

Martin Sauter

**Grundkurs
Mobile
Kommunikationssysteme**

Leserstimmen zu vorangegangenen Auflagen:

„Leicht verständliche und übersichtliche Darstellung mit hoher Praxisrelevanz. Als Lernhilfe mit Fragen und Aufgaben (und gut gepflegtem Online-Service mit Antworten) bestens geeignet.“

Achim Büge, Berufskolleg Mühlheim

„Eine echte Einführung! Gut strukturiert, passende Tiefe, angenehmer Umfang. Ich werde das Buch auf der nächsten IT-Lehrerfortbildung vorstellen.“

Jürgen Schumacher, Erich-Gutenberg-Berufskolleg Köln

„Gute Einführung und Nachschlagewerk zu den derzeitigen digitalen mobilen Kommunikationssystemen für Studierende und Praktiker.“

Prof. Dr.-Ing. Bernhard Hoier, FH Brandenburg

„Klare Struktur und verständliche Sprache bei gleichzeitig tiefgehendem Wissen zu den wesentlichen mobilen Kommunikationssystemen machen dieses Buch auch zu einem gelungenen Nachschlagewerk.“

Prof. Dr. Bettina Schnor, Universität Potsdam

„Endlich ein Buch, das NICHT-Elektrotechnikern, z. B. Informatikern, den Einstieg in mobile Kommunikationstechnologien ermöglicht.“

Prof. Dr. Gernot Bauer, FH Münster

„Alle mobilen Technologien in einem Buch.“

Prof. Dr. Jörg Keller, Fernuniversität Hagen

„Das Buch besticht durch seine Aktualität und die Praxisnähe des Autors. Ich bin begeistert!“

Prof. Dr. Johannes Maucher, HDM Stuttgart

„Dieses Buch bietet dem Leser praxis- und detailgerechtes Wissen zu mobilen Kommunikationssystemen. Vom derzeitigen GSM und GPRS über UMTS bis hin zu WLANs und Bluetooth werden die technischen Konzepte, Standards und Protokolle verständlich dargestellt.“

Prof. Dr. Jürgen Scherff, FH Furtwangen

Martin Sauter

Grundkurs Mobile Kommunikationssysteme

**Von UMTS und HSDPA, GSM und GPRS zu
Wireless LAN und Bluetooth Piconetzen**

Mit 196 Abbildungen

3., erweiterte Auflage



Bibliografische Information Der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der
Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über
<<http://dnb.d-nb.de>> abrufbar.

Das in diesem Werk enthaltene Programm-Material ist mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Der Autor übernimmt infolgedessen keine Verantwortung und wird keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Programm-Materials oder Teilen davon entsteht.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne von Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürfen.

Höchste inhaltliche und technische Qualität unserer Produkte ist unser Ziel. Bei der Produktion und Auslieferung unserer Bücher wollen wir die Umwelt schonen: Dieses Buch ist auf säurefreiem und chlorfrei gebleichtem Papier gedruckt. Die Einschweißfolie besteht aus Polyäthylen und damit aus organischen Grundstoffen, die weder bei der Herstellung noch bei der Verbrennung Schadstoffe freisetzen.

1. Auflage 2004
2. Auflage 2006
- 3., erweiterte Auflage 2008

Alle Rechte vorbehalten

© Friedr. Vieweg & Sohn Verlag | GWV Fachverlage GmbH, Wiesbaden 2008

Lektorat: Sybille Thelen / Andrea Broßler

Der Vieweg Verlag ist ein Unternehmen von Springer Science+Business Media.

www.vieweg.de



Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Umschlaggestaltung: Ulrike Weigel, www.CorporateDesignGroup.de

Druck und buchbinderische Verarbeitung: MercedesDruck, Berlin

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.

Printed in Germany

ISBN 978-3-8348-0397-9

Vorwort zur dritten Auflage

Zwischen der zweiten und dritten Auflage dieses Buches hat sich in nur 12 Monaten wieder einiges in der Mobilfunkwelt getan und die aktuelle Auflage enthält wiederum zahlreiche Erweiterungen. Während eine der wichtigsten Neuerungen der zweiten Auflage die Beschreibung des UMTS Turbo „HSDPA“ war, ist in der Zwischenzeit auch „HSUPA“, eine Technik für schnellere Geschwindigkeiten im Uplink, verfügbar und darf deshalb in diesem Buch nicht fehlen.

