

**Martin Sauter**

# **Grundkurs Mobile Kommunikationssysteme**

UMTS, HSPA und LTE, GSM, GPRS,  
Wireless LAN und Bluetooth

**5., überarbeitete und erweiterte Auflage**

 **Springer Vieweg**

# Inhaltsverzeichnis

## GSM

- 1.1 Leitungsvermittelnde Datenübertragung
  - 1.1.1 Klassische Leitungsvermittlung
  - 1.1.2 Virtuelle Leitungsvermittlung über IP
- 1.2 Standards
- 1.3 Übertragungsgeschwindigkeiten
- 1.4 Das Signalisierungssystem Nr. 7
  - 1.4.1 Klassischer SS-7-Protokollstack
  - 1.4.2 Spezielle SS-7-Protokolle für GSM
  - 1.4.3 IP-basierter SS-7-Protokollstack
- 1.5 Die GSM Subsysteme
- 1.6 Das Network Subsystem
  - 1.6.1 Die Mobile Vermittlungsstelle (MSC), Server und Gateway
  - 1.6.2 Das Visitor Location Register (VLR)
  - 1.6.3 Das Home Location Register (HLR)
  - 1.6.4 Das Authentication Center (AC)
  - 1.6.5 Das Short Message Service Center (SMSC)
- 1.7 Das Base Station Subsystem (BSS) und Sprachcodierung
  - 1.7.1 Frequenzbereiche
  - 1.7.2 Base Transceiver Station (BTS)
  - 1.7.3 Die GSM-Luftschnittstelle
  - 1.7.4 Der Base Station Controller (BSC)
  - 1.7.5 Die TRAU für Sprachdatenübertragung
  - 1.7.6 Channel Coder und Interleaver in der BTS
  - 1.7.7 Verschlüsselung und Sicherheitsaspekte
  - 1.7.8 Modulation
  - 1.7.9 Voice Activity Detection

1.8	Mobility Management und Call Control	55
1.8.1	Cell Reselection und Location Area Update	56
1.8.2	Mobile Terminated Call	57
1.8.3	Handoverszenarien	60
1.9	Mobile Endgeräte	63
1.9.1	Aufbau eines einfachen GSM Telefons	63
1.9.2	Aufbau eines Smartphones	65
1.10	Die SIM-Karte	67
1.11	Das Intelligent Network Subsystem und CAMEL	72
1.12	Fragen und Aufgaben	74
<b>2</b>	<b>GPRS und EDGE</b>	<b>77</b>
2.1	Leitungsvermittelte Datenübertragung	77
2.2	Paketorientierte Datenübertragung	78
2.3	GPRS auf der Luftschnittstelle	81
2.3.1	GPRS Timeslot-Nutzung im Vergleich zu GSM	81
2.3.2	Gleichzeitige Nutzung einer Basisstation von GSM und GPRS . . . .	83
2.3.3	Coding Schemes	84
2.3.4	EDGE (EGPRS)	86
2.3.5	Mobile Device Classes	87
2.3.6	Network Operation Mode (NOM)	88
2.3.7	GPRS-Kanalstruktur auf der Luftschnittstelle	90
2.4	GPRS-Zustandsmodell	93
2.5	GPRS-Netzwerkelemente	96
2.5.1	Die Packet Control Unit (PCU)	96
2.5.2	Der Serving GPRS Support Node (SGSN)	98
2.5.3	Der Gateway GPRS Support Node (GGSN)	100
2.6	GPRS Radio Resource Management	100
2.7	GPRS-Schnittstellen und Protokolle	104
2.8	GPRS Mobility und Session Management (GMM/SM)	109
2.8.1	Mobility Management-Aufgaben	109
2.8.2	GPRS Session Management	112
2.9	Session Management aus Anwendersicht	115
2.9.1	Leitungsvermittelter Verbindungsaufbau	115
2.9.2	GPRS-Verbindungsaufbau	116
2.10	Der Multimedia Messaging Service (MMS) über GPRS	119
2.11	Weiterentwicklung von EDGE	124
2.12	Fragen und Aufgaben	124
<b>3</b>	<b>UMTS und HSPA</b>	<b>127</b>
3.1	Überblick, Historie und Zukunft	127
3.1.1	3GPP Release 99: Die erste Version des neuen Radionetzwerks . . .	129
3.1.2	3GPP Release 4: Bearer Independent Core Network	130

