



Mobile Communication Systems and Security

MAN YOUNG RHEE

Companion Website

Contents

Preface	xi
Acknowledgement	xvii
About the Author	xix
Abbreviations	xxi
1 Global System for Mobile Communications	1
1.1 GSM Bandwidth Allocation	1
1.2 GSM System Architecture	2
1.2.1 Mobile Station (SIM + ME)	2
1.2.2 Base Station Subsystem (BSS)	3
1.2.3 Network SubSystem (NSS)	3
1.2.4 Operating SubSystem (OSS)	5
1.3 GSM Transmission Network Architecture	5
1.3.1 Message Management Layer (Layer 3)	5
1.3.2 Data Link Layer (Layer 2)	7
1.3.3 Physical Layer (Layer 1)	7
1.4 Signaling Channels on the Air Interface	8
1.4.1 Broadcast Channels (BCHs)	8
1.4.2 Common Control Channels (CCCHs)	8
1.4.3 Dedicated Control Channel (DCCH)	9
1.5 GSM Security Architecture	10
1.5.1 GSM Authentication	10
1.5.2 GSM Confidentiality	16
1.5.3 Multiple Encryption	20
1.5.4 Encryption by AES Rijndael Algorithm	24
2 cdmaOne IS-95A Technology	27
2.1 Reverse CDMA Channel	28
2.1.1 Reverse Traffic Channel	28
2.1.2 Access Channel	58
2.1.3 Multiplex Option 1 Information	64
2.1.4 Multiplex Option 2 Information	65

2.2	Forward CDMA Channel	65
2.2.1	Pilot Channel	68
2.2.2	Sync Channel	70
2.2.3	Paging Channel	78
2.2.4	Forward Traffic Channel	86
3	General Packet Radio Service (GPRS)	95
3.1	GPRS System Architecture	95
3.1.1	GPRS Network Support Nodes	96
3.1.2	Reference Points and Data Transfer Interfaces	96
3.1.3	Signaling Transfer Interfaces	97
3.1.4	GPRS-PLMN Backbone Networks	98
3.2	GPRS Logical Functions	99
3.2.1	Network Access Control	99
3.2.2	Packet Transfer and Routing	99
3.2.3	Mobility Management	100
3.2.4	State Models for Location Management	101
3.2.5	State Transitions of a Mobile Station	102
3.2.6	Packet Mobility Management (I_u Mode)	103
3.3	Layered Protocol Architecture of Transmission Plane	105
3.3.1	User Plane for A/G _b Mode	105
3.3.2	Control Plane for A/G _b Mode	107
3.3.3	Control Plane for I_u Mode	107
3.4	GPRS Ciphering Algorithm	108
3.4.1	Parameters for Algorithm Design	109
3.4.2	GPRS Encryption Algorithm 3 (GEA3)	110
3.4.3	Ciphering and Deciphering	111
4	Third-generation Partnership Projects (3GPP and 3GPP2)	119
4.1	3G Partnership Projects	120
4.2	Evolution of Mobile Radio Technologies	122
4.2.1	2G Mobile Radio Technologies	122
4.2.2	2.5G Mobile Radio Technologies	123
4.2.3	3G Mobile Radio Technologies (Situation and Status of 3G)	124
4.3	Cryptographic Protocols Applicable to Wireless Security Technologies	127
5	Universal Mobile Telecommunication System (UMTS)	133
5.1	UMTS Standardization	133
5.2	FDD/TDD Modes for UTRA Operation	134
5.3	UMTS Architecture	135
5.4	UTRAN Architecture	136
5.5	UTRAN Terrestrial Interface	137
5.5.1	Horizontal Layers	137
5.5.2	Vertical Planes	137
5.6	UTRAN-CN Interface via I_u	138