Zum Erstaunen vieler Experten erfreuen sich die schon recht lange in der Praxis betriebenen GSM/GPRS Netze weiterhin weltweit eines starken Wachstums und der GPRS Beschleuniger EDGE wird mittlerweile auch in Deutschland von zwei Netzbetreibern angeboten. Schnelle Internetverbindungen sind somit nun auch in ländlichen Gebieten möglich, in denen es noch keine UMTS/HSPA Versorgung gibt. Diesem Trend wurde schon in der zweiten Auflage Rechnung getragen. Die dritte Auflage enthält nun auch Informationen über neue GPRS und EDGE Endgeräteklassen, die noch höhere Übertragungsgeschwindigkeiten unterstützen.

Während Wireless LAN bei Erscheinen der ersten Auflage nur wenig verbreitet war, hat es seither einen wahren Ansturm auf diese Art der Heim- und Bürovernetzung gegeben. Außerdem nimmt die Verbreitung von Wireless LAN Hotspots in Hotels, Flughäfen und Cafés weiter zu. Während heute der 802.11g Standard mit etwa 20 MBit/s auf Anwendungsebene üblich ist, gibt es mittlerweile eine stabile Vorversion des 802.11n Standards mit Datenraten auf Anwendungsebene von 150 MBit/s und mehr. In dieser Auflage wurde das Wireless LAN Kapitel deshalb stark erweitert und enthält jetzt eine Beschreibung von 802.11n sowie der 802.11e Quality of Service Erweiterung, die auch unter dem Namen Wireless Multimedia (WMM) bekannt ist. Schließlich hat sich auch beim Thema WLAN Sicherheit seit dem Erscheinen der ersten Auflage einiges getan und Kapitel 4 enthält nun eine ausführlichere Beschreibung zu Authentifizierung und Verschlüsselung mit WPA und WPA2.

Auch beim Bluetooth Standard gibt es zahlreiche Neuerungen. Vermehrt bieten heute Smartphones und auch Mobiltelefone im

mittleren Preissegment eine MP-3 Player Funktion, für die eine Verbindung zu einem Kopfhörer über das Headset- oder Handsfree Profil keine ausreichende Klangqualität bietet. Deshalb setzen Endgerätehersteller vermehrt auf das Advanced Audio Distribution Profil (A2DP), das nun im Bluetooth Kapitel beschrieben ist. Die in 2007 erschienene Bluetooth 2.1 + EDR Erweiterung brachte zudem neue Pairing Protokolle, um gefundene Schwachstellen zu beseitigen. Eine Beschreibung dieser Protokolle und anderer Verbesserungen wie z.B. die Verwendung von Near Field Communication (NFC) Tags sowie neuer Stromsparmechanismen ist nun ebenfalls enthalten.

Bleibt mir noch, Ihnen an dieser Stelle viel Freude beim Studium dieses Buches, und beim Experimentieren und Nutzen mobiler Kommunikation zu wünschen.

Paris, im August 2007

Martin Sauter

Vorwort

Mobile Kommunikationssysteme wie GSM, GPRS, UMTS, Wireless LAN und Bluetooth bieten heute eine große Vielfalt von Anwendungsmöglichkeiten. Um einen Einblick in die Technik dieser Systeme zu gewinnen, gibt es eine große Anzahl von Publikationen. In Buchform sind diese jedoch meist sehr umfangreich und für eine Einführung oft zu komplex. Publikationen im Internet hingegen sind meist nur sehr kurz und oberflächlich oder beschäftigen sich nur mit einer speziellen Eigenschaft eines Systems. Aus diesem Grund konnte ich während meiner Vorlesungen zu diesem Thema keine einzelne Publikation empfehlen, die eine Einführung in diese Systeme mit der nötigen Detailtiefe geboten hätte. Mit dem vorliegenden Buch möchte ich dies ändern.

