Transport, and Physical Channels	145
3.4.4	Example: Network Search	149
3.4.5	Example: Initial Network Access Procedure	151
3.4.6	The Uu Protocol Stack	153
3.5	The UMTS Terrestrial Radio Access Network (UTRAN)	158
3.5.1	Node-B, Iub Interface, NBAP, and FP	158
3.5.2	The RNC, Iu, Iub, and Iur Interfaces, RANAP and RNSAP	159
3.5.3	Adaptive Multi Rate (AMR) Codec for Voice Calls	164
3.5.4	Radio Resource Control (RRC) States	165
3.6	Core Network Mobility Management	170
3.7	Radio Network Mobility Management	171
3.7.1	Mobility Management in the Cell-DCH State	171
3.7.2	Mobility Management in Idle State	179
3.7.3	Mobility Management in Other States	181
3.8	UMTS CS and PS Call Establishment	183
3.9	UMTS Release 99 Performance	186
3.9.1	Data Rates, Delay, and Applications	186
3.9.2	Radio Resource Management Example	187
3.9.3	UMTS Web Browsing Experience	190
3.9.4	Number of Simultaneous Users per Cell	191
3.10	UMTS Release 5: High-Speed Downlink Packet Access (HSDPA)	193
3.10.1	HSDPA Channels	194
3.10.2	Shorter Delay Times and Hybrid ARQ (HARQ)	195
3.10.3	Node-B Scheduling	198
3.10.4	Adaptive Modulation, Coding, and Transmission Rates	198
3.10.5	Establishment and Release of an HSDPA Connection	200
3.10.6	HSDPA Mobility Management	201
3.11	UMTS Release 6: High-Speed Uplink Packet Access (HSUPA)	202
3.11.1	E-DCH Channel Structure	204
3.11.2	The E-DCH Protocol Stack and Functionality	207
3.11.3	E-DCH Scheduling	208



3.11.4	<i>E-DCH Mobility</i>	222
3.11.5	<i>E-DCH Terminals</i>	223
3.12	<i>UMTS and CDMA2000</i>	223
3.13	<i>Questions</i>	223
	<i>References</i>	223
<b>4</b>	<b>Wireless Local Area Network (WLAN)</b>	227
4.1	<i>Wireless LAN Overview</i>	227
4.2	<i>Transmission Speeds and Standards</i>	228
4.3	<i>WLAN Configurations: From Ad-hoc to Wireless Bridging</i>	229
4.3.1	<i>Ad-hoc, BSS, ESS, and Wireless Bridging</i>	229
4.3.2	<i>SSID and Frequency Selection</i>	230
4.4	<i>Management Operations</i>	232
4.5	<i>The MAC Layer</i>	232
4.5.1	<i>Air Interface Access Control</i>	232
4.5.2	<i>The MAC Header</i>	233
4.6	<i>The Physical Layer</i>	233
4.6.1	<i>IEEE 802.11b – 11 Mbit/s</i>	233
4.6.2	<i>IEEE 802.11g with up to 54 Mbit/s</i>	234
4.6.3	<i>IEEE 802.11a with up to 54 Mbit/s</i>	234
4.7	<i>WLAN Security</i>	240
4.7.1	<i>Wired Equivalent Privacy (WEP)</i>	240
4.7.2	<i>Wireless Protected Access (WPA), WPA2, and 802.11i</i>	242
4.8	<i>Comparison of WLAN and UMTS</i>	243
4.9	<i>Questions</i>	247
	<i>References</i>	247
<b>5</b>	<b>802.16 and WiMAX</b>	249
5.1	<i>Overview</i>	250
5.2	<i>Standards, Evolution, and Profiles</i>	252
5.3	<i>WiMAX PHYs for Point-to-Multipoint FDD or TDD Operation</i>	253
5.3.1	<i>Adaptive OFDM Modulation and Coding</i>	254
5.3.2	<i>Physical Layer Speed Calculations</i>	257
5.3.3	<i>Cell Sizes</i>	258
5.4	<i>Physical Layer Framing</i>	260
5.4.1	<i>Frame Structure in FDD Mode for Point-to-Multipoint Networks</i>	260
5.4.2	<i>Frame Structure in TDD Mode for Point-to-Multipoint Networks</i>	264
5.5	<i>Ensuring Quality of Service</i>	264
5.6	<i>MAC Management Functions</i>	269
5.6.1	<i>Connecting to the Network</i>	269
5.6.2	<i>Power, Modulation, and Coding Control</i>	273
5.6.3	<i>Dynamic Frequency Selection</i>	274
5.7	<i>MAC Management of User Data</i>	274
5.7.1	<i>Fragmentation and Packing</i>	275
5.7.2	<i>Data Retransmission (ARQ)</i>	276
5.7.3	<i>Header Compression</i>	278