5.6.1	I _u CS Protocol Structure	139
5.6.2	I _u PS Protocol Structure	140
5.7	UMTS Security Related Features	142
5.7.1	KASUMI Encryption Function	142
5.7.2	User and Signaling Data Confidentiality	149
5.7.3	KGCORE (Core Keystream Generation Function)	152
5.7.4	Summary of Four Confidentiality Functions	153
5.7.5	Key Scheduling	153
5.8	UTRAN Overall Functions	162
5.9	UTRAN I _{ub} Interface Protocol Structure	163
5.10	UTRAN I _{ur} Interface Protocol Structure	165
6	High Speed Downlink Packet Access (HSDPA)	167
6.1	Basic Structure of HS-DSCH	167
6.1.1	Protocol Structure	167
6.1.2	HS-DSCH Physical Layer Model	169
6.2	Overview of HSDPA Enhancement Technologies	172
6.2.1	CQI Enhancement (FDD Mode)	172
6.2.2	Multiple Simultaneous Transmission to a UE Within Sub-Frame	173
6.2.3	Code Reuse for Downlink HS-DSCH	173
6.2.4	Fast Signalling Between Node B and UE	173
6.2.5	Fast Adaptive Emphasis	174
6.2.6	ACK/NACK Transmit Power Reduction for HS-DPCCH	174
6.2.7	Fractional Dedicated Physical Channel (F-DPCH)	174
6.3	HS-DSCH MAC Architecture—UE Side	175
6.3.1	Overall Architecture	175
6.3.2	MAC-d Entity	176
6.3.3	MAC-c/sh Entity	177
6.3.4	MAC-hs Entity	177
6.3.5	MAC-ehs Entity	178
6.4	HS-DSCH MAC Architecture—UTRAN Side	180
6.4.1	Overall MAC Architecture	180
6.4.2	MAC-c/sh Entity	180
6.4.3	MAC-hs Entity	180
6.4.4	MAC-ehs Entity	182
6.5	Overview of HSDPA Techniques to Support UTRA	184
6.5.1	Adaptive Modulation and Coding (AMC)	184
6.5.2	Hybrid ARQ (HARQ)	185
6.5.3	Fast Cell Selection	186
6.5.4	Multiple Input Multiple Output Antenna Processing	187
6.5.5	Handling for Error Cases	189
6.6	Orthogonal Frequency Division Multiplexing (OFDM)	190
6.6.1	OFDM Modulation Scheme	190
6.6.2	Signal Processing Over OFDM Transceiver	194
6.7	Prospect of OFDM-based Applications	195

7	CDMA2000 1x High Rate Packet Data System (1xEV-DO)	197
7.1	Architectural Reference Protocol Model	197
7.2	Air Interface Layering Protocol	200
7.2.1	Application Layer Protocols	200
7.2.2	Multi-Flow Packet Application	204
7.3	Stream Layer Protocol	206
7.3.1	Protocol Initialization	207
7.3.2	Procedures and Messages for the InConfiguration and InUse Instances	208
7.4	Session Layer Protocol	208
7.4.1	Default Session Management Protocol (SMP)	209
7.4.2	Default Address Management Protocol (AMP)	210
7.4.3	Default Session Configuration Protocol	212
7.5	Connection Layer Protocol	213
7.5.1	Data Encapsulation for InUse Protocol Instance	214
7.5.2	Air-Link Management Protocol	214
7.5.3	Initialization State Protocol	215
7.5.4	Idle State Protocol	216
7.5.5	Connected State Protocol	216
7.5.6	Route Update Protocol	217
7.5.7	Packet Consolidation Protocol	218
7.5.8	Overhead Messages Protocol	220
7.6	Security Layer Protocols	220
7.6.1	Security Layer Encapsulation	220
7.6.2	Default Security Protocol	221
7.6.3	Diffie-Hellman Key Exchange Protocol	222
7.6.4	Access Terminal (AT) Requirements	223
7.6.5	Access Network (AN) Requirements	224
7.6.6	Authentication Key and Encryption Key Generation	229
7.7	MAC Layer Protocols	234
7.7.1	Data Encapsulation for the MAC Protocols	234
7.7.2	Control Channel MAC Protocol	234
7.7.3	Procedures and Messages for the InUse Instance	237
7.7.4	Control Channel Capsules	237
7.7.5	Access Channel MAC Protocol	239
7.7.6	Forward Traffic Channel MAC Protocol	243
7.7.7	Reverse Traffic Channel MAC Protocol	247
7.8	Physical Layer Protocol	251
7.8.1	Subtype 0 (Default) and Subtype 1 Physical Layer Protocol	251
7.8.2	Frame Check Sequence (FCS) Computation	252
7.8.3	Role of Access Terminal	254
7.8.4	Access Network Requirements	269