3.1.3	3GPP Release 5: IP Multimedia Subsystem und HSDPA	132
3.1.4	3GPP Release 6: High Speed Uplink Packet Access (HSUPA)	135
3.1.5	3GPP Release 7: HSPA+ und CPC	135
3.1.6	3GPP Release 8: LTE, HSPA+ Verbesserungen und Femtozellen ..	136
3.1.7	3GPP Release 9: Digitale Dividende und Dual Cell	137
3.1.8	3GPP Release 10 und 11: LTE-Advanced	138
3.2	Wichtige neue Konzepte in UMTS Release 99	139
3.2.1	Der Radio Access Bearer (RAB)	139
3.2.2	Aufteilung in Access Stratum und Non-Access Stratum	140
3.2.3	Gemeinsames Übertragungsprotokoll für CS und PS	141
3.3	Code Division Multiple Access (CDMA)	142
3.3.1	Spreizfaktor, Chiprate und Prozessgewinn	146
3.3.2	Der OVSF-Codebaum	147
3.3.3	Scrambling in Uplink- und Downlink-Richtung	148
3.3.4	Frequenz- und Zellplanung in UMTS	150
3.3.5	Near-Far-Effekt und Zellatmung	150
3.3.6	Vorteile des UMTS-Radionetzwerkes gegenüber GSM	152
3.4	UMTS-Kanalstruktur auf der Luftschnittstelle	154
3.4.1	User Plane und Control Plane	154
3.4.2	Common und Dedicated-Kanäle	155
3.4.3	Logische, Transport- und Physikalische Kanäle	156
3.4.4	Beispiel: Netzwerksuche	160
3.4.5	Beispiel: Der erste Netzwerkzugriff	162
3.4.6	Der Uu Protokoll Stack	164
3.5	Das UMTS Terrestrial Radio Access Network (UTRAN)	169
3.5.1	Node-B, Iub Interface, NBAP und FP	169
3.5.2	Der RNC, Iu, Iub und Iur-Schnittstelle, RANAP und RNSAP	171
3.5.3	Adaptive Multi-Rate-NB und-WB für Sprachübertragung	176
3.5.4	Radio Resource Control (RRC)-Zustände	178
3.6	Mobility Management aus Sicht des Kernnetzes	183
3.7	Mobility Management aus Sicht des Radionetzwerkes	184
3.7.1	Mobility Management im Cell-DCH-Zustand	184
3.7.2	Mobility Management im Idle-Zustand	192
3.7.3	Mobility Management in anderen Zuständen	194
3.8	UMTS CS und PS-Verbindungsaufbau	196
3.9	High Speed Downlink Packet Access (HSDPA)	200
3.9.1	HSDPA-Kanäle	200
3.9.2	Kleinere Delay- Zeiten und Hybrid ARQ (HARQ)	202
3.9.3	Scheduling im Node-B	204
3.9.4	Adaptive Modulation, Codierung und Geschwindigkeit	205
3.9.5	Auf- und Abbau einer HSDPA-Verbindung	208
3.9.6	HSDPA Mobility Management	209

3.10	High Speed Uplink Packet Access (HSUPA)	210
3.10.1	E-DCH-Kanalstruktur	212
3.10.2	Der E-DCH-Protokoll Stack	215
3.10.3	E-DCH Scheduling	217
3.10.4	E-DCH Mobility	220
3.10.5	E-DCH-Endgeräte	221
3.11	Continuous Packet Connectivity	222
3.11.1	Ein neues Uplink Control Channel Slot Format	222
3.11.2	Reduzierung des CQI Reporting Intervals, DTX und DRX	223
3.11.3	HS-SCCH Discontinuous Reception	223
3.11.4	HS-SCCH-less Operation	224
3.11.5	Enhanced Cell-FACH, Cell/URA PCH States	225
3.12	FastDormancy	227
3.13	Fragen und Aufgaben	227
4	<b>Long Term Evolution (LTE)</b>	229
4.1	Einleitung und Überblick	229
4.2	Netzwerk-Architektur und Schnittstellen	231
4.2.1	LTE-Endgeräte und die LTE Uu-Schnittstelle	232
4.2.2	Der eNodeB und die S1 und X2-Schnittstellen	234
4.2.3	Die Mobility Management Entity (MME)	238
4.2.4	Das Serving-Gateway	239
4.2.5	Das PDN-Gateway	240
4.2.6	Das HSS	240
4.3	Die LTE-Luftschnittstelle und das Radionetzwerk	241
4.3.1	OFDMA für die Datenübertragung im Downlink	242
4.3.2	SC-FDMA für Uplink Übertragungen	244
4.3.3	Symbole, Slots, Radio Blocks und Frames	245
4.3.4	Referenz- und Synchronisations-Signale	247
4.3.5	Das LTE-Kanalmodell in Downlink-Richtung	248
4.3.6	Downlink Management-Kanäle	249
4.3.7	System Information Messages	250
4.3.8	Das LTE-Kanalmodell in der Uplink-Richtung	250
4.3.9	Multiple Input Multiple Output Übertragungen	251
4.3.10	HARQ	253
4.3.11	PDPCP – Komprimierung und Verschlüsselung	253
4.4	Scheduling	254
4.4.1	Downlink Scheduling	254
4.4.2	Uplink Scheduling	257
4.5	Grundsätzliche Prozeduren	258
4.5.1	Netzwerksuche	258
4.5.2	Attach und Aktivierung des Default Bearers	261
4.5.3	Handover Szenarien	265