Jedes der fünf Kapitel gibt eine detaillierte Einführung und Überblick über jeweils eines der zu Anfang genannten Systeme. Besonders wichtig ist mir auch, einen Eindruck zu vermitteln, welche Gedanken hinter der Entwicklung der unterschiedlichen Systeme standen. Neben dem „Wie“ ist also auch das „Warum“ zentraler Bestandteil jedes Kapitels. Außerdem wird durch zahlreiche Vergleiche zwischen den unterschiedlichen Technologien deutlich, wo die Anwendungsgebiete der einzelnen Systeme liegen. In manchen Fällen konkurrieren die Systeme miteinander, in vielen Fällen jedoch ergibt erst eine Kombination mehrerer Systeme eine interessante Anwendung. Abgerundet wird jedes Kapitel durch einen Fragen- und Aufgabenkatalog zur Lernzielkontrolle und Wiederholung.

Um einen tieferen Einblick in das eine oder andere System zu gewinnen, sind in den Kapiteln zahlreiche Verweise auf die entsprechenden Standards zu finden. Sie bilden eine ideale Ergänzung für einen tieferen Einblick in die einzelnen Systeme und sollten mit Hilfe der Hintergrundinformationen in diesem Buch auch etwas einfacher zu interpretieren sein.

Den Entschluss, mein Wissen zu diesen Themen als Buch zu veröffentlichen, fasste ich nach vielen theoretischen Gedankenspielen ganz spontan in einer Pariser Buchhandlung. Dort stieß ich zufällig auf ein Buch mit einem ganz anderen Themenschwerpunkt, mit dessen Autor ich jedoch den Umstand gemeinsam habe, dass wir für die gleiche Firma arbeiten. Ich nahm

Kontakt mit ihm auf, und er schilderte mir während eines ausgedehnten Mittagessens, wie man von der ersten Idee zu einem fertigen Buch kommt. An dieser Stelle möchte ich mich deshalb sehr herzlich bei Pierre Lescuyer bedanken, dessen Tipps mir beim Start meines eigenen Buchprojekts sehr weitergeholfen haben.

Außerdem gebührt mein großer Dank auch Berenike, die mir mit Ihrer Liebe und Freundschaft während dieses Projekts immer inspirierend zur Seite stand.

Weiterhin gebührt mein Dank auch Thomas Kempf, Christophe Schmid, Markus Rösch, Thomas Ehrle und ganz besonders Jörg Becker. Mit ihrem Wissen und großen Einsatz ihrer privaten Zeit haben sie mich vor einigen Fehlern bewahrt und in zahlreichen Gesprächen wichtige Anregungen und Verbesserungsvorschläge gegeben.

Nicht zuletzt gilt mein Dank auch Dr. Reinald Klockenbusch, der dieses Buchprojekt von Anfang an begleitet hat und an der Ausrichtung des Buches maßgeblich beteiligt war.

Paris, im Juni 2004 Martin Sauter

Inhaltsverzeichnis

1	GSM	1
1.1	Leitungsvermittelnde Datenübertragung	1
1.2	Standards	3
1.3	Übertragungsgeschwindigkeiten	5
1.4	Das Signalisierungssystem Nr. 7	6
1.4.1	Allgemeiner SS-7 Protokoll Stack	8
1.4.2	Spezielle SS-7 Protokolle für GSM	11
1.5	Die GSM Subsysteme	12
1.6	Das Network Subsystem	13
1.6.1	Die Mobile Vermittlungsstelle (MSC)	13
1.6.2	Das Visitor Location Register (VLR)	17
1.6.3	Das Home Location Register (HLR)	18
1.6.4	Das Authentication Center (AC)	24
1.6.5	Das Short Message Service Center (SMSC)	26
1.7	Das Base Station Subsystem (BSS)	28
1.7.1	Frequenzbereiche	28
1.7.2	Base Transceiver Station (BTS)	31
1.7.3	Die GSM Luftschnittstelle	33
1.7.4	Der Base Station Controller (BSC)	43
1.7.5	Die TRAU für Sprachdatenübertragung	50
1.8	Mobility Management und Call Control	62
1.8.1	Location Area und Location Area Update	63
1.8.2	Mobile Terminated Call	65
1.8.3	Handoverszenarien	68
1.9	Die Mobile Station	71
1.10	Die SIM Karte	75
1.11	Das Intelligent Network Subsystem und CAMEL	82
1.12	Fragen und Aufgaben	86