8	CDMA2000 1x Evolution-Data and Voice (1xEV-DV)	287
8.1	UMTS (WCDMA) Versus CDMA2000—Physical Layer Harmonization	288
8.2	Reverse CDMA Channel	288
8.2.1	Reverse Pilot Channel (R-PICH)	288
8.2.2	Reverse Secondary Pilot Channel (R-SPICH)	290
8.2.3	Access Channel	291
8.2.4	Enhanced Access Channel (R-EACH)	291
8.2.5	Reverse Common Control Channel (R-CCCH)	293
8.2.6	Reverse Packet Data Control Channel (R-PDCCH)	294
8.2.7	Reverse Request Channel (R-REQCH)	295
8.2.8	Reverse Dedicated Control Channel (R-DCCH)	296
8.2.9	Reverse Acknowledgment Channel (R-ACKCH)	298
8.2.10	Reverse Channel Quality Indicator Channel (R-CQICH)	298
8.2.11	Reverse Fundamental Channel (R-FCH)	299
8.2.12	Reverse Supplemental Channel (R-SCH)	301
8.2.13	Reverse Supplemental Code Channel (R-SCCH)	303
8.2.14	Reverse Packet Data Channel (R-PDCH)	303
8.3	Forward CDMA Channel	306
8.3.1	Pilot Channels	309
8.3.2	Sync Channel (F-SYNCH)	311
8.3.3	Paging Channel (F-PCH)	312
8.3.4	Quick Paging Channel (F-QPCH)	312
8.3.5	Broadcast Control Channel (F-BCCH)	313
8.3.6	Common Assignment Channel (F-CACH)	313
8.3.7	Forward Common Control Channel (F-CCCH)	315
8.3.8	Forward Indicator Control Channel (F-ICCH)	316
8.3.9	Forward Grant Channel (F-GCH)	320
8.3.10	Forward Acknowledgment Channel (F-ACKCH)	321
8.3.11	Forward Packet Data Control Channel (F-PDCCH)	323
8.3.12	Forward Dedicated Control Channel (F-DCCH)	325
8.3.13	Forward Fundamental Channel (F-FCH)	326
8.3.14	Forward Supplemental Channel (F-SCH)	329
8.3.15	Forward Supplemental Code Channel (F-SCCH)	330
8.3.16	Forward Packet Data Channel (F-PDCH)	332
8.4	CDMA2000 Entities and Service Interfaces	332
8.4.1	CDMA2000 1x EV-DV Service Interface Structure (Mobile Station)	332
9	Advanced Encryption Standard and Elliptic Curve Cryptosystems	341
9.1	Advanced Encryption Standard (AES)	342
9.1.1	Notational Conventions	342
9.1.2	Mathematical Operations	344
9.1.3	AES Algorithm Specification	347
9.1.4	Key Expansion	347
9.1.5	AES Cipher	349
9.1.6	AES Inverse Cipher	354

9.2	Elliptic Curve Cryptosystem (ECC)	357
9.2.1	Elliptic Curves	357
9.2.2	Elliptic Curves Over Prime Field $\mathbb{Z}_p$	357
9.2.3	Elliptic Curve Over Finite Galois Field $\text{GF}(2^m)$	364
9.3	Elliptic Curve Cryptosystem versus Public-Key Cryptosystems	366
9.3.1	Diffie–Hellman Key Exchange	366
9.3.2	Elliptic Curve Diffie–Hellman Key Exchange	367
9.3.3	RSA Signature Algorithm	371
9.3.4	Elliptic Curve RSA Signature Algorithm	372
9.3.5	ElGamal Public-Key Encryption	374
9.3.6	Elliptic Curve ElGamal Encryption	375
9.3.7	Schnorr’s Authentication Algorithm	379
9.3.8	EC Schnorr’s Authentication Protocol	380
9.3.9	Public-Key Digital Signature Algorithm	381
9.3.10	Elliptic Curve Digital Signature Algorithm	382
10	Hash Function, Message Authentication Code, and Data Expansion Function	387
10.1	MD5 Message-Digest Algorithm	387
10.1.1	Append Padding Bits	387
10.1.2	Append Length	388
10.1.3	Initialize MD Buffer	388
10.1.4	Define Four Auxiliary Functions (F, G, H, I)	388
10.1.5	FF, GG, HH, and II Transformations for Rounds 1, 2, 3, and 4	389
10.1.6	Computation of Four Rounds (64 Steps)	390
10.2	Secure Hash Algorithm (SHA-1)	400
10.2.1	Message Padding	400
10.2.2	Initialize 160-Bit Buffer	400
10.2.3	Functions Used	401
10.2.4	Constants Used	401
10.2.5	Computing the Message Digest	402
10.3	Hashed Message Authentication Codes (HMAC)	406
10.3.1	HMAC Structure	406
10.3.2	HMAC Computation Using RFC Method	406
10.3.3	HMAC Computation (Alternative Method)	409
10.4	Data Expansion Function	412
	Bibliography	417
	Index	421