

Communication Systems for the Mobile Information Society

Martin Sauter

Nortel Networks, Germany



John Wiley & Sons, Ltd

Contents

Preface	xi
List of Figures	xiii
List of Tables	xix
List of Abbreviations	xxi
1 Global System for Mobile Communications (GSM)	1
1.1 Circuit-Switched Data Transmission	1
1.2 Standards	3
1.3 Transmission Speeds	4
1.4 The Signaling System Number 7	5
1.4.1 <i>The SS-7 Protocol Stack</i>	5
1.4.2 <i>SS-7 Protocols for GSM</i>	8
1.5 The GSM Subsystems	9
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>	12
1.6.3 <i>The Home Location Register (HLR)</i>	13
1.6.4 <i>The Authentication Center</i>	17
1.6.5 <i>The Short Messaging Service Center (SMSC)</i>	19
1.7 The Base Station Subsystem (BSS)	20
1.7.1 <i>Frequency Bands</i>	21
1.7.2 <i>The Base Transceiver Station (BTS)</i>	22
1.7.3 <i>The GSM Air Interface</i>	24
1.7.4 <i>The Base Station Controller (BSC)</i>	30
1.7.5 <i>The TRAU for Voice Data Transmission</i>	35
1.8 Mobility Management and Call Control	44
1.8.1 <i>Location Area and Location Area Update</i>	45
1.8.2 <i>The Mobile Terminated Call</i>	46
1.8.3 <i>Handover Scenarios</i>	49

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

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

3.11.4	<i>E-DCH Mobility</i>	211
3.11.5	<i>E-DCH Terminals</i>	212
3.12	UMTS and CDMA2000	213
3.13	Questions	215
	References	215
4	Wireless Local Area Network (WLAN)	217
4.1	Wireless LAN Overview	217
4.2	Transmission Speeds and Standards	218
4.3	WLAN Configurations: From Ad-hoc to Wireless Bridging	220
4.3.1	<i>Ad-hoc, BSS, ESS, and Wireless Bridging</i>	220
4.3.2	<i>SSID and Frequency Selection</i>	223
4.4	Management Operations	225
4.5	The MAC Layer	231
4.5.1	<i>Air Interface Access Control</i>	231
4.5.2	<i>The MAC Header</i>	234
4.6	The Physical Layer	235
4.6.1	<i>IEEE 802.11b – 11 Mbit/s</i>	235
4.6.2	<i>IEEE 802.11g with up to 54 Mbit/s</i>	238
4.6.3	<i>IEEE 802.11a with up to 54 Mbit/s</i>	240
4.7	WLAN Security	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	Comparison of WLAN and UMTS	243
4.9	Questions	247
	References	247
5	802.16 and WiMAX	249
5.1	Overview	250
5.2	Standards, Evolution, and Profiles	252
5.3	WiMAX PHYs for Point-to-Multipoint FDD or TDD Operation	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	Physical Layer Framing	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	Ensuring Quality of Service	264
5.6	MAC Management Functions	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	MAC Management of User Data	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	279
5.8.1	Authentication	279
5.8.2	Ciphering	281
5.9	Advanced 802.16 Functionalities	282
5.9.1	Mesh Network Topology	282
5.9.2	Adaptive Antenna Systems	284
5.10	Mobile WiMAX: 802.16e	286
5.10.1	OFDM Multiple Access for 802.16e Networks	286
5.10.2	MIMO	288
5.10.3	Handover	289
5.10.4	Power-Saving Functionality	292
5.10.5	Idle Mode	293
5.11	WiMAX Network Infrastructure	294
5.11.1	Network Reference Architecture	295
5.11.2	Micro Mobility Management	297
5.11.3	Macro Mobility Management	298
5.12	Comparison of 802.16 with UMTS, HSDPA, and WLAN	300
5.13	Questions	301
	References	301
6	Bluetooth	303
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

6.7 Comparison between Bluetooth and Wireless LAN	347
6.8 Questions	347
References	348
Index	351