5.8	Security	
5.8.1	Authentication	279
5.8.2	Ciphering	279
5.9	Advanced 802.16 Functionalities	281
5.9.1	Mesh Network Topology	282
5.9.2	Adaptive Antenna Systems	282
5.10	Mobile WiMAX: 802.16e	284
5.10.1	OFDM Multiple Access for 802.16e Networks	286
5.10.2	MIMO	286
5.10.3	Handover	288
5.10.4	Power-Saving Functionality	289
5.10.5	Idle Mode	292
5.11	WiMAX Network Infrastructure	293
5.11.1	Network Reference Architecture	294
5.11.2	Micro Mobility Management	295
5.11.3	Macro Mobility Management	297
5.12	Comparison of 802.16 with UMTS, HSDPA, and WLAN	298
5.13	Questions	300
	References	301
<b>6</b>	<b>Bluetooth</b>	<b>303</b>
6.1	Overview and Applications	303
6.2	Physical Properties	304
6.3	Piconets and the Master/Slave Concept	307
6.4	The Bluetooth Protocol Stack	309
6.4.1	The Baseband Layer	310
6.4.2	The Link Controller	315
6.4.3	The Link Manager	317
6.4.4	The HCI Interface	319
6.4.5	The L2CAP Layer	321
6.4.6	The Service Discovery Protocol	323
6.4.7	The RFCOMM Layer	324
6.4.8	Bluetooth Connection Establishment Overview	326
6.5	Bluetooth Security	327
6.5.1	Pairing	327
6.5.2	Authentication	328
6.5.3	Encryption	329
6.5.4	Authorization	330
6.5.5	Security Modes	331
6.6	Bluetooth Profiles	331
6.6.1	Basic Profiles: GAP, SDP, and the Serial Profile	333
6.6.2	The Network Profiles: DUN, LAP, and PAN	334
6.6.3	Object Exchange Profiles: FTP, Object Push, and Synchronize	337
6.6.4	Headset, Hands-Free, and SIM Access Profile	340
6.6.5	High-Quality Audio Streaming	344



# Preface

Wireless technologies such as GSM/UMTS, wireless LAN, 802.16 (WiMAX), and Bluetooth have revolutionized the way we communicate and exchange data by making services like telephony and Internet access available at anytime and from almost anywhere. Today, a great variety of technical publications offer background information about these technologies but they all fall short in one way or another. Books covering these technologies usually describe only one of the systems in detail and are generally too complex as a first introduction. The Internet is also a good source, but the articles one finds are usually too short and superficial or only deal with a specific mechanism of one of the systems. Because of this, it was difficult for me to recommend a single publication to students in my telecommunication classes, which I've been teaching in addition to my chosen profession as a wireless systems consultant. This book aims to change this.

All wireless technologies discussed in the book continue to evolve, with increasing transmission speeds being the driving goal. This book covers some of the evolutions such as HSDPA and HSUPA enhancements, which deliver increased transmission speeds in UMTS networks, and EDGE, which does the same thing for GPRS. As WiMAX already offers high transmission speeds for stationary users (802.16d), the evolution path of this system introduces mobility. Therefore, the mobility extension of WiMAX (802.16e) is also discussed.

Beyond speed and mobility improvements, research is being performed into how future multi-mode wireless devices can offer anytime, anywhere connectivity. The challenge of this approach is determining how to offer a seamless transition from one radio technology to another for users roaming out of the coverage area of a network. As this book describes the similarities and differences between the major radio technologies, which will form the basis of such 4G networks, it also provides a wealth of information for readers involved in this area of research.

Each of the six chapters in this book gives a detailed introduction and overview of one of the wireless systems mentioned above. Special emphasis has also been put into explaining the thoughts and reasoning behind the development of each system. Not only the 'how', but also the 'why' is of central importance in each chapter. Furthermore, comparisons are made between the different technologies to show the differences and commonalities of the systems. For some applications, several technologies compete directly with each other, while in other cases only a combination of different wireless technologies creates a practical application for the end user. For readers who want to test their understanding of a system, each chapter concludes with a list of questions. For further investigation, all chapters contain references to the relevant standards and other documents. These provide an ideal additional source to find out more about a specific system or topic.