2	GPRS und EDGE	87
2.1	Leitungsvermittelte Datenübertragung	87
2.2	Paketorientierte Datenübertragung	88
2.2.1	GPRS und das IP Protokoll	92
2.2.2	GPRS im Vergleich zur Datenübertragung im Festnetz	92
2.3	GPRS auf der Luftschnittstelle	93
2.3.1	GPRS Timeslot Nutzung im Vergleich zu GSM	93
2.3.2	Gleichzeitige Nutzung einer Basisstation von GSM und GPRS	96
2.3.3	Coding Schemes	97
2.3.4	EDGE (EGPRS)	99
2.3.5	Mobile Station Classes	101
2.3.6	Network Operation Mode (NOM)	102
2.3.7	GPRS Kanalstruktur auf der Luftschnittstelle	105
2.4	GPRS Zustandsmodell	108
2.5	GPRS Netzwerkelemente	112
2.5.1	Die Packet Control Unit (PCU)	112
2.5.2	Der Serving GPRS Support Node (SGSN)	114
2.5.3	Der Gateway GPRS Support Node (GGSN)	117
2.6	GPRS Radio Resource Management	118
2.7	GPRS Schnittstellen und Protokolle	122
2.8	GPRS Mobility und Session Management (GMM/SM)	128
2.8.1	Mobility Management Aufgaben	129
2.8.2	GPRS Session Management	132
2.9	Session Management aus Anwendersicht	136
2.9.1	Leitungsvermittelter Verbindungsaufbau	136
2.9.2	GPRS Verbindungsaufbau	138
2.10	Der Multimedia Messaging Service (MMS) über GPRS	141
2.11	Fragen und Aufgaben	148

3 UMTS und HSPA	149
3.1 Überblick, Historie und Zukunft	149
3.1.1 Release 99: Neues Radionetzwerk	150
3.1.2 UMTS Release 4: Bearer Independent Core Network	154
3.1.3 UMTS Release 5: Einführung des IP Multimedia Subsystems	155
3.1.4 UMTS Release 5: High Speed Downlink Packet Access (HSDPA)	158
3.1.5 UMTS Release 6: High Speed Uplink Packet Access (HSUPA).....	160
3.2 Wichtige neue Konzepte in UMTS Release 99	160
3.2.1 Der Radio Access Bearer (RAB).....	160
3.2.2 Aufteilung in Access Stratum und Non-Access Stratum	161
3.2.3 Gemeinsames Übertragungsprotokoll für CS und PS.....	162
3.3 Code Division Multiple Access (CDMA)	163
3.3.1 Spreizfaktor, Chiprate und Prozessgewinn	169
3.3.2 Der OVFS Codebaum	170
3.3.3 Scrambling in Uplink- und Downlink Richtung	172
3.3.4 Frequenz- und Zellplanung in UMTS	174
3.3.5 Near-Far Effekt und Zellatmung	175
3.3.6 Vorteile des UMTS Radionetzwerkes gegenüber GSM.....	178
3.4 UMTS Kanalstruktur auf der Luftschnittstelle.....	180
3.4.1 User Plane und Control Plane.....	180
3.4.2 Common und Dedicated Kanäle.....	181
3.4.3 Logische, Transport- und Physikalische Kanäle	182
3.4.4 Beispiel: Netzwerksuche	188
3.4.5 Beispiel: Der erste Netzwerkzugriff.....	191
3.4.6 Der Uu Protokoll Stack.....	193
3.5 Das UMTS Terrestrial Radio Access Network (UTRAN).....	200
3.5.1 Node-B, Iub Interface, NBAP und FP.....	200
3.5.2 Der RNC, Iu, Iub und Iur Schnittstelle, RANAP und RNSAP.....	202
3.5.3 Adaptive Multi Rate (AMR) für Sprachübertragung	210
3.5.4 Radio Resource Control (RRC) Zustände	211
3.6 Mobility Management aus Sicht des Kernnetzes	218
3.7 Mobility Management aus Sicht des Radionetzwerkes.....	220