4.6	Mobility Management und Leistungsoptimierung	268
4.6.1	Mobilitätsmanagement im Connected State	268
4.6.2	Mobility Management im Idle State	269
4.7	LTE Sicherheitsarchitektur	271
4.8	Zusammenspiel mit UMTS und GSM	272
4.8.1	Cell Reselection zwischen LTE und GSM/UMTS	273
4.8.2	Release mit Redirect zwischen LTE und GSM/UMTS	274
4.8.3	Handover zwischen LTE und GSM/UMTS	275
4.9	Backhaulverbindungen	276
4.10	Self-Organizing Networks	277
4.11	CS-Fallback für Sprache und SMS mit LTE	278
4.11.1	SMS über SGs	279
4.11.2	CS Fallback	280
4.12	Voice over LTE (VoLTE)	283
4.12.1	Das Session Initiation Protocol (SIP)	284
4.12.2	Das IP Multimedia Subsystem (IMS) und VoLTE	289
4.12.3	Single Radio Voice Call Continuity	293
4.13	Fragen und Aufgaben	295
<b>5</b>	<b>Wireless LAN IEEE 802.11</b>	<b>297</b>
5.1	Wireless LAN Überblick	297
5.2	Geschwindigkeiten und Standards	298
5.3	WLAN-Konfigurationen: Von Ad-hoc bis Wireless Bridging	300
5.3.1	Ad-hoc, BSS, ESS und Wireless Bridging	300
5.3.2	SSID und Frequenzwahl	303
5.4	Management-Operationen	305
5.5	Die MAC-Schicht	311
5.5.1	Zugriffssteuern auf das Übertragungsmedium	311
5.5.2	Der MAC Header	314
5.6	Physical Layer und MAC-Erweiterungen	315
5.6.1	IEEE 802.11b mit bis zu 11 Mbit/s	316
5.6.2	IEEE 802.11g mit bis zu 54 Mbit/s	318
5.6.3	IEEE 802.11a mit bis zu 54 Mbit/s	320
5.6.4	IEEE 802.11n mit bis zu 600 Mbit/s	321
5.6.5	802.11ac	331
5.7	Wireless LAN-Sicherheit	333
5.7.1	Wired Equivalent Privacy (WEP)	333
5.7.2	WPA und WPA2 Personal Mode-Authentifizierung	335
5.7.3	WPA und WPA2 Enterprise Mode Authentifizierung	336
5.7.4	Authentifizierung mit EAP-SIM	338
5.7.5	Verschlüsselung mit WPA und WPA2	340
5.7.6	Wi-Fi Protected Setup (WPS)	342
5.8	IEEE 802.11e und WMM – Quality of Service	343

5.9	Vergleich zwischen Wireless LAN und LTE	350
5.10	Fragen und Aufgaben	354
<b>6</b>	<b>Bluetooth</b>	<b>355</b>
6.1	Überblick und Anwendungen	355
6.2	Physikalische Eigenschaften	357
6.3	Piconetze und das Master Slave Konzept	359
6.4	Der Bluetooth Protokoll Stack	362
6.4.1	Der Baseband Layer	362
6.4.2	Der Link Controller	367
6.4.3	Der Link Manager	370
6.4.4	Das HCI Interface	372
6.4.5	Der L2CAP Layer	374
6.4.6	Das Service Discovery Protocol	376
6.4.7	Der RFCOMM Layer	378
6.4.8	Aufbau einer Verbindung im Überblick	380
6.5	Bluetooth Sicherheit	381
6.5.1	Pairing bis Bluetooth 2.0	381
6.5.2	Pairing ab Bluetooth 2.1 (Secure Simple Pairing)	383
6.5.3	Authentifizierung	385
6.5.4	Verschlüsselung	386
6.5.5	Autorisierung	387
6.5.6	Sicherheitsmodi	387
6.6	Bluetooth Profile	388
6.6.1	Grundlegende Profile: GAP, SDP und Serial Profile	390
6.6.2	Object Exchange Profile: FTP, Object Push und Synchronize	391
6.6.3	Headset, Hands-Free und SIM-Access Profile	394
6.6.4	High Quality Audio Streaming	397
6.7	Fragen und Aufgaben	401
	<b>Weiterführende Literatur</b>	<b>403</b>
	<b>Sachwortverzeichnis</b>	<b>405</b>