3.7.1	Mobility Management im Cell-DCH Zustand	221
3.7.2	Mobility Management im Idle Zustand.....	232
3.7.3	Mobility Management in anderen Zuständen	233
3.8	UMTS CS und PS Verbindungsaufbau.....	236
3.9	High Speed Downlink Packet Access	240
3.9.1	HSDPA Kanäle	240
3.9.2	Kleinere Delay- Zeiten und Hybrid ARQ (HARQ).....	243
3.9.3	Scheduling im Node-B.....	246
3.9.4	Adaptive Modulation, Codierung und Geschwindigkeit	247
3.9.5	Auf- und Abbau einer HSDPA Verbindung	250
3.9.6	HSDPA Mobility Management.....	252
3.10	UMTS Release 6: High Speed Uplink Packet Access (HSUPA)	253
3.10.1	E-DCH Kanalstruktur	256
3.10.2	Der E-DCH Protokoll Stack	260
3.10.3	E-DCH Scheduling	262
3.10.4	E-DCH Mobility	267
3.10.5	E-DCH Endgeräte	268
3.11	Fragen und Aufgaben.....	270
4	Wireless LAN IEEE 802.11	271
4.1	Wireless LAN Überblick	271
4.2	Geschwindigkeiten und Standards	272
4.3	WLAN Konfigurationen: Von Ad-hoc bis Wireless Bridging	275
4.3.1	Ad-hoc, BSS, ESS und Wireless Bridging	275
4.3.2	SSID und Frequenzwahl.....	279
4.4	Management Operationen.....	282
4.5	Die MAC Schicht.....	289
4.5.1	Zugriffssteuerung auf das Übertragungsmedium.....	290
4.5.2	Der MAC Header.....	294
4.6	Physical Layer und MAC-Erweiterungen.....	295
4.6.1	IEEE 802.11b mit bis zu 11 MBit/s.....	295
4.6.2	IEEE 802.11g mit bis zu 54 MBit/s.....	300

4.6.3	IEEE 802.11a mit bis zu 54 MBit/s	302
4.6.4	IEEE 802.11n mit bis zu 600 MBit/s.....	303
4.7	Wireless LAN Sicherheit	317
4.7.1	Wired Equivalent Privacy (WEP)	318
4.7.2	WPA und WPA2 Personal Mode Authentifizierung.....	319
4.7.3	WPA und WPA2 Enterprise Mode Authentifizierung	322
4.7.4	Authentifizierung mit EAP-SIM.....	324
4.7.5	Verschlüsselung mit WPA und WPA2	327
4.8	IEEE 802.11e und WMM – Quality of Service.....	329
4.9	Vergleich zwischen Wireless LAN und UMTS	337
4.10	Fragen und Aufgaben.....	343
5	Bluetooth	345
5.1	Überblick und Anwendungen	345
5.2	Physikalische Eigenschaften.....	348
5.3	Piconetze und das Master Slave Konzept	352
5.4	Der Bluetooth Protokoll Stack.....	355
5.4.1	Der Baseband Layer.....	355
5.4.2	Der Link Controller.....	363
5.4.3	Der Link Manager	367
5.4.4	Das HCI Interface.....	368
5.4.5	Der L2CAP Layer	372
5.4.6	Das Service Discovery Protocol.....	374
5.4.7	Der RFCOMM Layer.....	376
5.4.8	Aufbau einer Verbindung im Überblick.....	379
5.5	Bluetooth Sicherheit	380
5.5.1	Pairing bis Bluetooth 2.0	381
5.5.2	Pairing ab Bluetooth 2.1 (Secure Simple Pairing).....	382
5.5.3	Authentifizierung.....	385
5.5.4	Verschlüsselung	386
5.5.5	Autorisierung.....	387
5.5.6	Sicherheitsmodi.....	388

5.6	Bluetooth Profile	390
5.6.1	Grundlegende Profile: GAP, SDP und Serial Profile	392
5.6.2	Netzwerkprofile: DUN, LAP und PAN	393
5.6.3	Object Exchange Profile: FTP, Object Push und Synchronize.....	398
5.6.4	Headset, Hands-Free und SIM-Access Profile	402
5.6.5	High Quality Audio Streaming	407
5.7	Vergleich zwischen Bluetooth und Wireless LAN	411
5.8	Fragen und Aufgaben.....	412
	Literaturverzeichnis	415
	Sachwortverzeichnis.....	417